

**Česká zemědělská univerzita v Praze**



Technická fakulta

**Spolehlivost biometrických systémů pro identifikaci na základě obličeje  
v závislosti na druhu použitého přívsvitu**

Diplomová práce

Vedoucí diplomové práce: Ing. Veronika Hartová, Ph.D.

Diplomant: Bc. Tomáš Fiala

PRAHA 2017

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

## ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Tomáš Fiala

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Spolehlivost biometrických systémů pro identifikaci na základě obličeje v závislosti na druhu použitého přisvitu

Název anglicky

Reliability of biometrics systems for identification based on the face depending on the kind of illuminators

---

Cíle práce

Téma diplomové práce se věnuje biometrické identifikaci osob, která je založena na rozpoznání obličeje uživatele. Rozebírá jednotlivé možnosti této identifikace a její výhody a nedostatky. Práce je zaměřena na různé druhy přisvitu a jak tyto odlišnosti v přisvitech ovlivňují spolehlivost těchto čteček.

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýzách odborných informačních zdrojů. Praktická část práce je zaměřena na otestování jednotlivých druhů přisvitu k těmto čtečkám a následné zpracování naměřených dat. Na základě rozboru teoretických poznatků a výsledků praktické části práce budou formulovány závěry diplomové práce.

**Doporučený rozsah práce**

50-60 str.

**Klíčová slova**

identifikace, přísvit, biometrie, sken tváře

---

**Doporučené zdroje informací**

HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475.

JAIN, A.; BOLLE, R.; PANKANTI, S. „Biometrics. Personal Identification in Networked Society.“ Norwell, Massachusetts, USA, Kluwer Academic Publisher, 1999, ISBN 0-7923-8345-1.

KŘEČEK, S., a spol.: Příručka zabezpečovací techniky. Blatná: Circetus, 2006. 313s. ISBN 80-902938-2-4.

RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kolektiv. „Biometrie a identita člověka ve forenzních a komerčních aplikacích.“ Praha, Nakladatelství Grada, 2012

---

**Předběžný termín obhajoby**

2016/17 LS – TF

**Vedoucí práce**

Ing. Veronika Hartová, Ph.D.

**Garantující pracoviště**

Katedra elektrotechniky a automatizace

---

Elektronicky schváleno dne 12. 1. 2016

**prof. Ing. Jaromír Volf, DrSc.**

Vedoucí katedry

Elektronicky schváleno dne 2. 3. 2016

**prof. Ing. Vladimír Jurča, CSc.**

Děkan

V Praze dne 19. 01. 2017

---

## Prohlášení

Prohlašuji, že jsem diplomovou práci na téma: **Spolehlivost biometrických systémů pro identifikaci na základě obličeje v závislosti na druhu použitého přísvitu** vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

Prohlašuji, že tištěná i elektronická verze diplomové práce jsou totožné.

.....

Bc. Tomáš Fiala

## **Poděkování**

Velmi bych chtěl poděkovat své vedoucí diplomové práce paní Ing. Veronice Hartové, Ph.D. za veškeré rady, připomínky, vedení, ochotu a poskytnuté konzultační hodiny. Dále bych chtěl poděkovat panu Ing. Janu Hartovi, Ph.D. za hodnotné připomínky a paní Mgr. Adrianě Laputkové za gramatickou kontrolu anglického abstraktu. Dále bych velmi rád poděkoval zejména svým rodičům, mé rodině a přátelům, kteří mě v průběhu studia podporovali. V neposlední řadě bych chtěl poděkovat všem testovaným subjektům, kteří se zúčastnili měření a katedře Technologické zařízení staveb za poskytnutí biometrických systémů, měřících zařízení a technického zázemí pro celé měření.

# Abstrakt

Diplomová práce se zabývá spolehlivostí biometrické identifikace osob na základě rozpoznávání obličeje uživatele při užití, či neužití dodatečného přísvitu. Diplomová práce je rozdělena do dvou hlavních částí – teoretická a praktická.

Teoretická část práce je následně rozdělena na část věnovanou biometrickým algoritmům, metodám a přístupům, které se využívají k identifikaci tváří a na část věnovanou přísvitům – ve viditelném spektru a infračerveném spektru. V této části jsou shrnuty také výhody, nevýhody a zásady plynoucí z použití jednotlivých přísvitů a jednotlivých metod, případně obecných přístupů k biometrii tváří. Teoretická část práce zahrnuje popis přístupu určení spolehlivosti a chybovosti jednotlivých systémů.

Praktická část práce je věnována testování čtyř nejpoužívanějších biometrických čteček obličejů v ČR bez použití dodatečného přísvitu a s použitím dodatečného přísvitu. Dodatečný přísvit byl realizován prostřednictvím RGB LED přísvitu s regulací a měření byla realizována v rozdílných světelných podmínkách – odlišných barevných spektrech přísvitu. Byl stanoven výchozí čas přijatelné doby trvání identifikace obličeje a na tomto základě bylo prováděno měření spolehlivosti čteček. Z měření byly stanoveny závěry, zda je dodatečný přísvit u testovaných biometrických čteček přínosem či nikoliv a zda je ovlivněna spolehlivost těchto čteček a čas identifikace, případně v jaké míře a jaká barevná spektra přísvitu jsou nejpříjemnější z hlediska vjemu lidského oka.

**Klíčová slova:** identifikace, přísvit, biometrie, sken tváře

# Abstract

The thesis focuses on reliability of biometric identification of people based on the user's facial recognition when using or not using additional external illumination. It is divided into two main parts - theoretical and practical.

The theoretical part is divided into two sections, the first of which is dedicated to biometric algorithms, methods and approaches used for identifying faces, and the second to additional types of illumination - in the visible spectrum and in the infrared, invisible spectrum. This part also summarizes the advantages, disadvantages and the principles deriving from the use of individual illuminators and methods, alternatively general approaches to biometry of faces. The theoretical part also includes a description of the most common approaches used to determine reliability and error rates of individual systems.

The practical part focuses on testing four most frequently used biometric systems in the Czech Republic, with and without additional external illumination. The additional illumination was realized using RGB LED strips. The illumination as well as the amount and the colour of the visible emitted light were regulated using a remote control. The testing and the measuring process were conducted in different lighting conditions – different lighting spectrums (different colours of visible spectrums - RGB and white spectrum). Acceptable length of time for face recognition was determined, based on which the reliability of the biometric systems was measured in different visible spectrum conditions. The issues that can be addressed from the measurements are whether the additional illuminators used with the tested biometric systems are beneficial or not, whether or to what extent something influences the reliability of these biometric systems and the identification time, and what colour spectrum of illuminators is most comfortable to the human eye.

The conclusion of the thesis contains calculations of expected error rates in differently coloured spectrums, of the impact on the duration of the identification process and also a summary of the benefits of these illuminators. Evaluation of differently coloured spectrums and recommendations are also included.

**Key words:** identification, illumination, biometry, face scan

# Obsah

1 Úvod.....	1
2 Cíl práce .....	3
3 Metodika práce.....	4
4. Přehled řešené problematiky .....	5
4.1 Biometrie .....	5
4.2 Princip biometrické technologie .....	5
4.2.1 Identifikace .....	7
4.2.2 Verifikace .....	8
4.3 Spolehlivost a chybovost biometrických metod .....	9
4.4 2D/3D biometrický přístup k rozpoznávání tváří .....	11
4.5 Identifikace osoby na základě fotografického portrétu.....	13
4.5.1 Analyticko-statistická metoda .....	14
4.5.2 Grafická metoda .....	15
4.6 Automatizace obličejové biometrie .....	16
4.6.1 Metoda Eigenface.....	17
4.6.2 Metoda Eigenhead.....	19
4.6.3 Metoda neuronových sítí – detekce obličeje .....	20
4.6.4 Metoda neuronových sítí – rozpoznávání obličeje .....	21
4.6.5 Metoda distribuce odstínu šedi – detekce obličeje .....	22
4.6.6 Metoda distribuce odstínu šedi – rozpoznávání obličeje.....	23
4.6.7 Metoda optických toků – detekce obličeje .....	23
4.6.8 Metoda optických toků – rozpoznávání obličeje.....	24
4.6.9 Metoda rozpoznání rysů, kontur – detekce obličeje .....	25
4.6.10 Metoda distribuce barev obličeje – rozpoznání obličeje .....	26
4.6.11 Metoda založená na symetrii – detekce obličeje .....	27
4.6.12 Metoda založená na markantech a geometrických tvarech – rozpoznávání obličeje ...	27



4.6.13 Metoda deformačních modelů – rozpoznávání obličeje.....	28
4.7 Přisvit v biometrii a využívaná spektra.....	29
4.7.1 Biometrie a viditelné spektrum, přisvit .....	30
4.7.2 Zdroje okolního světla.....	31
4.7.3 Bílý LED přisvit.....	33
4.7.4 Nevýhody využití viditelného spektra přisvitu.....	34
4.7.5 Ideální nasvícení subjektu .....	35
4.7.6 Zásady při realizaci viditelného přisvícení.....	36
4.8 Biometrie v infračerveném spektru, přisvitu .....	37
4.8.1 Biometrie a infračervené spektrum, přisvit .....	39
4.8.2 Termografie .....	40
4.8.3 Zásady při realizaci infračerveného přisvícení.....	41
4.8.4 Zdroje infračerveného přisvitu .....	42
4.8.5 Výhody využití infračerveného spektra přisvitu .....	43
4.8.6 Experimentální metoda rozpoznání lidské kůže v IR spektru .....	43
5 Praktická část práce.....	45
5.1 Použitá zařízení.....	45
5.1.1 Čtečka č.1 – iFace 302 .....	46
5.1.2 Čtečka č.2 – Multibio 700 .....	47
5.1.3 Čtečka č.3 – AccuFace EFR-T1 .....	48
5.1.4 Čtečka č.4 – Aktion AFT-500 .....	49
5.1.5 Luxmetr – CEM-DT 8809A .....	50
5.1.6 Přisvit – LED RGB pásek .....	51
5.2 Postup měření.....	52
5.2.1 Vyhodnocovací stavy .....	56
5.2.2 Bodový souhrn jednotlivých kroků měření .....	57
5.2.3 Registrace nových uživatelů u čtečky iFace 302 a Multibio 700 .....	57
5.2.4 Registrace nových uživatelů u čtečky AccuFace EFR-T1 .....	58

5.2.5 Registrace nových uživatelů u čtečky Aktion AFT-500 .....	59
5.3 Měřené hodnoty – příklad záznamu z měření.....	60
6 Výsledky .....	63
6.1 Naměřené hodnoty osvitů jednotlivých barevných přísvitů .....	63
6.2 Test rozpoznání subjektů po měření po 3 letech na starších čtečkách (č.1 a č.2).....	65
6.3 Naměřené hodnoty doby identifikace .....	66
6.4 Naměřené hodnoty spolehlivosti (FRR) .....	69
7 Diskuse.....	75
8 Závěr .....	77
Reference .....	81
Seznam příloh .....	86
Seznam obrázků .....	87
Seznam tabulek .....	89
Seznam grafů.....	90
Přílohy.....	I

# 1 Úvod

Spolehlivá a korektní identifikace osob je velmi obtížnou disciplínou a je rozvíjena již od pradávných dob, kdy nebyly dostupné nyní lidem známé automatizační prostředky, jako počítače či jiná elektronická zařízení. Identifikace osob byla vždy úzce spojována s bezpečností. Již v prvopočátcích lidstva byli lidé nuceni jednoznačně odlišit přítele od nepřítele ve vlastním zájmu přežití. Tento aspekt rozpoznávání lidských tváří je nazýván vizuální identifikace a je rozvíjen u lidí již od prvních dnů od narození, kdy lidé ve stádiu nemluvněte již po prvotních dnech jsou schopni jednoznačně odlišovat tváře, ačkoliv bez bližšího kontextu. Ve standardních podmínkách rozlišují osobu blízkou, zejména matku bezpečně jako první, jelikož jsou v úzkém kontaktu již od narození.

Metody identifikace se historicky vyvíjely od prvotních primitivních podob po stále sofistikovanější řešení. Přístupy k identifikaci, jako takové se měnily postupem času od přístupů založených na vlastnictví (jména a příjmení, záznamů v matrice, osobní doklady, identifikační karty, čipy, biočipy atd.), znalostí (hesla – statická a dynamická, kódy, znalosti přezdívky, rodinného stavu, rodinné historie, rodinné skladby atd.) a následně na unikátních, do jisté míry neměnných biometrických charakteristikách (otisk prstu, sken tváře, sken sítnice, geometrie ruky, DNA, záznam hlasu atd.).

Biometrická identifikace poskytuje mnoho výhod, kterými ostatní přístupy nedisponují a je možné také tento biometrický přístup kombinovat s jinými přístupy založenými na vlastnictví/znalosti k ještě většímu stupni zabezpečení. Mezi největší výhody biometrie do jisté míry patří zejména nepřenositelnost, neodcizitelnost, pohotovost (vždy je k dispozici, nelze ji zapomenout), rychlost identifikace, přirozenost a automatizovatelnost.

S vývojem a rozvojem počítačů a elektroniky obecně se neustále snižují výrobní ceny elektronických součástí a biometrické systémy se stávají stále dostupnější, zejména z hlediska finančního. Biometrické identifikační systémy se používají stále více v běžných zařízeních (mobilní telefony, počítače), v domácnostech, v menších i větších firmách, korporacích a nejsou již jen doménou armády, zabezpečení jaderných zbraní, ostře střeženého finančního sektoru (bankovníctví), letištních areálů, stadionů, recepcí významných míst či jiných významně střežených míst a lokalit.

Nejpoužívanější biometrickou identifikací je daktyloskopie (rozpoznávání otisku prstů) a následně biometrie na základě rozpoznávání obličejů. Biometrická identifikace má za cíl zajistit vysokou míru bezpečnosti a zároveň usnadnit proces této identifikace, případně zpříjemnit tento proces uživatelům, jak jen je to možné.

Z tohoto hlediska se již od šedesátých let 20. století zdokonalují algoritmy a metody na rozpoznávání lidských tváří. Mění se obecné přístupy 2D/3D identifikace tváří, mění se jednotlivé algoritmy, založené na metodách analyticko-statistických či grafických. Využívají se jiná elektromagnetická spektra, ve kterých tyto čtečky následně fungují – viditelné či neviditelné infračervené spektrum, využívají se různé přísvity.

Myšlenka vysoké bezpečnosti a usnadnění přístupu do objektů, případně obecná identifikace s využitím této technologie je velmi slibná, ale jaké je reálné fungování těchto čteček v praxi?

V dnešním moderním uspěchaném světě je důraz kladen také na rychlost identifikace. V případě nedostatečné spolehlivosti, případně rychlosti těchto čteček může docházet ke značné frustraci uživatelů, zdiskreditování věrohodnosti bezpečnostního systému, zpomalení procesu identifikace mající za následek v určitých případech vzrůst ztrátovosti, případně nekorektního vpuštění nežádoucí osoby do objektu představující hrozbu.

Samozřejmě se od sebe liší jednotlivá řešení v závislosti na místě užití, stupni požadované bezpečnosti, cenové nákladnosti a případně utajení, ale jak si stojí dnešní nejpoužívanější biometrické čtečky založené na rozpoznávání obličejů v ČR, v oblasti běžných komerčních biometrických čteček pro firmy a domácnosti? Jakou spolehlivostí disponují tyto čtečky a jak dlouho trvá samotný proces identifikace bez přísvitu a s přísvitem? Je navržené originální řešení od výrobce s použitým přísvitem dostačující? Má dodatečný přísvit u těchto čtyř zvolených čteček smysl, případně jaký přísvit, jaké barevné spektrum je nejvhodnější pro zlepšení těchto čteček? Dochází ke zlepšení/zhoršení spolehlivosti či identifikačních časů na těchto čtečkách při užití jednotlivých přísvitů? Všemi těmito otázkami se zabývá praktická část této diplomové práce.

## 2 Cíl práce

Cílem diplomové práce je vytvořit přehled jednotlivých přístupů, metod a algoritmů v problematice biometrického rozpoznávání tváří a následně zhodnotit výhody, nevýhody obecné biometrie obličejů i jednotlivých přístupů. Práce je zaměřena na využití přísvitů u těchto čteček.

V diplomové práci bude vytvořen přehled jednotlivých druhů přísvitů, které se využívají, s ohledem na využívané elektromagnetické spektrum – viditelné a neviditelné infračervené. V práci budou shrnuty výhody, nevýhody jednotlivých přísvitů, jejich způsoby využití a zásady při realizaci přísvitu jako takového.

V praktické části bude empiricky ověřeno, zda testované biometrické čtečky – nejpoužívanější čtečky v ČR, mají dostatečný přísvit od výrobce, jak jsou tyto čtečky spolehlivé v praxi při měření (bez přísvitu/s přísvitem) a zda má vliv použití dodatečného přísvitu v různých barevných spektrech na spolehlivost těchto čteček, případně rychlost vyhodnocení těchto čteček.

Na tomto základě budou stanoveny závěry, zda originální přísvit od výrobce je dostatečný, případně k jakému ovlivnění dochází při použití dodatečného externího přísvitu a případně jakého barevného spektra.

### **Shrnutí cílů:**

- vytvořit přehled přístupů, metod a algoritmů biometrie obličejů
- vytvořit přehled používaných přísvitů v el.mg. spektru – viditelné, neviditelné infračervené
- vytvořit přehled výhod, nevýhod a zásad při realizaci přísvitu
- zjistit spolehlivost čtyř nejpoužívanějších biometrických čteček na trhu v ČR, bez dodatečného přísvitu
- zjistit spolehlivost čteček s dodatečným přísvitem v odlišných barevných spektrech (použitá spektra – R (červené), G (zelené), B (modré) a bílé)
- stanovit přínosy jednotlivých přísvitů v odlišných barevných spektrech (spolehlivost, přínos v rychlosti vyhodnocení identifikace uživatele, příjemnost osvětlení pro lidské oko)

### 3 Metodika práce

Teoretická část diplomové práce bude zpracována převážně z ověřených vědeckých článků, dostupných skript, internetových publikací a knižní literatury. Teoretická část práce bude následně rozdělena do dvou dílčích částí. První část teoretické části se bude zabývat obecným pojetím obličejové biometrie, přístupy a principy, spolehlivostí této technologie a především metodami strojového rozpoznávání obličejů - biometrickými systémy včetně jejich výhod a nevýhod. Druhá část teoretické části se bude zabývat jednotlivými přísvity a spektry ve kterém působí, jejich rozdělením, výhodami a nevýhodami jednotlivých typů přísvitů, jejich zásadami při realizaci přísvitu a jednotlivými zdroji těchto přísvitů.

V praktické části bude provedeno měření na testovacích subjektech z areálu ČZU v Praze. Toto měření bude probíhat v laboratorních podmínkách, které bude blíže specifikováno v praktické části diplomové práce. Toto měření bude probíhat na čtyřech nejpoužívanějších biometrických čtečkách v ČR. Při měření bude nejdříve změřeno přirozené světlo luxmetrem a následně případně zregulováno okolní světlo v místnosti na stanovenou úroveň. Následně budou proměřeny jednotlivé přísvity z hlediska podávaného osvětlení v jednotlivých barevných spektrech. Pro testování bude vyhrazena jednotná, časová hranice doby identifikace, pro jeden identifikační pokus. Samotné testování bude rozděleno do pěti měření, pro jednotlivé přísvity. Prvotní měření bude realizováno bez použití dodatečného přísvitu, ostatní měření budou realizována s dodatečnými přísvity v jednotlivých barevných spektrech (červené, zelené, modré a bílé). V každém spektru se bude měření opakovat 10x. Při měření budou zaznamenávány jednotlivé časy identifikace, případná falešná odmítnutí či falešná přijetí.

Z naměřených hodnot bude provedena analýza dat, dopočítání hodnoty FRR (false rejection rate, míra falešného odmítnutí), dopočítání jednotlivých průměrných časů u jednotlivých čteček v rozdílných barevných spektrech přísvitu a také dopočítání dílčích případných zlepšení či zhoršení vlivem těchto přísvitů. Na základě této analýzy bude provedeno vyhodnocení a budou stanoveny závěry, zda dodatečný přísvit má smysl, zda přináší výhody či nevýhody, případně jaké barevné spektrum je nejpřínosnější. Z hlediska vjemu lidského oka bude zhodnoceno také nejvhodnější barevné spektrum. V neposlední řadě bude provedeno doporučení, pro jaké situace je vhodné využít dodatečný přísvit.

## 4. Přehled řešené problematiky

V této kapitole se nachází celý teoretický přehled řešené problematiky. Tato kapitola je rozdělena do dvou částí. První část se věnuje biometrii obličeje jako takové, zejména metodám, algoritmům a jednotlivým přístupům k identifikaci a verifikaci tváří. Tato část zahrnuje také teoretický způsob určení spolehlivosti biometrických čteček. Druhá část se věnuje konkrétním přísvitům, jejich výhodám, nevýhodám, způsobům užití, zdrojům těchto přísvitů a také zásadám, které je nutné dodržovat při realizaci těchto přísvitů.

### 4.1 Biometrie

Biometrie je automatizovaná metoda ověření identity subjektu (autentizace), založená na principech rozpoznávání unikátních biologických charakteristik (markantů) zkoumaného živého subjektu – zejména osoby. Filosofie biometrické metody vychází z myšlenky jedinečnosti a neměnnosti zkoumaného subjektu jak z hlediska anatomického, fyziologického, ale také i behaviorálního. Biometrie zahrnuje soubor vědních poznatků, založených na statistickém a analytickém přístupu, jejichž hlavním cílem je jednoznačné identifikování či verifikování zkoumaného subjektu. Tento termín představuje mimo jiné měřitelné biometrické charakteristiky (obrazce, data atd.) zkoumaného subjektu. Tyto charakteristiky se získávají snímáním prostřednictvím biometrických systémů, následně se zpracovávají, vyhodnocují a uchovávají v procesu identifikace a verifikace. [1] [2] [3] [4]

**Anatomicko-fyziologické biometrické charakteristiky** jsou snímány a následně užívány k identifikaci a verifikaci osob biometrickými systémy. Tento druh systémů využívá exaktní, vědecké poznatky. Tyto charakteristiky jsou unikátní a časově stálé. Nejčastěji používané unikátní biometrické charakteristiky jsou charakteristiky otisku prstů, oční duhovky, oční sítnice, tváří či DNA. [2]

**Behaviorální biometrické charakteristiky** jsou získávány prostřednictvím nabytých, vědeckých znalostí o hlasu, pohybu těla či schopnostech a způsobech psaní. Tyto charakteristiky jsou také unikátní a mohou být časově nestálé. [2]

### 4.2 Princip biometrické technologie

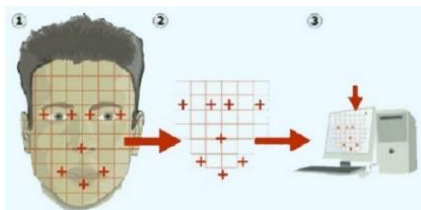
Obecný princip porovnávání a následující identifikace, případně verifikace osoby na základě biometrických charakteristik je u všech typů biometrických metod totožný, případně liší se pouze v drobných detailech. Celý proces se skládá ze čtyř dílčích úkonů, kterými jsou – biometrický vzorek, biometrické charakteristiky, biometrické markanty a biometrická šablona. Všechny kroky jsou zobrazeny na obr. 4. [2] [5]

**Biometrický vzorek** je svým způsobem jakýmsi vstupem pro celý biometrický proces. Jedná se o vstup, který je odebrán, sejmuto, odměřen či jinak získán ze zkoumaného subjektu a následně je využíván jako testovací vzorek. Vzorkem se rozumí biometrická hodnota, data použitelná pro konkrétní biometrický systém - v případě biometrického systému rozpoznávající osoby na základě tváře je vstupem fotografie nebo video. Na obr. 2 je biometrický vzorek znázorněn jako část obrázku s označením č.1. [2] [5]

**Biometrická charakteristika** vychází z předchozího kroku, biometrického vzorku, ze kterého různými metodami, dle konkrétního systému, získává měřitelné či jinak exaktně získatelné údaje. Z těchto naměřených údajů vytváří výsledný ucelený popis vstupu v takových hodnotách, které jsou použitelné, kompatibilní pro konkrétní identifikační algoritmus daného biometrického systému. Obsahuje všechny důležité charakteristické rysy tváře, ale nemusí nutně všechny být upotřebeny v procesu rozpoznávání tváře. Na obr. 2 je biometrická charakteristika znázorněna jako část obrázku s označením č.2. [2] [5]

**Biometrické markanty** vychází opět z předchozího kroku, kdy se z biometrické charakteristiky vybírají pouze ty charakteristiky, hodnoty, které budou efektivně použitelné v budoucím procesu rozpoznávání tváře. Těmito markanty v oblasti tváře jsou například body vnitřních a vnějších koutků oka, vnější horizontální body rtů či bod špičky nosu. Na obr. 2. jsou biometrické markanty znázorněny jako část obrázku s označením č.3. Na obr. 1 jsou znázorněny základní biometrické markanty tváře. Způsob výběru a hustota markantů se může diametrálně lišit s rozdílnou technologií biometrického systému. [2] [5]

*Obrázek 1 - Základní biometrické markanty tváře*



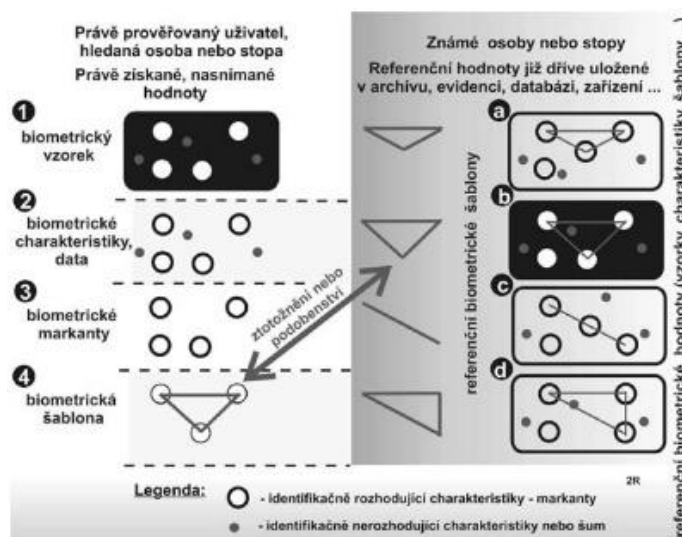
[5]

**Biometrická šablona** vychází ze všech předchozích kroků a představuje finální výstup při tvorbě biometrické šablony, která bude následně sloužit pro plně automatizované rozpoznávání tváří při procesech identifikace a verifikace. Ze všech podkladů uskutečněných v předchozích krocích se provede finální výběr markantů, potřebných k úspěšné identifikaci tváře, následně se vykoná optimalizace a vytvoření samotné šablony. Tato šablona je následně uložena do databáze. Při vytváření šablony je také snaha o co nejmenší velikost celkové šablony z důvodu úspory místa a zároveň zajištění co možná nejkratší doby načítání šablony.



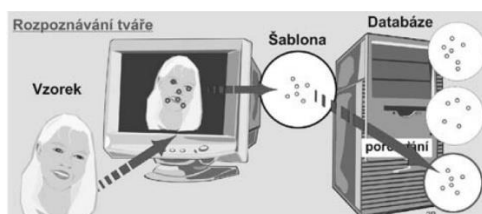
Z důvodu ochrany osobních údajů osoby nejsou většinou uchovávány originální fotografie, videa, které sloužily jako vstupní biometrické vzorky. Na obr. 2 je biometrická šablona znázorněna jako část obrázku s označením č.4. Na obr. 3 je zachyceno zjednodušené znázornění procesu vytvoření šablony tváře. [2] [5]

Obrázek 2 - Princip biometrického porovnávání



[2]

Obrázek 3 - Proces vytvoření šablony tváře



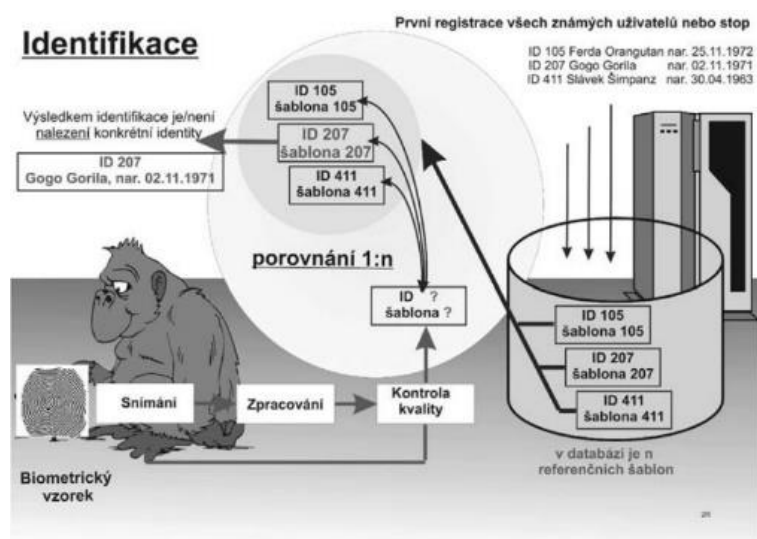
[2]

## 4.2.1 Identifikace

Proces biometrické identifikace lze vystihnout termínem ztotožnění. Identifikace se rozlišuje na pozitivní a negativní. Pozitivní identifikace má za cíl potvrdit, že oprávněná osoba je opravdu osobou, za kterou se vydává. Princip spočívá v tom, že pokud byla v databázi nalezena shoda se zkoumaným vzorkem, je osoba identifikována pozitivně a je jí následně povolen přístup. Pokud nebyla nalezena shoda v databázi, je přístup zamítnut. Negativní identifikace má za cíl dokázat, že neoprávněná osoba není tou osobou, za kterou se vydává. Princip spočívá v tom, že jestliže byla v databázi nalezena shoda se zkoumaným vzorkem, je osoba identifikována negativně a je jí následně zamítnut přístup. Pokud nebyla nalezena shoda v databázi, je přístup povolen. [2]

Jedná se o proces porovnávání šablon, ve kterém dochází k porovnávání přístupem 1:N. Dochází k porovnávání jednoho konkrétního, nasnímaného biometrického vzorku s celou databází vzorků. Porovnávání se provádí na úrovni šablon. Identifikace má za cíl zjistit, kterému vzorku v databázi odpovídá vzorek nově nasnímaný. Identifikaci je možné vyjádřit otázkou „Co je to za osobu?“. Celý proces identifikace je zobrazen na obr. 4. Nejdříve se provádí snímání biometrického vzorku, následně dojde ke zpracování vzorku (vytvoření šablony), následně dojde ke kontrole kvality nasnímaného vzorku a poté dojde k porovnání s ostatními šablonami (množství n) v databázi na základě kterého dojde k vyvození závěru/rozhodnutí. [2]

Obrázek 4 - Proces identifikace



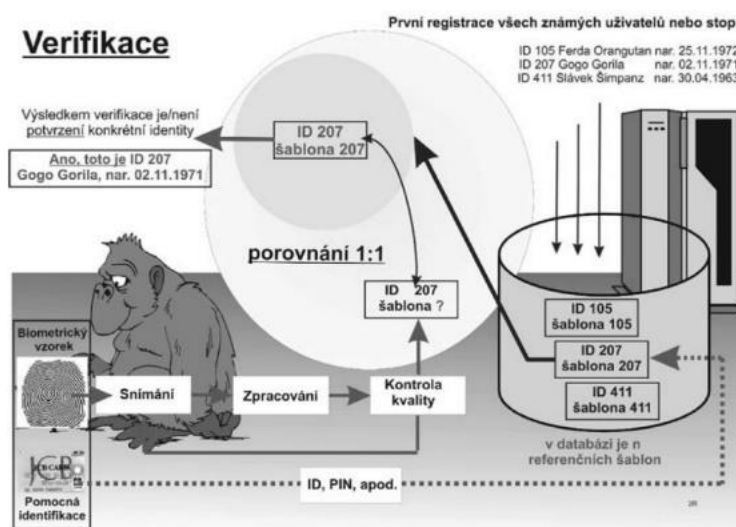
[2]

## 4.2.2 Verifikace

Proces biometrické verifikace je odvozen od procesu identifikace. Verifikace má za cíl potvrdit, zda aktuálně nasnímaný vzorek je shodný s jedním, konkrétním vzorkem uloženým v databázi, údajně patřící zkoumanému subjektu. Verifikaci je možné vyjádřit otázkou „Je tato osoba opravdu osobou, za kterou se vydává?“. Tento proces je velmi podobný klasické identifikaci, avšak s tím rozdílem, že dochází k porovnávání šablon pouze přístupem 1:1. [2]

Tento proces je výrazně rychlejší, méně náročnější na celkové hardwarové vybavení systému a celkově jednodušší. Celý proces verifikace je zobrazen na obr. 5. Nejdříve se provádí snímání biometrického vzorku, následně dojde ke zpracování vzorku (vytvoření šablony), poté dojde ke kontrole kvality nasnímaného vzorku a ve finále dojde k porovnání se šablonou (údajně patřící testovanému subjektu) v databázi, které dojde k vyvození závěru/rozhodnutí. [2]

Obrázek 5 - Proces verifikace



[2]

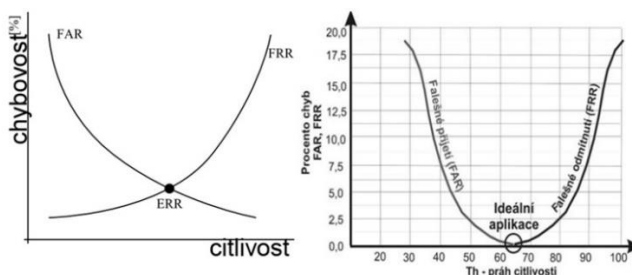
### 4.3 Spolehlivost a chybovost biometrických metod

Velmi důležitým aspektem celého biometrického systému bývá spolehlivost systému a jeho chybovost – která je velmi důležitá v procesu rozhodování o typu nasazení a aplikaci systému. Mezi základní chybové parametry celého systému se řadí míra chybného přijetí (FAR – false acceptance rate), míra chybného odmítnutí (FRR – false rejection rate). Dále stav, ve kterém jsou hodnoty FAR a FRR vyrovnané – EER (equal error rate), chybovost zavádění referenční šablony subjektu do systému (FTE – failure to enroll), opakovaná chybovost získání korektní, použitelné šablony (FTA – failure to acquire) a chyby špatného ztotožnění (FM – false match) a špatného neztotožnění (FNM – false not match). Na základě chyb FAR a FRR se následně také vytváří aplikační křivka, charakteristika ROC – receiver operating characteristics, která se využívá v procesu rozhodování o aplikaci systému. [2] [6]

Důležitým parametrem souvisejícím se spolehlivostí je parametr prahu citlivosti – Th (threshold). Pakliže oprávněný či neoprávněný uživatel dosahuje míry ztotožnění větší, než je práh citlivosti, je akceptován, v opačném případě odmítnut. Mohou tedy nastat 4 stavy – oprávněný uživatel přijat, neoprávněný uživatel přijat (chyba systému, případně obelstění systému), oprávněný uživatel odmítnut (chyba systému), neoprávněný uživatel odmítnut. Z těchto stavů jsou vyhovující samozřejmě jen dva stavy, a to přijetí oprávněného uživatele a odmítnutí neoprávněného uživatele. Při každém procesu autentizace dochází ke snímání originálního biometrického vzorku a následného porovnání s referenční šablonou. Naměření a následné ztotožnění šablon se vždy drobně liší. Nedochozí téměř nikdy k absolutnímu ztotožnění. Výsledné ztotožnění je následně vyjádřeno v hodnotě míry ztotožnění, případně skóre. [2] [6]

Parametry FAR a FRR nelze spočítat, tyto parametry lze získat jen exaktním měřením systému, ozkoušením a následným využitím statistických metod. Dle způsobu využití, aplikace systému se upravují a nastavují tyto hodnoty, aby vytvořily vhodný funkční kompromis pro danou problematiku. Zmenšení hodnoty FAR vyvolá zvětšení hodnoty FRR, a naopak zvětšení hodnoty FAR vyvolá zmenšení hodnoty FRR. Průsečík, ve kterém se obě závislosti setkávají tvoří bod EER, v tomto bodu je FAR=FRR. V ideálním případě by platila rovnost FAR=FRR=0. Oba tyto případy jsou zachyceny na obr. 6. [2] [6]

Obrázek 6 - Charakteristiky FAR, FRR, ERR a ideální ERR



[7] [2]

**Míra chybného přijetí (FAR – false acceptance rate)** – požadavkem je, aby systém neakceptoval neoprávněné osoby. Hodnota FAR je vyjádřena následujícím vztahem.

$$FAR = \frac{N_{FA}}{N_{IIA}} = \frac{N_{FA}}{N_{IVA}}$$

$N_{FA}$  = počet chybných přijetí

$N_{IIA}$  = počet pokusů neoprávněných osob o identifikaci

$N_{IVA}$  = počet pokusů neoprávněných osob o verifikaci

[2]

**Míra chybného odmítnutí (FRR – false rejection rate)** – požadavkem je, aby systém korektně akceptoval oprávněné osoby. Hodnota FRR je vyjádřena následujícím vztahem.

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}}$$

$N_{FR}$  = počet chybných odmítnutí

$N_{EIA}$  = počet pokusů oprávněných osob o identifikaci

$N_{EVA}$  = počet pokusů oprávněných osob o verifikaci

[2]

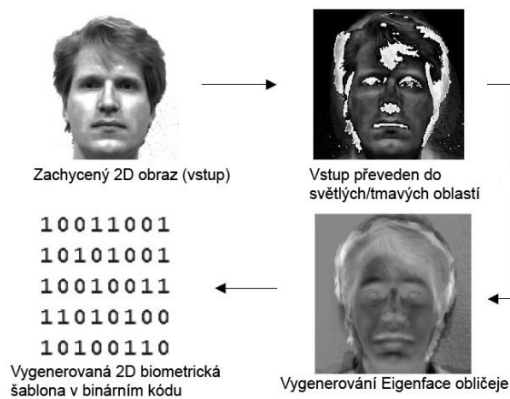
## 4.4 2D/3D biometrický přístup k rozpoznávání tváří

Existují dva obecné přístupy k biometrii tváří, a to dvourozměrný-2D a třírozměrný-3D. Oba přístupy využívají jiný způsob počítačového vidění, využívají jiné metodiky, logiky přístupu a algoritmů. [8]

**Dvourozměrný přístup** zpracování tváří bývá obhajován tím, že tento přístup je přirozený snímacím kamerám a očím, a tím je také lehce využitelný. Z finančního hlediska je přístupnější a také přizpůsobitelnější pro další zautomatizování biometrického procesu. [8]

**Obecný proces 2D zpracování tváří** je znázorněn na obr. 7. Nejdříve dochází k nasnímání biometrického vzorku tváře, následně ke konverzi na tmavá a světlá místa (normalizaci), poté se vygeneruje průměrný obraz tváře pomocí metody Eigenface a ve finálním kroku se provede vygenerování 2D šablony obličeje. [8]

Obrázek 7 - Obecný přístup zpracování tváří 2D technikou



[8]

**Dvourozměrné techniky** biometrického zpracování obličejů bývají velmi často ovlivňovány okolním světlem, které mohou identifikaci napomáhat, ale také škodit. V případě okolního světla se zdroje světla obecně rozlišují na přirozené a umělé. Škodit může jak přebytek světla, tak nedostatek světla a také přítomnost stínů. Z tohoto důvodu se využívají různé snímací kamery, které jsou závislé na rozdílném způsobu přisvícení biometrických čteček, okolním světlem ovlivnitelné i okolním světlem do jisté míry neovlivnitelné (IR – infračervené spektrum). Dvourozměrné techniky mohou být ovlivnitelné také znečištěním obličeje, případně přítomností velkého množství kosmetiky na obličeji. Výsledek identifikace také může negativně ovlivňovat případná póza, výraz obličeje a vzdálenost zkoumaného subjektu. Při dvourozměrném rozpoznávání tváří je potřebné zajistit dostatečně kvalitní snímek tváře a tento snímek musí být z většiny případů sejmut z předního pohledu (portrét). [8]

U některých méně sofistikovaných dvourozměrných metod zpracování obličejů byly zaznamenány případy obelstění systému prostřednictvím vytištěného portréту osoby na papíru. Všechny klady a zápory dvourozměrné technologie jsou zformulovány do ucelené tabulky 1. [8]

Tabulka 1 - Klady/Zápory 2D technologie zpracování tváři

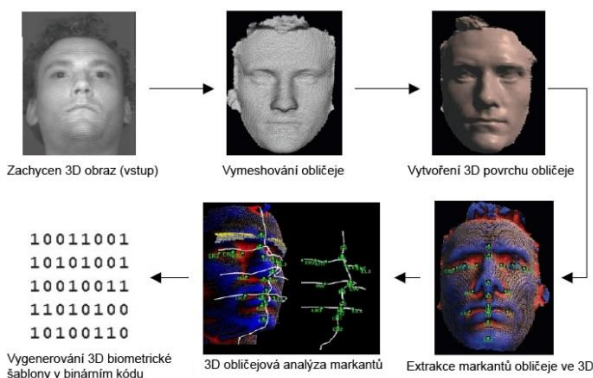
Klady +	Zápory -
Rychlé	Citlivé na světlo a stíny - dle použité technologie
Jednoduché	Citlivé na pózu, výrazy a vzdálenost obličeje
Obecně levnější	Citlivé na přítomnost znečištění/kosmetiky na obličeji
Malá velikost šablony	2D šablona – málo informací
Nenáročnost zpracování	

[8]

**Třírozměrný přístup** zpracování tváři bývá obhajován tím, že tento přístup obsahuje mnohem více informací, než klasické dvourozměrné zpracování, a tím pádem mnohem přesněji reprezentuje běžný přístup vnímání okolního světa. Tento přístup je ale obecně považován za obtížnější, finančně méně dostupný. Proces zautomatizování biometrického zpracování bývá také z pravidla obtížnější. [8]

**Obecný proces 3D zpracování tváři** je znázorněn na obr. 8. Nejdříve dochází k nasnímání biometrického vzorku tváře, následně dochází k 3D meshování (vytvoření síťové podoby obličeje), poté k vytvoření samotného povrchu obličeje a z tohoto povrchu se následně extrahují 3D rysy obličeje. V posledním kroku se provede analýza vyextrahovaných markantů a na tomto základě je vytvořena 3D šablona obličeje. [8]

Obrázek 8 - Obecný přístup zpracování tváři 3D technikou



[8]

**Třírozměrné techniky** biometrického zpracování obličejů využívají metodiku zpracování třírozměrné geometrie obličeje. Technika zahrnuje zkoumání hloubky rysů obličeje, jednotlivých obrysů, kontur a také vzdáleností jednotlivých rysů. Tato technika využívá pokřivení zkoumajícího paprsku na základě geometrie obličeje. Z principu třírozměrného přístupu rozpoznávání tváří se výhradně využívají techniky nezávislé na okolním světle. Při zkoumání obličeje dochází k vytvoření 3D meshe (třírozměrné sítě obličeje), který reprezentuje zkoumanou tvář a je následně využíván jako podklad k vytvoření šablony. Všechny klady a zápory třírozměrné technologie jsou zformulovány do ucelené tabulky 2. [8]

Tabulka 2 - Klady/Zápory 3D technologie zpracování tváří

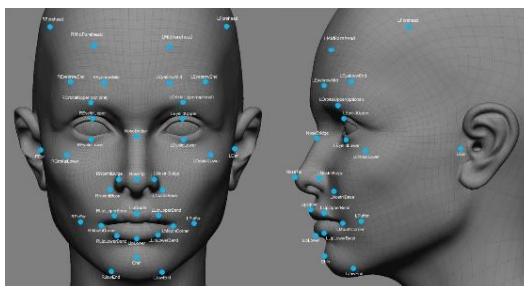
Klady +	Zápory -
Nezávislé na póze, výrazech v obličejí	Pomalejší
Méně závislé na znečištění/kosmetice v obličejí	Obtížnější
Odolné vůči okolnímu světlu	Obecně nákladnější
Odolné vůči natočení až do 45°	Větší velikost šablony (3D mesh)
Lepší rozhodovací schopnost	Náročnost zpracování
3D šablona – hodně informací	

[8]

## 4.5 Identifikace osoby na základě fotografického portréту

Biometrické systémy s rozpoznáváním na základě obličeje byly vyvíjeny již od 60 let 20. století, zejména sovětské techniky byly ve své době velmi pokrokové. Celý proces vývoje se zabýval na počátku nejdříve tím, jak vlastně funguje takový proces rozpoznávání obličejů u lidí, jako takových, aby bylo možné tyto postupy následně uměle reprodukovat, případně zautomatizovat v elektronické digitální podobě. Vědci zjistili, že lidský mozek rozeznává od sebe jednotlivé obličeje na základě takzvaných markantních bodů, ve zkratce „markantů“, které jsou do jisté míry jedinečné pro každou osobu. Samozřejmě každý plně vyvinutý zdravý jedinec vlastní z makro hlediska stejné identifikační prvky - oči, uši, nos, ústa, lící kosti a jiné důležité identifikátory. Z makro hlediska by šlo usuzovat, že lidé jsou stejní. Z mikro hlediska tomu tak ve skutečnosti není a biometrie využívá drobných detailů, ve kterých se lidé odlišují. Každá osoba má odlišné tvary, velikosti, zaoblení, hloubku či odstín jednotlivých identifikačních markantů. Nejdůležitější rozeznávací markanty obličeje jsou znázorněny na obr. 9, kterými jsou například – vnitřní a vnější koutky oka, body očních víček, vnější body rtů, body špičky nosu či bodu, kde nos přechází v čelo, body obočí, body lících kostí případně spodní body čelisti. [2]

Obrázek 9 - Markanty na obličejí



[9]

Na základě těchto poznatků, které jsou mimo jiné exaktně vědecky popsatelné a vyjádřitelné byly vyvíjeny metody, kterými by bylo možné identifikovat osoby na základě fotografického portréту. Těmito metodami jsou analyticko-statistická metoda a grafická metoda. [2]

#### 4.5.1 Analyticko-statistická metoda

Metoda analyticko-statistická je založena na výpočtech vzdáleností mezi jednotlivými markantními body, jejich prostorovou transformací, případně deformací. V průběhu času bylo zjištěno, že k identifikaci osoby touto metodou dostačuje 12 bodů, rysů tváře. Na základě těchto markantů se následně vytvoří úsečky, které ještě lépe popisují a vystihují identitu lidské tváře. Tyto markanty a úsečky je možné názorně vidět na obr. 10 a). [2]

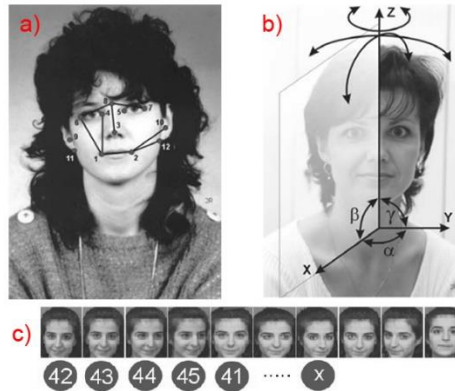
Tato metoda je závislá na preciznosti a konzistentnosti snímání jednotlivých fotografií, portrétů osob. Při této metodě je nutné zachovat co možná nejvíce totožné podmínky snímání tváří, zejména úhlu natočení vzhledem k snímacímu zařízení, jelikož se změnou vzdálenosti, natočením či jiným vychýlením z požadované polohy dochází k prostorové transformaci identifikačních bodů. Natačení těžiště hlavy je možné ve třech osách – x, y, z a následně lze vyjádřit ono natočení v úhlech (využití souřadnicového systému). Způsoby natočení těžiště hlavy je možné názorně vidět na obr. 10 b). Aby bylo možné použít tuto metodu k praktické identifikaci, je potřebné znát závislost velikosti úsečky mezi markanty na změně úhlu natočení. Z tohoto hlediska se jednotlivé snímky označují také příslušnými úhly natočení, při kterých byl snímek pořízen. Z celkového snímání je poté sestaveno výsledné album náležící konkrétní osobě se všemi snímky, lišící se v úhlech pořízení snímku. Příklad evidence alba s různými úhly natočení osoby je možné názorně vidět na obr. 10 c). [2]

Ze všech snímků se následně vypočítají velikosti úseček, spojující jednotlivé markanty. Ze všech výpočtů se následně vytvoří tabulky s těmito údaji. Markanty tváře, které nebyly z důvodu natočení těžiště hlavy vidět na snímku se v příslušné tabulce vynechají, vyškrtnou. Na základě těchto údajů se následně vypočítá koeficient změn všech úseček. Tyto koeficienty jsou přiřazeny konkrétním snímkům (dle úhlu natočení). [2]



Z těchto hodnot a dle nastavení citlivosti shody (akceptovatelný rozsah velikosti změn koeficientů) je možné rozlišovat, identifikovat jednotlivé osoby – pakliže jsou koeficienty změny spojnic ve stanoveném rozmezí, je nalezena shoda. [2]

Obrázek 10 - Analyticko-statistická metoda



[2]

#### 4.5.2 Grafická metoda

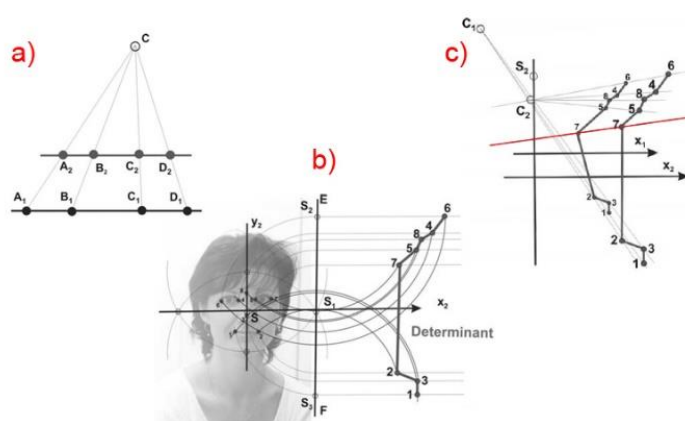
Grafická metoda identifikace osob využívá poznatky a znalosti z geometrie. Metoda vychází z myšlenky, že každý objekt je možné vyjádřit množinou bodů, markantů, které se následně využívají k prokázání geometrického podobnosti posuzovaných objektů. Zkoumané objekty jsou posuzované na základě geometrické projekce, která využívá principu, že objekty jsou totožné i v odlišném měřítku při určitém pootočení (existuje vztah perspektivní projekce). [2]

Tento postup je názorně zobrazena na obr. 11 a). Při porovnávání dvou objektů se využívá bod centra projekce C, následně se provádí protnutí porovnávaných bodů, markantů (A1-A2) prostřednictvím přímky. Tento postup se následně opakuje u všech ostatních markantů (B1-B2, C1-C2, D1-D2). Pakliže výsledné přímky protínají bod projekce C, dochází ke ztotožnění objektů, nalezení shody. Přímky někdy nemusí zcela přesně protínat bod projekce C. Z tohoto hlediska se upravuje práh citlivosti – rozmezí tolerance, akceptovatelné vzdálenosti přímky od místa projekce C. V praxi se také ale může lišit ještě úhel natočení těžiště hlavy. Z tohoto důvodu je nutné ještě zjistit poměry velikostí úseček mezi jednotlivými markanty. [2]

Z tohoto přístupu grafického porovnávání tváří přímo vychází metoda obličejových determinantů. Obličejové determinanty jsou tvořeny průniky kružnic s vynášejícími přímkami markantních bodů obličeje. Jedná se o spojitou křivku, na které leží všechny identifikační body subjektu – markanty. Tato křivka je jedinečná pro každou osobu, lišící se více či méně. Determinant je názorně zobrazen na obr. 11 b). [2]

K finální identifikaci osoby, ztotožnění dochází v procesu porovnávání jednotlivých determinantů subjektů, znázorněno na obr. 11 c). V tomto příkladu se porovnávají dvě odlišné osoby – dva odlišné determinanty. Tyto determinanty se porovnávají stejným způsobem, jako v prvním obecném příkladu na obr. 11 a). Využívá se projekčních center a následně dochází k utvoření protínajících přímek porovnávaných markantních bodů subjektů. V případě protnutí projekčních center příslušnými přímkami dochází k identifikaci osoby, ztotožnění. V tomto příkladu nedochází k protnutí projekčního centra s přímkou protínající markantní body s označením 7 – osoby nejsou totožné. [2]

Obrázek 11 - Grafická metoda



[2]

## 4.6 Automatizace obličejové biometrie

Ze všech biometrických disciplín, je biometrická identifikace na základě rozpoznávání lidských tváří jednou z nejobtížnějších, nejkomplexnějších. Tato disciplína je rozvíjena již od 60 let 20. století a řada bezpečnostních složek využívá této identifikace. Na rozdíl od ostatních typů biometrických identifikací je možné tuto identifikaci využívat skrytým způsobem tak, aniž by kontrolovaná osoba věděla o skutečnosti, že je právě prověřována. V praxi se tento způsob skryté identifikace rozšiřuje zejména u bezpečnostních složek, které mají za úkol chránit vytyčený perimetr, například letiště. V tomto příkladu se využívá identifikace z důvodu preventivního odhalení potenciálně nebezpečné, případně hledané osoby, například teroristy či zločince. [2]

Celý proces se rozlišuje na dva zásadní, stejně důležité kroky – detekce tváře a rozpoznání tváře. Algoritmy vykonávající oba kroky musí počítat s následujícími úskalími. [2]

**Detekce tváře** – detekce se provádí na základě rozpoznávání samotného obličeje, zda se nachází na scéně vůbec nějaký obličej, žádný obličej či více obličejů. Scénou se rozumí například aktuální kamerový přenos do monitorovacího centra na letišti. Tento krok, ačkoliv se jeví jako banalita, není zcela jednoduchý. Algoritmus musí rozpoznat tvář při působení různých ovlivňujících faktorů – vzdálenost obličeje (čím větší vzdálenost, tím menší počet rozpoznatelných identifikačních prvků – technická omezenost snímače), pozadí scény (nutno oddělit obličej od okolí, přesná rozpoznatelnost obličeje), případné pohyby na scéně (rychlost, stabilita snímacího prvku), výrazy, orientace tváří a osvětlení celé scény (ve viditelném světelném spektru se silně ovlivňují rysy, kontury obličeje - velký vliv stínů). Algoritmus musí mimo jiné být schopen rozeznání také reálné tváře, patřící živé osobě. [2]

**Rozpoznávání tváře** – rozpoznávání se provádí na základě extrakce biometrických charakteristik z detekovaného obličeje. V tomto příkladu dochází k identifikaci neznámé osoby na letišti v monitorovacím centru a na základě této identifikace dochází k vyhodnocení, zda je osoba potenciální hrozbou, hledanou osobou či nikoliv. [2]

V celém automatizovaném procesu identifikace se rozlišují následující přístupy:

- 2D a 3D přístupy (dvourozměrné, třírozměrné)
- černobílé, barevné, infračervené spektrum obrazů
- pohledy čelní (en face) a z boku (profilové)
- statické obrazy
- dynamické obrazy (sekvence obrazů - změna pohybu/výrazu/emoce tváře)

[2]

#### 4.6.1 Metoda Eigenface

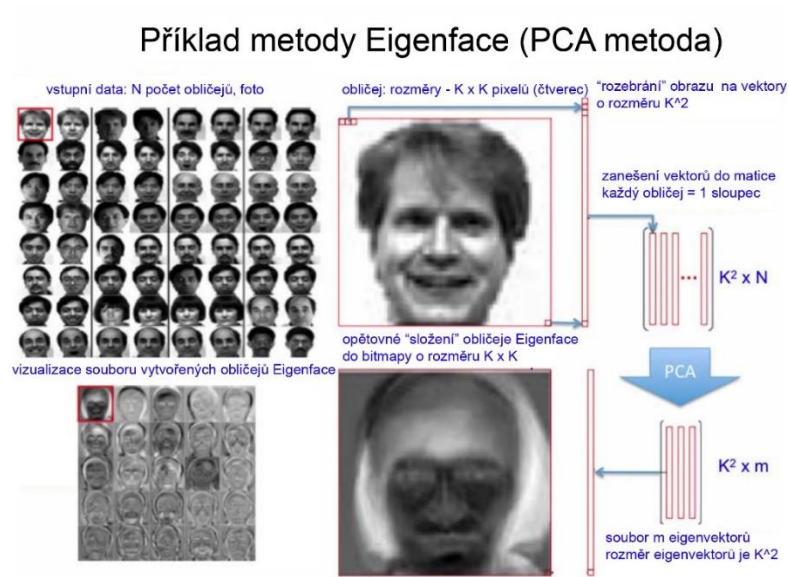
Metoda podprostoru Eigenface se snaží nalézt, detekovat charakteristické prvky obličeje, jako jsou oči, nos, ústa či uši. V případě detekování těchto charakteristických prvků lze usuzovat, že zkoumaný obraz odpovídá obličej. Tato metoda se využívá kromě detekce, lokalizace tváře, také pro rozpoznávání tváře. Přístup k metodě je založen na myšlence, že obraz obličeje je vícerozměrný vektor, skládající se z jednotlivých bodů a každá jeho dílčí část – bod (v digitální podobě pixel) odpovídá určité obrazové komponentě. Nalezení, detekování obličeje je vyjádřeno detekovaným podprostorem vektoru, ve kterém se obličej vyskytuje. [2] [10] [11]

Prostřednictvím transformačních metod dochází k vytvoření normalizovaného obrazu obličeje. Metoda využívá analýzu hlavních komponent (PCA – Principal Component Analysis). Prostřednictvím této matematické operace se generuje album normalizovaných obličejů (Eigenfaces). Normalizované obličeje se považují za standardizované obličeje, vycházející ze statistické analýzy z mnoha obrazů obličejů. Jakákoliv lidská tvář může být vyjádřena pomocí kombinací více či méně odlišných tváří. Tvář může být vytvořena prostřednictvím kombinace normalizovaného 1. obličeje z 10 %, 2. obličeje z 55 %, 3. obličeje z -3 % atd. [2] [10] [11]

Obecným normalizováním obličeje prostřednictvím metody Eigenface se rozumí změna měřítko obrazu obličeje, změna palety a škály odstínů barev, změna jasu obrazu, detekování a nastavení speciálních bodů – markantů (oči, nos, ústa či uši), díky kterému se následně zjistí orientace tváře, případně pozice a celková rotace obrazu obličeje. Cílem této normalizace je eliminovat či alespoň do jisté míry potlačit různorodé ovlivňující faktory, které byly přítomny v době pořízení obrazu – nestejně podmínky osvětlení, pozice fotoaparátu, vzdálenosti subjektu, natočení či orientace subjektu atd. Díky této normalizaci je následně možné efektivně porovnávat jednotlivé, dosud nekonzistentní obrazy takovým způsobem, jako by byly pořízené za stejných podmínek. Tyto tváře se mohou měnit na základě změny výrazů (emoce) či změny doplňků (brýle, pokrývky hlavy). Normalizované tváře jsou považovány za jakousi výchozí množinu identifikačních charakteristik jedné nebo více osob, které jsou následně využívány prostřednictvím algoritmu jako vstup pro identifikování či verifikování osob. [2] [10] [11]

Metoda Eigenface (zkoumání obličeje), je metodou dvourozměrného prostoru. V třírozměrném prostoru se tato metoda nazývá Eigenhead (zkoumání hlavy). Na obr. 12 je názorně vidět zjednodušený postup při vytváření normalizovaných obličejů metodou Eigenface. Jako vstup slouží album s celkovým počtem  $N$  obličejů – zastoupeno fotografiemi. Vybrána je první fotografie, skládající se z  $K \times K$  pixelů – čtvercová fotografie. Možno využít i obdélníkovou fotografii, ale postup je komplikovanější. Následně dochází k vyjádření fotografie, jednotlivých bodů (pixelů) do vektorové podoby. Dochází k vytvoření matice, kde každý sloupec reprezentuje jeden obličej – vektor obličeje. Po vytvoření matice je provedena matematická operace PCA, na základě které dojde k vytvoření Eigenvektorové matice. V posledním kroku dojde k formování standardizované tváře Eigenface a vytvoření alba se standardizovanými obličejí, připravenými k budoucímu porovnávání. [2] [10] [11]

Obrázek 12 - PCA, Eigenface

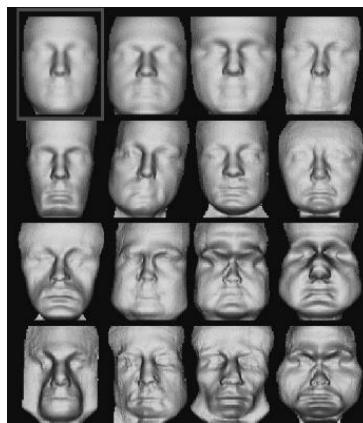


[10]

#### 4.6.2 Metoda Eigenhead

Jedná se o metodu, která přímo vychází ze svého předchůdce, z metody Eigenface, která je využívána ve dvourozměrném prostředí. Metoda Eigenhead využívá stejnou myšlenku k rozpoznávání obličejů, ale ve třírozměrném prostředí. Základní myšlenkou této metody je, že každou tvář, obličej, je možné získat za pomoci kombinace jednotlivých normalizovaných, třírozměrných modelů tváří. Tyto 3D tváře jsou znázorněny na obr. 13. [2]

Obrázek 13 - Eigenhead



[2]

Základním porovnávacím prvkem metody je plastický povrch tvořící masku obličeje. Při této metodě se využívají dva odlišné přístupy. První přístup využívá velké množství snímků, pořízených za jiných světelných podmínek a tím i odlišným nasvícením tváře. Druhý přístup využívá pouze jeden snímek, pro který se ale následně simulují a předpokládají stíny, které by mohly být přítomny v praxi. Při metodě Eigenhead dochází i k modelování jednotlivých svalů obličeje a je možné tak zpracovat velmi precizní třírozměrné modely obličejů. Při této metodě se využívá několik různých přístupů k popisu, definici, charakterizaci jednotlivých obličejů. Mezi nejčastější, deskriptivní způsoby patří využívání cylindrického, souřadnicového systému. Obličeje jsou následně vyjádřeny prostřednictvím množin bodů v třírozměrném prostoru. Kombinace jednotlivých, normalizovaných hlav (Eigenheads) odpovídajících hlavě zkoumaného subjektu je následně vyjádřena kombinační rovnicí, ve které jsou zaneseny také koeficienty shody dílčích hlav (například shoda z: 30 % Eigenhead 1., + 5 % Eigenhead 2., - 10 % Eigenhead 3.) V konečném kroku dochází k vypočítání energetické rovnice hlavy, do které jsou následně zaneseny parametry charakterizující jednak hlavu a jednak směr světelného zdroje. Metoda Eigenhead je velmi spolehlivou metodou, ale je nákladná, pomalá a výpočetně náročná. [2]

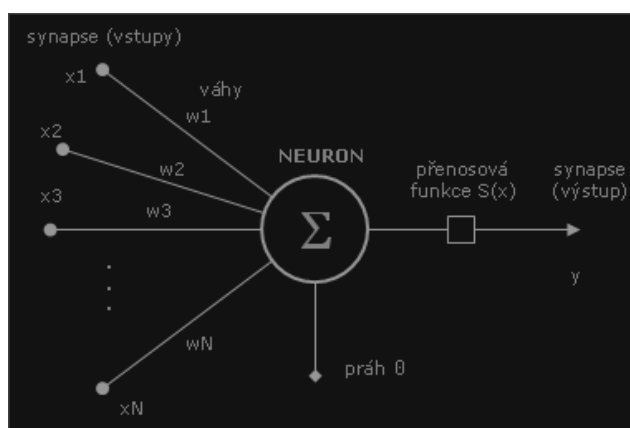
### **4.6.3 Metoda neuronových sítí – detekce obličeje**

Využívání neuronových sítí při rozpoznávání obličejů lze klasifikovat jako model o dvou třídách. První třída jsou obrazy obličejů, druhá třída jsou obrazy, které nejsou obličejem. Na tomto základu se následně učí neuronová síť automaticky rozpoznávat co obličejem je a co nikoliv. K tomu, aby se síť naučila rozpoznat tvář a odlišné objekty, se využívají knihovny se zástupci obrazů obou tříd. Jelikož existuje mnohem více objektů odlišných, které nejsou obličejem, je velmi důležité naučit rozpoznat síť zejména to, co obličejem není. Tedy postupovat a zaměřit se zejména opačným směrem, naučit síť co obličejem ve skutečnosti doopravdy není. [2] [12]

Tyto sítě se využívají zejména tam, kde popis chování modelu nebo algoritmu je velmi složitý, komplexní, ne zcela určitý a je velmi obtížné ho naprogramovat klasickým způsobem, případně nejsou-li zmapovány všechny vstupy či výstupy, případně je potřeba systém v budoucnu učít či přizpůsobovat novým podmínkám. Neuronovou sítí se rozumí rozložení jednotlivých neuronů ve vrstvách a následného spojení synapsemi. Neuron je základním prvkem sítě a vlastní libovolný počet vstupů a jeden výstup. Velmi důležitou roli zde určuje váha vstupu, která ovlivňuje hodnotu přenášené informace (jedná se v podstatě o koeficient paměti hodnoty, vstup  $\times$  váha = vstupní informace). Synapse zajišťuje spojení mezi jednotlivými neurony a určuje výslednou mohutnost sítě. Platí zde přímá úměra, čím více synapsí, tím více dat je síť schopna uchovat. Hodnotou, při které dochází k aktivaci výstupu neuronu se rozumí práh (citlivost). [2] [12]

Prostřednictvím přenosové funkce se následně výstupní hodnota upraví či zmoduluje do formy, v jaké je požadována. Model neuronu je možné názorně vidět na obr. 14. Neuronové sítě se rozlišují na sítě s učitelem a na sítě bez učitele. Sítě s učitelem se učí dle vstupních/výstupních dat a následně se z těchto dat sít' (algoritmus) sám učí (například Back-Propagation sít'). Výsledek (zpracován sítí či modelem) je porovnán s výsledkem pro učení a následně se zpětně upraví váhy na jednotlivých vstupech neuronů. Sítě bez učitele fungují na principu třídění vstupů a následně se je učí sami rozpoznávat (například Kohonenova sít'). [2] [12]

Obrázek 14 – Model neuronu



[12]

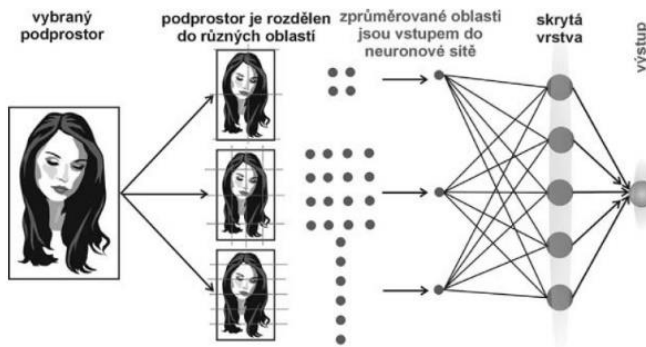
#### 4.6.4 Metoda neuronových sítí – rozpoznávání obličejů

Princip rozpoznávání obličejů prostřednictvím neuronových sítí je rozdělen do dvou skupin podle procesů, které vykonává. Do první skupiny se řadí neuronové sítě využívané pouze ke konečnému rozpoznání tváře (identifikaci, verifikaci), kdy předchozí proces – zajištění identifikačních charakteristik (markantů) je obstaráno jinými metodami, případně algoritmy. Do druhé skupiny se řadí neuronové sítě využívané kromě konečného rozpoznávání tváře také k zajištění identifikačních charakteristik (markantů). Na obr. 15 je znázorněna neuronová sít' přizpůsobená k identifikaci/verifikaci. Jako vstupním vzorkem je využívána fotografie, snímek subjektu. [2] [12]

Tento vstup je následně rozdělen dle tří odlišných přístupů. V prvním případě dochází k rozdělení vstupu do 4 bloků, v druhém případě dochází k rozdělení vstupu do 16 bloků a v případě třetím dochází k rozdělení vstupu pouze v horizontálním směru do 6 bloků. Rozdělení se provádí odlišně z důvodu jiného zaměření hledaných prvků. V rozdělení do 4 bloků se hledají zejména větší charakteristiky, jako jsou oči či nos, v rozdělení do 16 bloků se hledají zejména menší charakteristiky, jako jsou jednotlivé drobnější markanty (bod špičky nosu) a v rozdělení do 6 horizontálních bloků se hledají zejména podlouhlé charakteristiky, jako jsou ústa, obočí či čelo. [2] [12]

Ve všech třech případech dochází ke zprůměrování jednotlivých bloků a tyto zprůměrované bloky slouží jako vstup pro neuronovou síť. Síť následně porovnává jednotlivé vstupy a na základě svého předchozího učení konstatuje závěry v rozhodovacím procesu, zda došlo k nalezení shody či nikoliv. [2] [12]

Obrázek 15 - Neuronová síť



[2]

#### 4.6.5 Metoda distribuce odstínu šedi – detekce obličej

Tyto metody využívají princip rozložení šedi v obraze, ke kterému dochází při klasických všedních podmínkách nasvícení obličej. Toto rozložení stupňů šedi je obecně popsáno do souboru pravidel, kde je zaznamenáno, jakým způsobem dochází k distribuci šedi v obraze. Mezi tyto pravidla se řadí například distribuce šedi v oblasti čela a očí. Obecně platí, že v místě čela bývá obraz zřetelně světlejší než v místě očí, kde bývá zřetelně tmavší. Špička nosu, bývá opět velmi světlým místem a oblast úst bývá opět místem tmavším. Příklad detekovaného obličej v obraze touto metodou je znázorněn na obr. 16. Jednou z nejznámějších metod využívající tento přístup je metoda mozaiky. K finálnímu kroku zpracování metoda využívá ještě metodu detekce hran. Metoda postupuje systematicky tím způsobem, že si obraz nejdříve rozdělí do pravidelných bloků o předem definovaném počtu bloků, například 3 x 3 či 4 x 4. Následně dochází v těchto jednotlivých blocích k identifikaci jednotlivých markantů – očí, úst, nosu atd., algoritmus postupuje systematicky blok, po bloku. Algoritmus automaticky vyřazuje bloky, ve kterých se nevyskytují markanty. Pakliže je vstupem obraz skutečné tváře, jsou rozpoznány tyto charakteristické markanty na základě distribuce šedi v obraze. [2]

Ve finálním kroku rozpoznávání dochází ještě k přesnějšímu rozdělení bloků, ve kterých byly nalezeny markanty. Následně dochází k využití metody detekce hran. Díky této metodě celý algoritmus definitivně určuje pozici markantů a rozpoznává obličej. Tato metoda je velmi efektivní a často používaná, ačkoliv má také nedostatky, zejména v rychlosti zpracování a následnému vyhodnocování. [2]



Obrázek 16 - Detekce obličeje na principu rozložení šedi



[2]

#### 4.6.6 Metoda distribuce odstínu šedi – rozpoznávání obličeje

Rozpoznávání konkrétní tváře při procesu identifikace či verifikace na metodě rozložení šedi v obraze vychází z metody mozaiky, která je využívána při detekci obličeje. Postup je také velmi podobný. Dochází k porovnávání dvou konkrétních obrazů – jednoho aktuálně nasnímaného vzorku (zkoumaného subjektu) a jednoho vzorku z databáze osob. Oba obrazy se opět rozdělí do bloků o předem definovaném počtu bloků. Tyto bloky se systematicky porovnávají navzájem – porovnání mezi známým a neznámým obrazem. Navíc dochází ještě k porovnávání okolí bloků. K porovnávání se využívají  $n$ -rozměrné vektory, reprezentující jednotlivé bloky. Následně dochází k utvoření rozhodnutí, zda jsou dva porovnávané obrazy shodné. Porovnávání se provádí do doby, než je nalezena shoda, případně do doby, než dojde k porovnání všech vzorků z databáze. Metoda je velmi náročná na výpočetní výkon celého systému, zejména z důvodu, že se kromě porovnávání jednotlivých bloků porovnává také okolí jednotlivých bloků. [2]

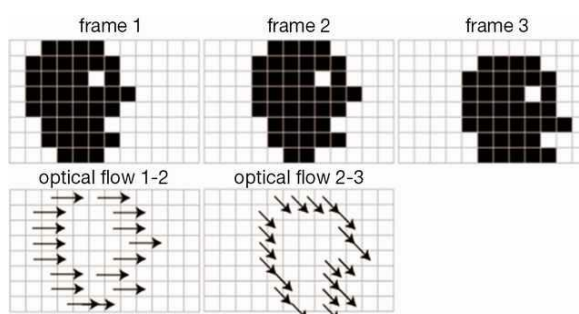
#### 4.6.7 Metoda optických toků – detekce obličeje

Metody využívající pohybu na scéně fungují na principu změny směru (orientace) a rychlosti jednotlivých markantních bodů. Jedná se o vektorovou analýzu, která zkoumá pohyb těchto bodů na scéně dle předem definovaných zkoumaných, hledaných prvků (oči, ústa, nos atd.). Jako vstupní data pro tuto analýzu se používají sekvenčně nasnímané snímky scény, po předem definovaných intervalech. Tyto snímky jsou následně označeny příslušným indexem. V průběhu detekce obličeju dochází ke zjištění vektorové mapy obličeje, na základě zjištění jednotlivých markantů. Tato vektorová mapa se následně stává objektem sledování. Na obr. 17 je znázorněn obecný princip metody sledování optických toků na scéně. Na obrazu jsou pořízeny sekvenčně 3 snímky scény (profil hlavy). [2]

Na části s označením frame 1 a frame 2 je zachycen obličej, kdy nemění svou polohu. Všechny optické toky jednotlivých bodů obličeje jsou zachyceny na části obrazu s označením optical flow 1-2 (optické toky mezi obrazy 1-2) směřující směrem doprava. Na části s označením frame 3 je zachycen obličej, kdy změní svou polohu – ve směru kladném osy  $x$  (doprava) a ve směru záporném osy  $y$  (dolů). [2]

Všechny optické toky jednotlivých bodů obličeje jsou zachyceny na části obrazu s označením optical flow 2-3 (optické toky mezi obrazy 2-3) směřující směrem po diagonále (doprava, dolů). Tato metoda je náchylná k chybám v případě, že se vyskytuje na scéně více pohybujících se osob odlišnými směry, pohybující se odlišnými rychlostmi a pakliže dochází k překrývání jednotlivých obličejů či zakrývání obličejů jinými objekty. [2]

Obrázek 17 - Pohyb na scéně



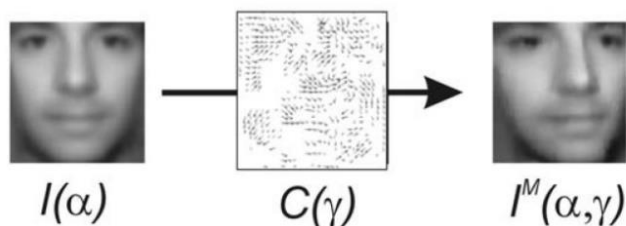
[13]

#### 4.6.8 Metoda optických toků – rozpoznávání obličeje

Rozpoznávání jednotlivých obličejů k identifikaci/verifikaci prostřednictvím metody optických toků je založeno na velmi podobném principu, jako detekce samotného obličeje. Jako vstupním vzorkem jsou zde opět sekvenční snímky pohybu hlavy. Tyto snímky jsou opět řazeny za sebou s postupem času. Na tomto základě dochází ke změně jednotlivých vektorových toků (mění se směr i rychlost) obličeje. Pomocí metody optického toku, lze následně rozlišovat rozdíly, mezi jednotlivými toky porovnávaných snímků (vstupní subjekt – databáze). Každý obličej má více či méně odlišnou vektorovou skladbu (mapu) obličeje. Tyto vektorové mapy se následně mezi sebou porovnávají do doby, než dojde k nalezení shody či porovnání se všemi referenčními snímky databáze. Navíc, kromě identifikace samotného obličeje je možné automatizovaně zjistit i případný pohyb a případně emoce, výraz subjektu. [2]

Prostřednictvím této metody je také mimo jiné možné odhadnout výslednou podobu obličeje v případě změny optického toku (pohybu obličeje). Tento proces je znázorněn na obr. 18. V části s označením I ( $\alpha$ ) je zobrazen výchozí snímek, v části s označením C ( $\gamma$ ) je znázorněn požadovaný optický tok, v části s označením I ( $\alpha, \gamma$ ) je znázorněna výsledná, pravděpodobná podoba obličeje při tomto předpokládaném pohybu obličeje. [2]

Obrázek 18 - Odhadnutí výsledné tváře při změně pohybu na základě optického toku



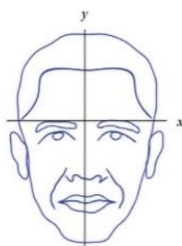
[2]

#### 4.6.9 Metoda rozpoznání rysů, kontur – detekce obličeje

Metody založené na detekci kontur obličeje vycházejí z matematického popsaní obličejových rysů. Kontury obličeje je možné popsat matematickým vyjádřením kontur za pomoci konvexních a konkávních tvarů. Při tomto postupu je důležité nejdříve korektně a co nejpřesněji definovat základní rysy obličeje, kontury. Na tomto základě se algoritmus snaží extrahovat tvary, nalezené v obraze a následně se snaží rozpoznat, zda tyto vyextrahované tvary mohou popisovat obličej. Algoritmus zjišťuje, jedná-li se skutečně o obličej. [2]

Algoritmus se snaží rozpoznat charakteristické markanty – oči, ústa, nos atd. V tomto procesu se využívá metody detekce hran, případně jiných metod, které umožňují rozlišovat jednotlivé tvary. Kontury obličeje detekovatelné algoritmem jsou znázorněné na obr. 19. Metoda je velmi závislá na schopnosti detekce hran. Pakliže algoritmus špatně vyhodnotí hranu či nepřesně, dochází následně ke zkreslení, případně nekorektnímu vyhodnocení tvaru, a to může mít za následek nekorektní detekci obličeje. [2]

Obrázek 19 - Kontury obličeje, vyjádřitelné matematickými funkcemi



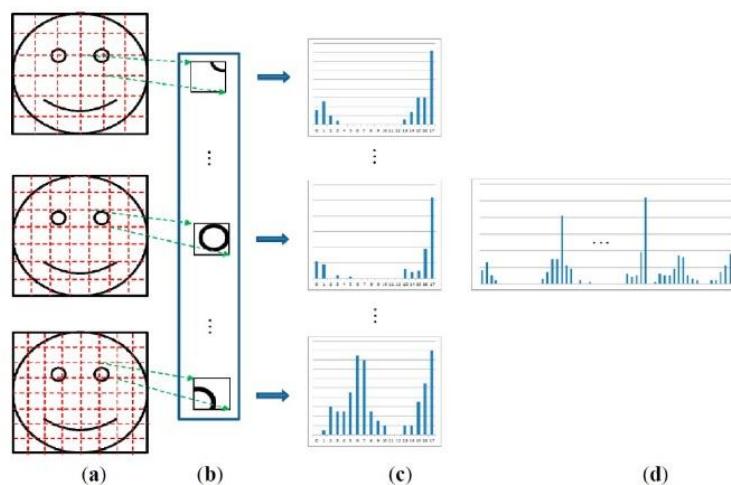
[14]

#### 4.6.10 Metoda distribuce barev obličeje – rozpoznání obličeje

Metody využívající barevného složení obrazu k rozpoznávání obličejů pracují na principu odlišnosti barevného popisu obličeje od okolního prostředí. Popis obličeje prostřednictvím barev je do jisté míry odlišitelný od svého prostředí a vychází z metody rozpoznávání obličejů na základě odstínů šedi. Každý obličej lze vyjádřit velmi podobnou skladbou, uskupením, rozložením barev v obrazu. Odlišnosti nastávají při rozdílné etnicitě zkoumaného subjektu, jelikož lidé mají mírně či více odlišnou barvu pleti (světlejší či tmavší). Na tomto základě je nutno definovat jednotlivé složení barev pro každé rasové zastoupení, aby nedocházelo k nekorektnímu rozpoznávání obličejů z důvodu odlišných odstínů pleti. Obličej se stejně jako u metody rozpoznávání obličejů na základě distribuci šedi rozlišuje do bloků, kde se očekává určité barevné složení. Těmito bloky mohou být například oči, líce, čelo, nos či ústa. [2] [15]

Příklad detekce obličeje na barevné skladbě obrazu je znázorněn na obr. 20. V části obrázku označené a) je zjednodušeně zobrazen blok obličeje testovaného subjektu. Tento obličej je rozdělen do jednotlivých bloků. Přesnost a citlivost detekce je přímo úměrná počtu bloků. Čím více bloků, tím přesnější detekce. V části obrázku označené b) je zobrazen aktuálně zkoumaný blok. V části obrázku označené c) je zobrazen histogram – barevná skladba bloku. Ze všech dílčích histogramů se následně vytvoří výsledný histogram v části obrázku s označením d), a následně dochází či nedochází k rozpoznání tváře. Tato metoda je silně ovlivnitelná světelnými podmínkami. Velmi důležité je také směr a úhel, ze kterého dopadá světlo na subjekt, jelikož se následně vytváří stíny, které ovlivňují vzhled obličeje pro kamery. V případě, že je světlo příliš silné, či naopak příliš slabé, dochází k nekorektnímu určení barevné skladby obrazu, na základě kterého může následně dojít ke špatné detekci obličeje na scéně. [2] [15]

Obrázek 20 - Příklad histogramu obličeje

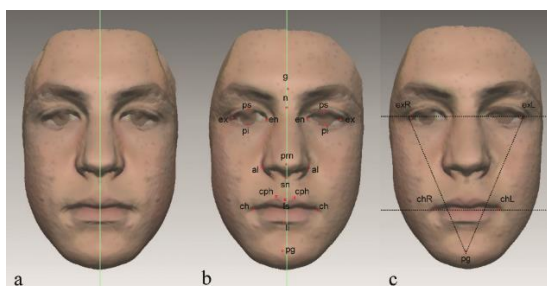


[15]

#### 4.6.11 Metoda založená na symetrii – detekce obličeje

Metody detekující obličej jsou založeny na poznání, že lidské obličej jsou do jisté míry symetrické a na tomto základě je lze rozeznávat od okolních objektů. Přístupy v definování symetrie tváře jsou odlišné a jejich rozpoznávací algoritmy také. Tyto algoritmy fungují na principu hledání předem definovaného symetrického obrazce patřícího charakteristickému prvku obličeje. Na tomto základě se hledají například konkrétní kruhové tvary v obraze, reprezentující oči, případně se hledají body, které by odpovídaly markantům obličeje a byly zároveň do určité míry symetrické. Na obr. 21 je zjednodušeně zobrazena symetrie obličeje, kde v části s označením a) je obecné znázornění symetrie obličeje, v části s označením b) jsou znázorněny konkrétní symetrické markanty a v části s označením c) je znázorněna tvář vyjádřena celkovým, symetrickým obrazcem. [2] [16]

Obrázek 21 - Symetrie obličeje

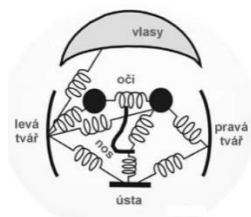


[16]

#### 4.6.12 Metoda založená na markantech a geometrických tvarech – rozpoznávání obličeje

Jednou z nejstarších metod rozpoznávání obličejů, která je důkladně zautomatizována, je metoda vycházející z metody analyticko-statistické identifikace osoby. Metoda je založena na antropometrických poznacích. Tato metoda je stále jednou z nejpoužívanějších a nejrozšířenějších i v dnešní době. Metoda je postavena na základních, charakteristických, markantních bodech, stejně jako metoda, z které vychází. Navíc jsou zde ještě dopočítávány geometrické tvary jednotlivých charakteristických částí obličeje (tvořené markanty). Tyto tvary a markanty jsou názorně zobrazeny na obr. 22. Vzdálenosti mezi jednotlivými markanty a geometrickými tvary jsou reprezentovány pružinami, které představují variabilní vzdálenosti mezi body, patřící odlišným obličejům. [2]

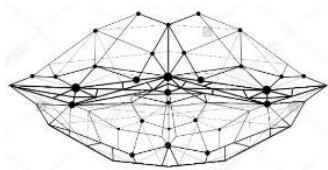
Obrázek 22 - Porovnávané markanty obličeje



[2]

Obličej je rozdělen do dílčích objektů. Každý tento objekt (oči, ústa, nos atd.) je následně vyjádřen deformační šablonou, případně parametrickým modelem. Deformační model rtů je znázorněn na obr. 23, včetně jednotlivých geometrických linií, kde tvar i velikost rtů je závislá na vzdálenostech jednotlivých parametrických bodů. Z tohoto modelu je následně spočítána energetická funkce, která je ovlivněna nejen vzdálenostmi a obrysy zkoumaného objektu, ale i distribucí odstínu šedi v obraze. Ve výsledku se porovnává dosažená hodnota energetické funkce. [2]

Obrázek 23 - Deformační model rtů



[17]

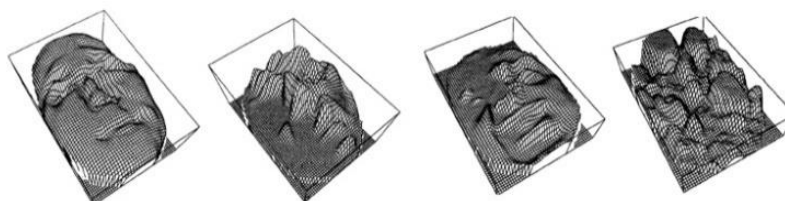
V průběhu času docházelo k odlišnému přístupu k vývoji algoritmů. Některé algoritmy se zaměřují na detekci markantních bodů očí, úst a nosu, některé algoritmy se zaměřují pouze na oči, některé se zaměřují na obrys tváře a některé se zaměřují na délku, šířku nosu, případně na umístění úst, brady subjektu. Mezi největší nedostatky této metody patří zejména závislost na kvalitním pořízení vstupního snímku – biometrického vzorku. Snímek musí být dostatečně kvalitní (rozlišení snímku), testovaný subjekt musí být dobře nasvícen a musí být také vhodně natočen a nasměrován (markanty musí být vidět, nesmí být zakryty případně zastíněny). Výpočet energetického minima je výpočetně náročný a zdlouhavý. [2]

#### 4.6.13 Metoda deformačních modelů – rozpoznávání obličeje

Při této metodě se využívá prostorového modelu obličeje. Nejdříve se vytvoří model tváře, který je tvořen sítí horizontálních a vertikálních čar, které jsou na sebe kolmé. Výsledná tvář, mapa obličeje je tvořena rozdílnou hustotou, počtem čar v jednotlivých oblastech obličeje, případně jejich zakřivením. [2]

V závislosti na hustotě a zakřivení čar vznikají jednotlivé kontury obličeje, obrysy a následně dochází k utvoření celkového, prostorového modelu obličeje. Linie, jejich úhly a body jednotlivých částí (oči, ústa, nos atd.) se mění se změnou výrazu, emocí subjektu. Po vytvoření normalizovaného modelu obličeje dochází k jeho porovnávání s ostatními 3D zakřivenými povrchy – dochází k elastickému srovnávání dvou zakřivených povrchů. Příklady korektního a nekorektního vyjádření 3D deformačního modelu obličejů jsou znázorněny na obr. 24. Každá osoba vlastní svou jedinečnou 3D mapu obličeje, případně jí náleží jedinečné změny povrchu v závislosti na aktuálně vyjadřovaných výrazech, emocích. Tato metoda dosahuje vysoké spolehlivosti, ale je výpočetně velmi náročná. [2]

*Obrázek 24 - Deformační modely*

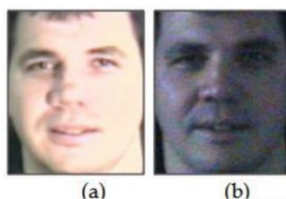


[2]

## 4.7 Přisvit v biometrii a využívaná spektra

U biometrických systémů se rozlišuje, zda se systém spoléhá pouze na okolní osvětlení či nikoliv. Mnoho výrobců těchto systémů využívá, případně nevyužívá dodatečná, umělá přisvícení těchto systémů. Toto přisvícení vyniká zejména v nevyhovujících světelných podmínkách, kdy bez použití přisvitu klesá spolehlivost rozpoznávání těchto obličejových čteček. Přisvity se rozdělují dle spektra, ve kterém působí na přisvity ve viditelném spektru a na přisvity v infračerveném spektru. Tyto dva typy přisvitů jsou momentálně nejrozšířenějšími způsoby přisvícení. Na obr. 25 je zobrazen rozdíl mezi využitím dodatečného přisvitu subjektu (ve viditelném spektru) a nevyužitím. Z tohoto obrazu jednoznačně vyplývá, že i když je v tomto případě subjekt jemně přesvícen a přisvit není ideálně vyvážen, čitelnost subjektu je mnohonásobně lepší s využitím umělého přisvitu, jednotlivé rysy a kontury obličeje jsou lépe čitelné a stíny jsou také do jisté míry potlačeny. Pro nejlepší - ideální způsob přisvícení by bylo nutné mírně snížit intenzitu osvětlení, vyvážit strany nasvícení (aby nebylo nasvícení dominantní pouze z pravé strany, aby bylo rovnoměrně distribuováno nejlépe z obou stran). [2] [18] [19]

Obrázek 25 - Rozdíl mezi využitím a nevyužitím přisvitu



[19]

Metody přisvícení u biometrických systémů se liší zejména elektromagnetickým spektrem, ve kterém působí. Nejčastěji využívaná elektromagnetická spektra v biometrii jsou viditelné spektrum (klasické světlo) a infračervené spektrum. Jednotlivá elektromagnetická záření je možné vidět na obr. 26, kde jsou názorně zobrazeny frekvence ( $f$ ) i vlnové délky ( $\lambda$ ) jednotlivých spekter. Odlišnost těchto zcela odlišných elektromagnetických spekter je nutné respektovat a přistupovat k oběma typům přisvícení zcela odlišně. Již při návrhu biometrického systému je nutné podřídit vybranému spektru metody a prostředky pracující v tomto typu přisvitu, jelikož ne všechny prostředky (kamery, senzory) či metody, algoritmy jsou mezi sebou kompatibilní. [2] [20] [21]

Obrázek 26 - Elektromagnetické spektrum



[20]

#### 4.7.1 Biometrie a viditelné spektrum, přisvit

Viditelné spektrum neboli světlo je ta část spektra, kterou je možné pozorovat pouhým lidským okem bez nutnosti použití speciálního prostředku k vizualizaci jako u jiných typů záření (například infračerveného záření). Viditelné světlo je část elektromagnetického spektra s vlnovou délkou menší, než je infračervené záření (IR) a zároveň větší než ultrafialové záření (UV). Vlnová délka světla má rozmezí mezi 400-800 nm. Viditelné světlo se skládá z několika základních, spektrálních barev, které do sebe plynule přecházejí. Tyto barvy se mohou následně také mísit a následně tvořit nespektrální barvy, jako například barvu bílou, černou či různé jiné barevné odstíny. Tyto barvy mají rozdílnou vlnovou délku a také frekvenci. Pokud objekt vykazuje určitou barvu, znamená to, že pohlcuje všechny ostatní barvy spektra, kromě těch, které jsou viditelné z důvodu, že se od povrchu objektu viditelné barvy odráží. Na obr. 27 je vidět přehled základních, spektrálních barev a jejich vlnových délek ( $\lambda$ ) a frekvencí ( $f$ ). [20] [21] [22]



Z obr. 27 vyplývá, že s rostoucí vlnovou délkou je tendence frekvence klesající. Nejmenší vlnovou délku nabývá barva fialová, která má zároveň nejvyšší frekvenci. Největší vlnovou délku nabývá barva červená, která má zároveň nejnižší frekvenci. [20] [21] [22]

Obrázek 27 - Viditelné spektrum, barvy

Barva	Vlnová délka	Frekvence
červená	~ 625 až 740 nm	~ 480 až 405 THz
oranžová	~ 590 až 625 nm	~ 510 až 480 THz
žlutá	~ 565 až 590 nm	~ 530 až 510 THz
zelená	~ 520 až 565 nm	~ 580 až 530 THz
azurová	~ 500 až 520 nm	~ 600 až 580 THz
modrá	~ 430 až 500 nm	~ 700 až 600 THz
fialová	~ 380 až 430 nm	~ 790 až 700 THz

[21]

Barva světla se také velmi odlišuje v závislosti na teplotě. Tato hodnota barvy se odborně nazývá teplota chromatičnosti a je znázorněna na obr. 28. Tato hodnota blíže specifikuje spektrum bílého světla a udává se v kelvinech. Prostřednictvím těchto hodnot se rozlišují barvy světel na teplé a studené barvy. Teplé barvy jsou zejména červená, oranžová či žlutá. Studené barvy jsou zejména modrá a fialová. U biometrických systémů se jako zdroj dodatečného viditelného světla - přísvitů využívají zejména LED žárovky. Pakliže tyto LED žárovky podávají bílé světlo, následně se ještě rozlišuje svým podávaným bílým světlem, na světlo podávající ve formě teplé bílé (2700-3500 K) a studené bílé (6000-6500 K). Dle použitého odstínu může následně také docházet k ovlivňování vzhledu, nasvícení subjektu. Barva by měla být volena, pokud možno takovým způsobem, aby co nejlépe osvětila subjekt a zvýraznila důležité rysy, kontury obličeje. [23] [24]

Obrázek 28 - Viditelné spektrum, barva světla v závislosti na teplotě



[23]

#### 4.7.2 Zdroje okolního světla

Obecně zdroje světla se rozlišují na přirozené a umělé zdroje. S oběma typy zdrojů je nutné počítat při návrhu biometrického systému, případně osvitů jako takového, jelikož může docházet k nežádoucím účinkům na porízených, biometrických snímcích (vzorcích). Zdroje světla se dále rozlišují na bodové a plošné. Bodová světla jsou takové zdroje, jejichž rozměry jsou vzhledem k vzdálenosti zanedbatelné (žárovka v lampě, hvězda). Plošná světla jsou takové zdroje, jejichž rozměry vzhledem k vzdálenosti nelze zanedbat (zářivka, slunce). [25]

**Přirozené denní světlo** - při návrhu je nutné počítat s tím, že pakliže bude biometrická identifikace řešena v otevřeném prostoru, případně v uzavřeném prostoru, ale s přístupem přirozeného denního světla (skrz okna, dveře atd.), je nutné počítat s těmito účinky - orientací světla, intenzitou a také nekonzistentností tohoto zdroje osvětlení. Toto přirozené osvětlení mění intenzitu, orientaci v závislosti na ročním období, hodině i počasí. S těmito jevy je nutné počítat a přizpůsobit řešení systému takovým způsobem, aby bylo schopné reagovat na tyto situace - možnost přebytku světla (slunečný den, do jisté míry potlačitelné slunečními clonami a filtry) či naopak nedostatku světla (noc, tma), deštivé počasí, sníh, mlha, nekonzistentnost orientace stínů atd. Je nutné předem počítat s těmito možnými negativními účinky denního světla a zvážit vhodnost použité technologie případně vhodného spektra a případného přísvitů. [25]

**Žárovka** – jedná se o slabý zdroj světla. Na výslednou barvu snímku mají vliv kromě stínítka žárovky také případné nedaleké barvy zdí či jiných předmětů, od kterých je možný světelný odraz. Žárovky jsou postupně vytlačovány jinými způsoby osvětlení, ale stále ještě jsou přítomné a je nutné s nimi proto počítat. Používají se zejména při osvětlování menších, vnitřních prostor. Na snímcích bývá žárovka většinou přeexponovaná (ostře bílá). [25]

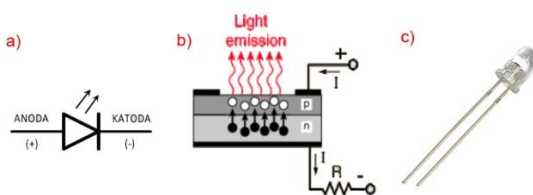
**Zářivka** – vzhledem k odlišnosti zářivek, nelze jednoznačně určit míru ovlivnění snímku, jelikož existuje mnoho typů zářivek, které snímek ovlivní ve větší či menší míře. Zářivky jsou velmi rozšířené a slouží jako způsob osvětlení zejména vnitřních prostor, malých i velkých. Hlavním zdrojem ovlivnění snímků bývá opět odraz světla zejména od případných okolních zdí a předmětů. Z principu funkce zářivky přirozeně blikají v závislosti na frekvenci, zhruba 100 x za vteřinu. Toto blikání, pokud je tedy zářivka v pořádku, není okem viditelné, případně jen velmi lehce, ale snímače a kamery mohou být na toto blikání citlivé (zejména v intervalu kratším než 1/50 vteřiny) a toto blikání může ovlivnit výslednou kvalitu snímku. [25]

**Halogen** – jedná se o velmi silný zdroj světla, který se může vyskytovat zejména ve venkovních prostorech, například při kombinaci s detektorem typu PIR (Passive Infrared Detector – detektor pohybu) při osvětlení vchodových dveří při zaznamenání pohybu. Halogeny se používají zejména při osvětlování venkovních prostor, případně pracovních prostor, jako jsou garáže. Světlo vyprodukované tímto zdrojem se na snímcích projevuje jako velmi ostré, vytváří velmi ostré stíny, velké odlesky, podává nevhodnou barvu (příliš modré barevné složky světla, omezitelné modrým korekčním filtrem). [25]

### 4.7.3 Bílý LED přísvit

LED (Light Emitting Diodes) přísvity využívají ke své funkci polovodičového přechodu PN. Pakliže dochází k průchodu elektrického proudu v propustném směru, dochází v aktivní vrstvě k emitování světla. Na obr. 29 v části s označením a) je znázorněna obecná schematická značka, v části s označením b) je znázorněn PN přechod a v části s označením c) je znázorněn příklad bílé LED. [26] [27]

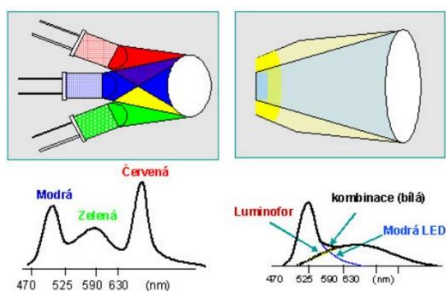
Obrázek 29 - Schematická značka, PN přechod, LED dioda



[26] [28]

LED mohou emitovat světlo určité, konkrétní barvy v závislosti na použité vlnové délce, případně emitovat jiný druh záření (IR či UV záření). Přísvit s využitím LED bývá jedním z nejrozšířenějších a nejpoužívanějších řešení. LED diody se vyvíjely již od 60 let 20. století. Nejdříve se vyvinuly základní barevné varianty spektra RGB (Red – červená, Green - zelená, Blue – modrá). K tomu, aby bylo možné vytvořit bílé LED světlo bylo zapotřebí určité kombinace všech těchto tří barev. Nejdříve se využívala kombinace všech tří separátních LED, kde v kombinaci byla zastoupena červená, zelená i modrá barva a z této kombinace došlo k utvoření bílé barvy. Tento postup je názorně zobrazen na levé části obr. 30. Následně se vyvinula speciální LED, která emitovala jasné modré světlo a s úpravou konstrukce LED, přidáním zejména fosforového luminoformu bylo možné vytvořit jasné bílé světlo prostřednictvím jedné, samostatné LED. V tomto případě dochází k emitování jasného modrého světla, které částečně prochází fosforovým luminoforem a částečně prochází přímo, bez ovlivnění luminiscenční vrstvou. Touto částečnou transformací světla (luminoforem) dochází k vytvoření ostatních barevných složek, které ve výsledku v kombinaci s přímým emitovaným světlem vytváří požadovanou bílou barvu. Tento postup je názorně zobrazen na pravé části obr. 30. Mezi velké výhody LED přísvitu patří zejména dlouhá životnost, vysoká svítivost, nízká energetická náročnost, odolnost vůči nárazům, kompaktnost a lehkost, ekologičnost. Mezi další velmi důležité výhody patří jednoduchá regulovatelnost, možnost stmívání a okamžitý proces zapnutí/vypnutí. Tento přísvit není náchylný na časté, opakované zapínání/vypínání. Kompaktnost a jednoduchost konstrukce LED neomezuje z konstrukčního hlediska osvětlovací systém. Z obecného hlediska lze považovat dnešní ceny tohoto řešení prostřednictvím využití LED technologie za velmi finančně příznivé řešení. [26] [27]

Obrázek 30 - LED, RGB barvy a bílá barva



[27]

#### 4.7.4 Nevýhody využití viditelného spektra přívsvitu

Mezi největší nevýhody viditelného spektra světla při pořizování biometrických snímků je zejména nekonzistentnost a obtížnost korektního nasvícení subjektu. Subjekt může být ovlivněn okolním světlem, případnými stíny, případně ve venkovním prostoru počasím (sníh, déšť, mlha), které mají zásadní vliv na citlivost a spolehlivost rozpoznání obličeje. Další nevýhodou je viditelnost přívsvitu lidským okem, při kterém může docházet k rušení zkoumaného subjektu, případně upozornění, že případný pachatel je prověřován (což může být považováno za pozitivum i negativum, dle úhlu pohledu). Mezi další nevýhody patří ovlivnitelnost spolehlivosti v negativním smyslu z důvodu změny odrazivosti, reflektivity povrchu obličeje (nečistota, mastnota, make-up atd.). Při nevhodném nasvícení může docházet k nadměrnému odrazu světla na subjektu (přebytečné nasvícení), případně může docházet k tvorbě nevhodných stínů (nedostatečné nasvícení, špatné úhly nasvícení či málo světelných zdrojů). [29] [30] [31] [32]

Z těchto všech nedostatků je nezbytné provádět mnoho dalších, dílčích opatření, aby byla zaručena konzistentnost snímků a jejich světelných podmínek, alespoň do použitelné míry při působení všech těchto faktorů. Na obr. 31 je znázorněno špatné a správné nasvícení subjektu. V obraze s označením a) dochází k nedostatečnému nasvícení (tvorba stínů), v obraze s označením b) dochází k přebytečnému nasvícení (tvorba odrazů) a v obraze s označením c) je znázorněno korektní nasvícení subjektu. [29] [30] [31] [32]

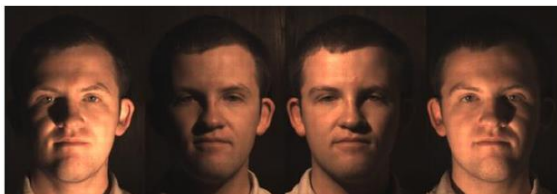
Obrázek 31 - Ukázky špatného a správného nasvícení



[29]

Na obr. 32 je znázorněna různá orientace stínů, dle směru nasvícení. Nasvícení je realizováno v levých dvou snímcích z pravého směru a liší se ve vzdálenosti nasvícení. Dále je nasvícení realizováno v pravých dvou snímcích z levého směru a liší se opět ve vzdálenosti nasvícení. Nasvícení je zde u všech příkladů nevyhovující – příliš mnoho stínů, nevyváženost nasvícení. [33]

Obrázek 32 - Orientace stínů



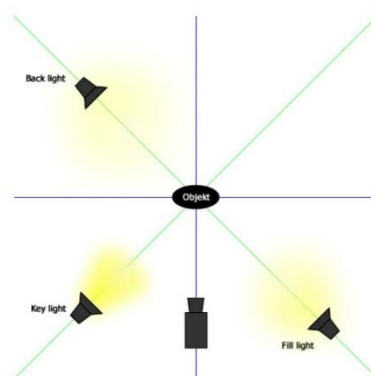
[33]

#### 4.7.5 Ideální nasvícení subjektu

Ideální nasvícení subjektu je takové nasvícení, při kterém je obličej subjektu vhodně světelně nasvícen, není přexponován (není přebytečně nasvícen) ani podexponován (není dostatečně nasvícen). Barva nasvícení je zvolena tak, aby co nejlépe vynikaly rysy, kontury obličeje a zásadně se neovlivňoval vzhled testovaného subjektu. Na obličejí musí být vidět dostatečně zřetelně kontury, rysy a markanty obličeje. Obličej by měl být nasvícen ze všech úhlů konzistentně, subjekt by měl být dostatečně odlišitelný od svého okolí. Stíny by měly být, pokud možno naprosto eliminovány a světlo by mělo rovnoměrně osvětlovat tvář subjektu, neměly by být vidět žádné bodové odrazy, odlesky či jiné světelné artefakty. [25]

Na obr. 33 je zobrazen ideální případ nasvícení, který ale není v mnoha situacích reálně přijatelný a proveditelný, slouží pouze jako ukázkový příklad, jakýsi referenční model, ke kterému je snaha se přiblížit, dle dostupných možností. [25]

Obrázek 33 - Ideální podmínky nasvícení



[25]

Tento model se nazývá tříbodový (Three-Point Lighting) a jedná se o základní techniku nasvícení s využitím tří světel. Celé nasvícení probíhá v uzavřené místnosti s bílými stěnami, bez přístupu přirozeného denního světla. Tato světla se nazývají key light, fill light a back light. Key light je hlavní světlo o největší intenzitě, které svírá  $45^\circ$  úhel s kamerou a zajišťuje hlavní nasvícení subjektu. Fill light je doplňkové světlo, které zjemňuje ostré stíny tvořené hlavním světlem. Jeho intenzita je oproti hlavnímu světlu nižší a rozptýlenost vyšší. Světlo svírá s osou kamery také  $45^\circ$ , ale v opačném směru. Back light osvětluje subjekt zezadu. Cílem tohoto světla je zajistit dostatečného zvýraznění subjektu oproti pozadí, takzvaně vytrhnout subjekt z pozadí scény. Intenzita světla je ze všech tří světel nejnižší a je nutné zajistit, aby světlo nesvítilo do kamery. [25]

#### 4.7.6 Zásady při realizaci viditelného přisvícení

Při samotné realizaci je nutné zvážit, zda biometrická identifikace bude realizována ve venkovním nebo vnitřním prostředí. Preferovaným prostředím pro tuto identifikaci s využitím viditelného spektra, by mělo být prostředí vnitřní, a to z důvodu náchylnosti na ovlivnitelnost světelných podmínek a velkého vlivu denního přirozeného světla. Následně je důležité umístění biometrického zařízení, ideálně do prostor, kde jsou bílé stěny (výborná odrazivost a rozptyl světla). Dále jednobarevné, nerušivé pozadí (jednoduchá a precizní oddělitelnost subjektu od pozadí) a pokud možno zajištění prostředí, kde je možné alespoň minimálního soukromí (pokud jsou k verifikaci požadované další identifikátory založené na typu například vlastnictví (karty, čipy), případně na typu znalostí (kódy, hesla)). V ideálních případech se využívají například specializované identifikační uličky, případně oddělené místnosti. Při realizaci ve venkovním, otevřeném prostředí je při návrhu přisvícení nutno počítat navíc i s okolním denním světlem a přizpůsobit způsob osvětlení. [2]

Při realizování osvětlení je nutné použít takový způsob přisvícení, který eliminuje nebo alespoň potlačí na přijatelnou míru nedostatky viditelného spektra. Z tohoto důvodu je nutné zvolit adekvátní typ přisvitu. Nejčastěji využívaným zdrojem přisvitu v tomto spektru jsou zdroje přisvitu LED. Následně je nutné zvolit vhodný typ a případně počet těchto LED (dle výkonnosti a svítivosti), aby intenzita tohoto osvětlení dostatečně osvětila požadovaný subjekt. Tato síla osvětlení je závislá na vzdálenosti zkoumaného subjektu a na citlivosti použitého snímače či objektivu kamery. [30]

Dále je nutné zajistit optimální tvar a způsob rozložení jednotlivých světelných přisvitů (například prstenc, linie), případně jejich pozice (například levá strana, střed, pravá strana), aby výsledný přisvit byl rovnoměrný, aby bylo přítomno co nejméně stínů (ideálně eliminované) a aby světlo zlepšovalo čitelnost subjektu. V neposlední řadě je nutné zajistit korektní synchronizaci aktivace přisvitu a snímacího zařízení, kamery. Přisvit je možné nechat aktivován neustále, případně aktivovat přisvit pouze v blízkosti zkoumaného subjektu, v době snímání, případně aktivovat přisvit pouze v nočních hodinách či v závislosti na okolních světelných podmínkách. Důležité je také precizní synchronizace místa osvětlení, osvětlení, dle použitého objektivu snímače, kamery – odlišné objektivy se liší ve vzdálenosti ostření a je nutné s touto vlastností počítat při návrhu osvětlení. [30]

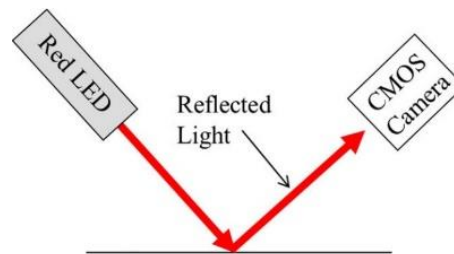
## **4.8 Biometrie v infračerveném spektru, přisvitu**

K biometrickým systémům rozpoznávání obličejů lze využít kromě klasického lidským okem viditelného, světelného spektra také lidským okem infračervené, neviditelné spektrum. Infračervené světelné spektrum má velikou výhodu v tom, že je méně ovlivnitelné přirozeným či umělým světelným zdrojem viditelného světla a z tohoto důvodu umožňuje podávání konzistentnější kvality zachycených snímků ve dne i v noci za přítomnosti tmy. V tomto spektru také dochází k eliminaci stínů a s tím spojených nedostatků. Na toto okem neviditelné spektrum musí být použité kamery, případně senzory či snímače s adekvátní citlivostí použitého infračerveného spektra (vlnovou délkou paprsku). V praxi se také využívá několik druhů infračerveného nasvícení odlišující se vlnovou délkou světelného, infračerveného paprsku. [2] [30] [34]

Princip snímání lidské tváře v tomto spektru spočívá ve snímání rozložení tepla v obličejí. Lidský obličej obsahuje stejně tak, jako ostatní části lidského těla krevní řečiště, cévy, žíly a kapiláry. V těchto oblastech dochází k roznášení kyslíku po celém obličejí prostřednictvím krve. Tato krev má výrazně vyšší teplotu, než okolí krevního řečiště a z tohoto důvodu vyzařuje také více tepla. Přesné tepelné rozložení je možné sledovat kamerami, které umožňují termovizi, tedy přesné zobrazení jednotlivých tepelných oblastí obličejí. Z této metodiky se následně vyvinul samostatný vědní obor nazvaný termografie. Kamery, snímače či senzory zachycující toto tepelné rozložení obličejí jsou velmi citlivé a jsou schopné pracovat v přesnosti až v řádech setin stupně celsia. [2] [34] [35]

Identifikační a verifikační procesy ale využívají princip porovnávání bodů, tvarů a obrazců v tomto spektru. V praxi se častěji využívá snímání infračerveného spektra v monochromatickém zobrazení než v termovizním zobrazení, zejména z důvodu finanční dostupnosti, jednoduchosti a rozšířenosti metod, algoritmů a prostředků využívajících k rozpoznávání obličejů toto zobrazení. Obecný, základní princip je názorně zachycen na obr. 34. Metodika funguje na principu vyslání infračerveného paprsku ze zdroje tohoto záření (IR LED, IR laser či IR lampy/žárovky), jeho odražení od obličeje a následného zachycení senzorem, snímačem či kamerou. Z tohoto zachyceného paprsku dojde k sestavení snímku a tento snímek se následně předává biometrickému systému ke zpracování a následnému vyhodnocení. [2] [31] [36]

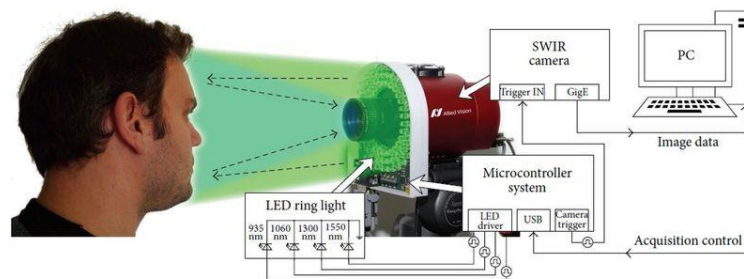
Obrázek 34 - Obecný princip IR snímání



[37]

Detailnější postup je znázorněn na obr. 35, kde je vystižena i komunikace mezi dílčími částmi biometrického systému. V tomto příkladu je využíváno SWIR kamery, tedy kamery, která je citlivá na tzv. short-wave infrared spektrum (krátké vlny IR záření). Na tomto obr. 35 je znázorněna mimo jiné také synchronizace celého systému, prostřednictvím mikrokontroléru, integrovaného obvodu, který zajišťuje synchronizaci IR LED prstence (zdroj IR spektra), snímače kamery (SWIR kamery) a následného odeslání pořízeného snímku k dalšímu zpracování do hlavního systému. [36]

Obrázek 35 - Detailnější postup IR snímání (short-wave IR kamera), vč. synchronizace



[36]



### 4.8.1 Biometrie a infračervené spektrum, přísvit

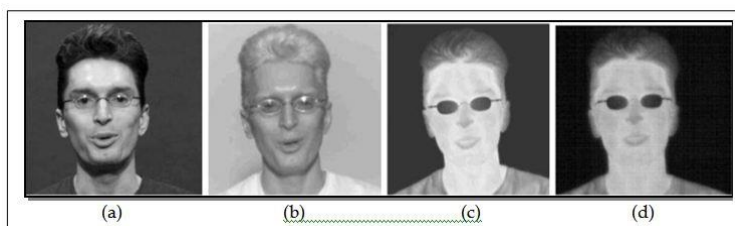
Infračervené záření je druh elektromagnetického záření s vlnovou délkou větší, než je viditelné světlo a zároveň menší než mikrovlnné záření. Frekvence infračerveného záření má rozmezí mezi 300 GHz – 400 THz. Vlnová délka infračerveného záření má rozmezí mezi 760 nm – 1 mm, dle IR záření. [19] [34]

- Blízké infračervené záření (NIR, near infrared, 0,76-1,4  $\mu\text{m}$ )
- IR krátké vlnové délky (SWIR, short-wave infrared, 1,4-3  $\mu\text{m}$ )
- IR střední vlnové délky (MWIR, medium-wave infrared, 3-8  $\mu\text{m}$ )
- IR dlouhé vlnové délky (LWIR, long-wave infrared, 8-15  $\mu\text{m}$ )
- Vzdálené infračervené záření (FIR, far infrared, 15-1000  $\mu\text{m}$ )

[19] [34]

Na obr. 36 je názorně vidět odlišnost zobrazení subjektu při zachycení snímků v odlišném spektru – viditelném a odlišném infračerveném. Na obraze s označením a) je subjekt zachycen ve viditelném spektru (černobílý snímek), s označením b) je subjekt zachycen v SWIR spektru, s označením c) je subjekt zachycen v MWIR spektru a s označením d) je subjekt zachycen v LWIR spektru. Infračervené záření je často považováno za tepelné záření, ale povrch těles zahřívá absorpcí libovolného elektromagnetického záření, infračervené záření ohřívá pouze zhruba z 50 %, zbytek ohřívání zapřičiňuje viditelné spektrum. [19] [34]

Obrázek 36 - Zobrazení obličejů při odlišném IR spektru

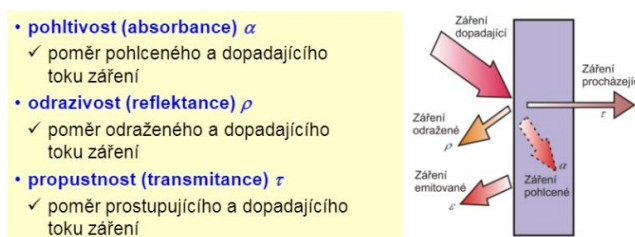


[19]

## 4.8.2 Termografie

Infračervená termografie je vědní obor, který se zabývá analyzováním rozložení tepelného záření na povrchu tělesa, bezkontaktním způsobem. Pro tento proces se využívá termovizních kamer, které dokáží analyzovat infračervenou, vyzařovanou energii a následně jí zobrazit v takové podobě, aby bylo ze snímku čitelné, jakým způsobem je teplo distribuované. Kamery jsou závislé na emisivitě objektů. Emisivita přímo určuje schopnost tělesa vyzařovat teplo. Emisivita je závislá na teplotě objektu, vlnové délce, barvě povrchu, struktuře povrchu a reflektivitě povrchu. Příkladem, kdy je emisivita objektu nižší, je například u lesklých, reflexních a světlých povrchů objektů. Emisivita je blíže názorně zobrazena na obr. 37 i s bližším popsáním jednotlivých dílčích částí záření. Pakliže je tepelná rovnováha, emisivita je v rovnováze s absorpcí (pohltivostí). Pakliže je teplota tělesa vyšší, než je teplota okolí, převažuje vyzařovaná energie (emisivita) nad jejím absorbováním (pohlcováním) a naopak. [2] [35] [38] [39]

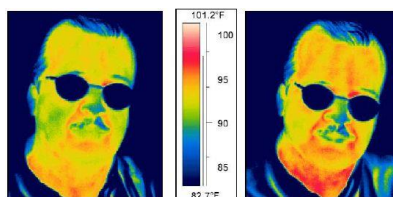
Obrázek 37 - Emisivita



[38]

Výstupem z termokamery bývá snímek, označovaný jako termogram. Na obr. 38 je znázorněn obraz dvou termogramů. Tepelné oblasti jsou vyznačeny příslušnými barvami v závislosti na teplotě. Teplota je vyjádřena ve stupních Fahrenheita. Na levé straně obr. 38 je zachycen subjekt v klidovém stavu, na pravé straně obr. 38 je zachycen subjekt po zalhání. Termovize je velmi přesná a citlivá metodika, díky které lze tedy i takto odhalovat jednotlivé výrazy, emoce či stavy subjektů. Biometrických systémů, které využívají přímo rozpoznávání obličejů na termovizní vizualizaci mnoho není, jelikož je tato metodika velmi nákladná a komplikovaná k realizaci, také má velmi specifické způsoby využití. [2] [35] [38] [39]

Obrázek 38 - Termogram



[35]

### 4.8.3 Zásady při realizaci infračerveného přisvícení

V počátku návrhu celkového řešení biometrického systému je nutné si uvědomit, zda bude systém pracovat v klasickém, okem viditelném spektru či v okem neviditelném, infračerveném spektru. Infračervené spektrum se využívá v případech, kdy není možné nebo vhodné využití klasického viditelného spektra. Následně je také nutné zvážit jaký snímací či kamerový prvek bude využíván k pořizování biometrických vzorků – snímků. Realizace je možná buďto s využitím kamer, které jsou citlivé na použité infračervené spektrum a zároveň mají integrován vlastní přisvit anebo je možná realizace s využitím kamery citlivé na použité infračervené spektrum a samostatného přisvícení adekvátního infračerveného přisvitu. [30] [31] [32] [40]

Při samotné realizaci je důležité dodržování následujících pravidel, která jsou nezbytná pro korektní funkci systému. Důležité je ověření citlivosti všech prvků na požadované infračervené záření. Následně je nezbytné zjistit (a otestovat v praxi), do jaké vzdálenosti je potřebné přisvícení kamery. Tato vzdálenost se může zásadně lišit s ohledem na využívané prostředí systému – otevřenost/uzavřenost prostoru, odrazivost ploch, prostředí či objektů. S ohledem na tento požadavek je nutné volit potřebné prvky s potřebnou citlivostí a dosvitem a pokud je to možné i případné okolní podmínky přizpůsobit tak, aby co nejvíce vyhovovaly danému systému. Velmi důležitým prvkem je také synchronizace/sladění úhlu záběru kamery a úhlu přisvitu. Toto je možné prostřednictvím využití více přisvitů, kombinací, případně s využitím různých modifikátorů úhlu osvětlení. S tímto prvkem také úzce souvisí ostření jednotlivých kamer, které mají odlišné způsoby ostření a je nutné volit takové objektivy, které jsou pro toto spektrum vhodné. Při použití běžného objektivu kamery (pro viditelné spektrum) ve dne s přisvícením pomocí infračerveného světla může dojít k rozostření obrazu. [30] [31] [32] [40]

Velmi důležité je také mít na paměti, že hodnoty udávané výrobcem, zejména parametry dosvitu jsou udávány při konkrétním nastavení citlivosti kamery výrobce, konkrétního objektivu a laboratorních podmínkách testovaného prostředí, tudíž se v praxi mohou více či méně lišit a je nutné dimenzovat systém s určitou rezervou. Černobílé kamery jsou obecně citlivější na infračervené přisvícení ve tmě a jsou obecně o něco více citlivější než kamery barevné. Infračervené přisvícení je možné použít u obecné většiny černobílých kamer, barevné kamery jsou na infračervené přisvícení méně citlivé. Většina barevných kamer není citlivá na infračervené záření a zobrazuje toto záření ve tmě prostřednictvím monochromatického podání barev. [30] [31] [32] [40]

#### 4.8.4 Zdroje infračerveného přísvitu

Mezi nejčastěji využívané zdroje infračerveného světla bývají využívány infračervené LED, infračervené lasery a infračervené lampy/žárovky. Jednotlivé světelné zdroje se od sebe liší způsobem využití, a to vnitřním a venkovním využitím (splnění, například stupně krytí IP65). Mezi hlavní parametry přísvitů bývají zmiňované parametry, jako životnost, vlnová délka záření, vzdálenost dosvitu, úhel dosvitu, výstupní výkon, spotřeba elektrické energie a způsob napájení. Jednotlivé přísvity se od sebe rozlišují také způsobem a tvarem konstrukce osvětlení, zejména jedná-li se o 1 světelný zdroj (1 x IR LED) či více světelných zdrojů (30 x IR LED konstruovaných do prstence). Detaily, jako konstrukce krytu osvitu (kov, plast atd.) a způsob montáže se také může lišit (stojanové, s montáží na stěnu či na strop atd.). [30] [31] [32] [40]

**Infračervené LED** bývají nejčastějším zdrojem tohoto světelného záření. Principiálně se jedná o LED zdroje fungující na stejném principu, jako klasické LED osvětlení, akorát emitující infračervené záření o konkrétní vlnové délce místo viditelného záření. Infračervené LED poskytují vlnovou délku infračerveného paprsku  $\lambda$  od 760 nm a více. Vyráběny jsou nejčastěji z GaAs (gallium a arsen) a AlGaAs (hliník, gallium a arsen). Napětí v propustném směru dosahuje hodnoty až 1,6 V a v závěrném směru hodnoty až 1,9 V. Na obr. 39 je znázorněn příklad přísvitu IR LED. [31]

Obrázek 39 - Přísvit IR LED



[41]

**Infračervené lampy/žárovky** využívají pokrytí povrchu lampy/žárovky infračerveným filtrem, který propouští pouze infračervené spektrum a blokuje viditelné spektrum, jinak jsou konstrukčně totožné, jako klasické lampy/žárovky. Na obr. 40 je znázorněn příklad přísvitu IR lampy/žárovky.

Obrázek 40 - Přísvit IR lampy/žárovky



[42]

**Infračervené lasery** (LASER – Light Amplification by Stimulated Emission of Radiation) jsou optickým zdrojem elektromagnetického záření, světla (v tomto případě zdrojem infračerveného záření). Záření je z laseru vyzařováno ve formě úzkého svazku, na rozdíl od světla přirozených, záření je emitováno ve formě konzistentních fotonů, které tvoří následně ucelený, souvislý paprsek infračerveného záření. Tento zdroj infračerveného záření je využíván pouze pro specializované účely a běžně se k přisvitu nepoužívá. Na obr. 41 je znázorněn příklad přisvitu IR laseru. [43]

*Obrázek 41 - Přisvit IR laser*



[44]

#### **4.8.5 Výhody využití infračerveného spektra přisvitu**

Mezi největší výhody infračerveného spektra pro biometrické systémy patří zejména mnohem nižší ovlivnitelnost kvality snímků na základě viditelného světla. Snímky nebudou do takové míry ovlivněny dnem, nocí, změnou okolního světla, mlhou, deštěm či sněhem. Využití tohoto spektra zajišťuje nativní podporu nočního vidění. Eliminace stínů patří k nedílné součásti související s potlačením vlivu viditelného okolního světla. [31] [30] [32]

V infračerveném spektru je také do jisté míry lepší viditelnost a čitelnost detailů. Kamery využívající toto spektrum mají velmi dobrou citlivost. Infračervené LED přisvity mají obecně velmi dobrou životnost a nízké energetické náklady. Velikou výhodou tohoto osvětlení je také neviditelnost záření lidským okem, tudíž zkoumaný subjekt není rušen žádným zářením, osvětlením obličeje a očí, případně pachatel neví, že je prověřován. [31] [30] [32]

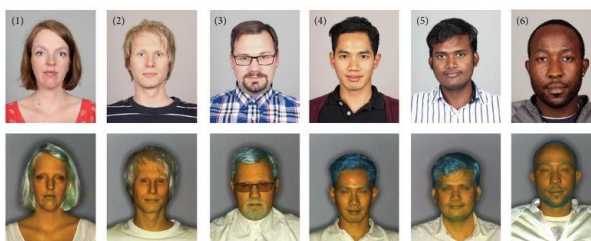
#### **4.8.6 Experimentální metoda rozpoznání lidské kůže v IR spektru**

Biometrické systémy na základě rozpoznání obličeje jsou neustále testovány a vyvíjeny jak z hlediska spolehlivosti, efektivity či rychlosti, ale také z hlediska zabezpečení či schopnosti rozpoznání snahy o obelstění systému. Velkým problémem u určitých systémů bývá možnost obelstění systému na základě vytištěného obrazu obličeje, případně vyrobené masky obličeje či jiného způsobu. Některé systémy jsou více či méně odolné vůči tomuto způsobu obelstění. Jedním ze způsobů zabezpečení vůči obelstění biometrického systému na základě vytisknutého obrazu obličeje, falešné masky či jiného způsobu představuje systém rozpoznání „živé, lidské“ kůže zkoumaného subjektu v infračerveném spektru. [36]

Z vědeckých poznatků bylo zjištěno, že kůže, pokožka není spolehlivě rozpoznatelná ve viditelném spektru na základě různých druhů barvy a odstínů kůže, případně stáří zkoumaného subjektu či zdravotního stavu subjektu. Negativní efekt na spolehlivé rozpoznávání kůže mohou mít vliv někdy také špatné světelné podmínky, při kterých nemohou někdy kamery jednoznačně odlišit barvy, případně odstíny. Odlišné materiály odráží světlo v odlišném množství, intenzitě. Ostatní části světla jsou buďto pohlceny, případně rozptýleny v osvětlovaném materiálu. Každý materiál má více či méně odlišný albedo koeficient (poměr dopadeného a odraženého světla) či reflexní koeficient. Tento koeficient se může výrazně lišit i v závislosti na barvě kůže. V některých situacích nemusí být takzvaný albedo či reflexní koeficient spolehlivým ukazatelem při rozpoznání kůže. Ostatní materiály jako maso, kůže či dřevo mohou mít v určitých situacích velmi podobné albedo hodnoty a mohou být zaměnitelné. Z tohoto důvodu nemůže být hodnota albedo brána jako spolehlivá při rozpoznání kůže ve viditelném spektru. [36]

Pakliže se ale změní viditelné spektrum na infračervené spektrum, proces rozpoznání „živé“ kůže subjektu je velmi spolehlivý. K tomuto rozpoznání se využívá SWIR spektrum (krátké vlnové délky). Díky velkému obsahu vody v kůži se ve SWIR spektru albedo hodnoty kůže dostatečně odlišují od ostatních objektů a již nejsou jednoduše zaměnitelné. Albedo hodnoty se odlišují od ostatních materiálů nyní v takové míře, že je možné jednoznačně rozpoznat živý obličej mezi ostatními objekty na scéně na základě kůže a zároveň odhalit pokus o obelstění systému. Bylo zjištěno, že při vlnových délkách nad 900 nm, pigmenty kůže již nehrají roli v hodnotách albedo a kůži lze bezpečně rozpoznat (bez rozdílu barvy pleti). Dříve ovlivňující faktory jako věk, typ kůže, etnicita, rasa, pohlaví či zdravotní stav, již nehrají roli ve spolehlivém rozpoznání kůže mezi ostatními objekty. V procesu rozpoznání kůže mezi ostatními objekty se kůže nyní vizualizuje pouze jednou, totožnou barvou (hnědou). Toto zobrazení je znázorněno na obr. 42. [36]

*Obrázek 42 - Rozpoznání živé kůže*



[36]

## **5 Praktická část práce**

V praktické části práce se nachází kapitoly použitá zařízení, kde jsou popsány všechna použitá zařízení v práci. V části věnovanému postupu měření se nachází zevrubně popsáný proces celého měření, následně se zde nachází i bodové shrnutí jednotlivých kroků, postup jednotlivých registrací na čtečkách a všechna opatření, která byla provedena. V kapitole měřené hodnoty – příklad záznamu z měření se nachází hodnoty, které byly měřeny a zaznamenávány při testování a také popis jednotlivých stavů, které mohly při měření nastat.

### **5.1 Použitá zařízení**

V této kapitole se nachází všechna zařízení, která byla v průběhu práce a procesu měření využita. Nachází se zde jejich zevrubný popis i případný způsob využití a také pracovní podmínky, které jsou stanovené výrobcem biometrických čteček.

### 5.1.1 Čtečka č.1 – iFace 302

Biometrická čtečka iFace 302 je od výrobce ZKTeco. Jedná se o multifunkční biometrický sken, který obsahuje biometrický sken obličeje a sken otisků prstů. Čtečka umožňuje funkci identifikace (1:N) i verifikace (1:1). Zařízení je vybaveno procesorem o frekvenci 800 Mhz, TFT dotykovým LCD displejem o velikosti 4,3", 2000 mAh záložní baterií (využití v případě výpadku stálé elektrické energie z napájecí sítě), kamerou s podporou NIR (near infrared, blízké IR záření), přísvitem v podobě IR LED – využívá v případě zhoršených světelných podmínek. Kapacita čtečky je 1200 obličejových šablon, případně 2000 šablon otisků prstů. Algoritmus obličejové biometrie je nazýván ZKFace VX 10.0 a jedná se o metodu rozpoznávání obličejů na základě markantů. Algoritmus biometrie otisku prstů se nazývá ZKFinger VX 10.0. Konektivita čtečky je zajištěna prostřednictvím sběrnice ethernetu TCP/IP, případně RS232/485. Zařízení disponuje také bezdrátovými komunikačními moduly a zajišťuje podporu standardů SMS, GPRS, 3G či Wi-Fi. Správa a administrace je také možná prostřednictvím počítače. Napájení čtečky vyžaduje napětí 12 V a proud 3A. Biometrická čtečka podporuje identifikaci i osob s brýlemi. Čtečka má plnou podporu českého jazyka. Provozní podmínky použití stanovené výrobcem jsou 0-45°C, 0-800 lx, vlhkost 20-80 %, výška montáže zařízení 120 cm, vzdálenost od čtečky 30-80 cm. Čtečka iFace 302 je zobrazena na obr. 43. [45] [46]

Obrázek 43 - Biometrická čtečka - iFace 302



[45]



## 5.1.2 Čtečka č.2 – Multibio 700

Biometrická čtečka Multibio 700 je od stejnojmenného výrobce ZKTeco. Jedná se také o multifunkční biometrický sken, který obsahuje biometrický sken obličeje a sken otisků prstů. Čtečka umožňuje funkci identifikace (1:N) i verifikace (1:1). Zařízení je vybaveno 32bit procesorem o frekvenci 630 Mhz, TFT dotykovým LCD displejem o velikosti 3", kamerou s vysokým rozlišením a podporou NIR (near infrared, blízké IR záření), přísvitem v podobě IR LED – využívá v případě zhoršených světelných podmínek. Kapacita čtečky je 1500 obličejových šablon, případně 2000 šablon otisků prstů. Algoritmus obličejové biometrie je nazýván ZKFace VX 7.0 a jedná se o metodu rozpoznávání obličejů na základě markantů. Algoritmus biometrie otisku prstů se nazývá ZKFinger VX 10.0. Konektivita čtečky je zajištěna prostřednictvím sběrnice ethernetu TCP/IP, případně RS232/485. Čtečka podporuje také USB konektivitu. Správa a administrace je také možná prostřednictvím počítače. Napájení čtečky vyžaduje napětí 12 V a proud 3A. Biometrická čtečka podporuje identifikaci i osob s brýlemi. Čtečka má plnou podporu českého jazyka. Provozní podmínky použití jsou totožné jako s předchozí čtečkou, stanovené výrobcem jsou 0-45°C, 0-800 lx, vlhkost 20-80 %, výška montáže zařízení 120 cm, vzdálenost od čtečky 30-80 cm. Čtečka Multibio 700 je zobrazena na obr. 44. [47] [48] [49]

Obrázek 44 - Biometrická čtečka - Multibio 700



[47]

### 5.1.3 Čtečka č.3 – AccuFace EFR-T1

Biometrická čtečka AccuFace EFR-T1 je od výrobce PSPsecurity. Jedná se o čtečku zaměřenou pouze na rozpoznávání obličejů. Čtečka disponuje opět dvěma módy – identifikace (1:N) a verifikace (1:1). Čtečka disponuje kapacitou pro 300 obličejových šablon v módu identifikace a kapacitou 1000 obličejových šablon v módu verifikace. Verifikace je řešená prostřednictvím RFID karty či PIN kódu. Komunikace čtečky je zajištěna prostřednictvím sběrnic ethernet protokolu TCP/IP, dále sběrnic RS232/485, anebo prostřednictvím bezdrátové komunikace prostřednictvím Wi-Fi konektivity. Čtečka podporuje také mobilní telefony a je možné ji spravovat prostřednictvím aplikací na platformách iOS (iPhone) či na platformách Android. Ovládání a správa čtečky je možná dvěma způsoby – prostřednictvím počítače, případně v módu „standalone“ (bez počítače) - prostřednictvím dálkového ovladače. Zařízení pracuje téměř výhradně v NIR režimu. Biometrická čtečka podporuje identifikaci i osob s brýlemi. Čtečka nepodporuje český jazyk. Výrobce udává rychlost identifikace do 1 sekundy. Provozní podmínky použití stanovené výrobcem jsou 0-50°C, 0-8000 lx, výška montáže zařízení 110-120 cm, vzdálenost od čtečky 30-80 cm. Napájení čtečky je zajištěno napětím 12 V a proudem 1,2A. Čtečka AccuFace EFR-T1 je zobrazena na obr. 45. [50] [51] [52]

Obrázek 45 - Biometrická čtečka - AccuFace EFR-T1



[50]

#### 5.1.4 Čtečka č.4 – Aktion AFT-500

Biometrická čtečka Aktion AFT-500 je od výrobce Aktion. Jedná se o biometrickou čtečku obličejů podporující identifikaci (1:N) i verifikaci (1:1). Metoda verifikace je možná s kombinací RFID karty/čipu, případně PIN kódu. Procesor čtečky má frekvenci 600 Mhz. Zařízení disponuje TFT displejem o velikosti 3,5" a kapacitní dotykovou klávesnicí o velikosti počtu dotykových ploch 4x4. Kapacita čtečky je 500 osob, případně prostřednictvím rozšíření až 1400 osob. Čtečka využívá kamery s vysokým rozlišením a také citlivostí na NIR, v horších světelných podmínkách využívá čtečka NIR přísvit. Biometrická čtečka nepodporuje identifikaci osob s brýlemi, při identifikaci/verifikaci je vždy nutné brýle odložit po dobu rozpoznávání uživatele. Biometrická čtečka plně podporuje český jazyk. Komunikace čtečky je zajištěna prostřednictvím ethernetu. Čtečka podporuje také rozhraní USB a vyměnitelné paměťové SD karty o kapacitě až 4 GB. Správa a administrace je také možná prostřednictvím počítače. Výrobce udává rychlost identifikace osoby do 1 sekundy, pakliže je v čtečce uloženo do 500 obličejových šablon. Provozní podmínky použití stanovené výrobcem jsou 0-40°C, 0-8000 lx, výška montáže zařízení 110-120 cm, vzdálenost od čtečky 30-80 cm. Napájení čtečky je zajištěno napětím 12 V a proudem 0,5 A. Čtečka Aktion AFT-500 je zobrazena na obr. 46. [53] [54]

Obrázek 46 - Biometrická čtečka - Aktion AFT-500



[53]

### 5.1.5 Luxmetr – CEM-DT 8809A

Luxmetr je měřicí přístroj, který slouží k měření intenzity osvětlení (osvětlenosti), případně svítivosti. Jednotkou intenzity osvětlení je lux (lx) - jedná se o odvozenou jednotku ze soustavy SI, jednotkou svítivosti je candela (cd) – jedná se o základní jednotku soustavy SI. Intenzita osvětlení (E) je vyjádřena jako poměr dopadajícího světla (v lumenech) na jednotku plochy ( $1\text{lx}=1\text{lm}/1\text{m}^2$ ). Svítivost (I) je vyjádřena jako poměr světelného toku ( $\Phi$ ) vyzářeného zdrojem v určitém směru do prostorového úhlu ( $\Omega$ ), steradiánu. Luxmetr obsahuje fotočlánek (v tomto případě fotodiody), měřicí systém a vyhodnocovací systém. Fotočlánek slouží jako přijímač světla a v závislosti na míře přijatého světla následně generuje fotoproud. Výsledný fotoproud je následně měřen a vyhodnocován luxmetrem. Na obr. 47 je fotografie použitého luxmetru, modelu CEM-DT 8809A. [55] [56] [57] [7]

Obrázek 47 – Luxmetr, CEM-DT 8809A



Jedná se o profesionální luxmetr s LCD displejem. Nepřesnost luxmetru výrobce udává 5 %. Luxmetr obsahuje dva režimy měření – intenzity osvětlení (lx) a svítivosti (cd). Přístroj obsahuje také možnost změny rozsahu měření intenzity osvětlení v rozmezí 0,1 - 400 000 lx a také funkci upozornění na překročení rozsahu. Rozsah je možno nastavit na následující stupně – 400 lx, 4000 lx, 40 000 lx a 400 000 lx. Luxmetr byl manuálně nastaven v procesu měření na pevný rozsah 4000 lx. Luxmetr obsahuje také funkci automatického přizpůsobení rozsahu přístroje. Fotočlen luxmetru snímá až 1.5x za sekundu a obsahuje vysoce zátěžovou, odolnou fotodiodu na bázi křemíku. Zařízení je napájeno 9 V baterií a také obsahuje USB port pro snadné spárování s počítačem a příslušný software dodávaný výrobcem. [58] [59]

## 5.1.6 Přísvit – LED RGB pásek

Přísvit biometrických čteček byl realizován prostřednictvím šesti pásků obsahující RGB LED osvětlení. Tento světelný pásek se skládá z 30 vysoce svítících RGB LED (s označením 5050) na metr. Příkon jednoho světelného pásku je 7,2 W/metr. Pásek je dělitelný po 10 cm úsecích, které jsou předem perforované. V každé RGB LED se nachází 3 čipy – červený (R), zelený (G) a modrý (B). Vzájemným mísením jednotlivých barevných složek dochází k vytvoření požadované barvy. Pásek obsahuje 4 fyzické vývody, 3 vývody pro jednotlivé barevné složky (regulací napětí dochází k mísení jednotlivých barev) a dle provedení pásku buďto společnou anodu nebo katodu. Napájení přísvitu je realizováno prostřednictvím externího stejnosměrného zdroje napětí o hodnotě 12 V. Přísvit je zobrazen na obr. 48. [60] [61]

Dálkový ovladač obsahuje 44 tlačítek, prostřednictvím kterých lze komfortně ovládat jednotlivé barvy přísvitu, jejich intenzitu či zapínat/vypínat světelné efekty. Pásek je možné ovládat prostřednictvím dálkového ovladače, který komunikuje prostřednictvím IR čidla dostupným na ovládacím členu přísvitu. Na obr. 49 a) je zobrazen dálkový ovladač a na obr. 49 b) je zobrazeno IR čidlo s ovládací napájecí jednotkou. [60]

Obrázek 48 - Přísvit - LED RGB pásek



[62]

Obrázek 49 a) dálkový ovladač přísvitu b) IR čidlo dálkového ovladače



## 5.2 Postup měření

Pro zajištění objektivitu celého měření bylo nutné zajistit, pokud možno totožné, případně co nejvíce totožné - v rámci možností, výchozí, laboratorní podmínky pro všechny testované biometrické čtečky a testované subjekty. S ohledem na výše zmíněné hledisko objektivitu byla vybrána laboratoř, která splňovala podmínky potřebné k zajištění stejných podmínek k měření na všech dostupných biometrických čtečkách.

Biometrické čtečky použité k měření byly vybrány na základě průzkumu nepoužívanějších biometrických čteček v ČR. Tento průzkum byl uskutečněn Ing. Veronikou Hartovou, Ph.D., ve spolupráci s firmami zabývajícími se zabezpečovacími systémy. Průzkum byl uskutečněn v roce 2014 a zúčastnilo se ho přes 500 firem, společností a státních institucí. [63]

Tyto biometrické čtečky, které byly vybrány, byly označeny následujícím označením č.1 – iFace 302, č.2 – Multibio 700, č.3 – AccuFace EFR-T1 a č.4 – Aktion AFT-500. Čtečky č.1 a č.2 jsou si podobné použitým algoritmem a vyvíjející společností (ZKTeco), jedná se o starší čtečky. Čtečky č.3 a č.4 jsou novějšího charakteru a vyvíjející společnosti se nazývají PSPsecurity (č. 3) a Aktion (č.4).

Laboratoř se nachází v areálu Technické fakulty ČZU v Praze. Laboratoř disponuje bílými stěnami, bez rušivých elementů. V úrovni snímané tváře testovaného subjektu nebyly přítomny žádné jiné rušivé objekty. Toto konzistentní, bílé, nerušivé pozadí zajišťuje totožné záhlaví pro všechny biometrické snímky a skeny testovaných subjektů a zároveň umožňuje rovnoměrnou distribuci světelných odrazů od přítomných stěn. V testovacích podmínkách byla dodržena standardní laboratorní teplota místnosti 20°C.

Velmi důležitým aspektem při měření biometrických čteček bylo nutné dodržení obdobných světelných podmínek, ze kterých vycházelo měření. Umístění biometrických čteček bylo zvoleno 3 metry od protějšího okna s ohledem na doporučení výrobců čteček. Intenzita osvětlení denního světla místnosti byla měřena profesionálním luxmetrem CEM-DT 8809A. V místnosti se nacházela 3 prosklená okna, skrz které procházelo denní přirozené světlo do laboratoře, které bylo následně zregulováno. Pracovní, světelný rozsah použitých biometrických čteček udávanými výrobci čteček byl odlišný. Čtečky iFace 302 a Multibio 700 mají doporučený pracovní rozsah 0-800 luxů, kdežto čtečky AccuFace EFR-T1 a Aktion AFT-500 mají doporučený pracovní rozsah 0-8000 luxů. Z těchto pracovních rozsahů bylo nutné vybrat nejhorší možný pracovní scénář, který teoreticky může nastat a zároveň, který bude v pracovní úrovni všech užitých čteček, aby byly hodnoty porovnatelné. Na tomto základě byl zvolen rozsah 0-100 luxů výchozího, přirozeného světla v místnosti.

Z tohoto důvodu bylo nutné následně regulovat míru průchodu tohoto denního světla skrz okna do místnosti, aby byl dodržen stanovený, výchozí rozsah. Průměrná hodnota výchozího, denního světla byla 76 luxů.

Při měření okolního denního světla místnosti prostřednictvím luxmetru CEM-DT 8809A bylo nutné nastavit nejdříve rozsah na hodnotu 4000 lx. Měřicí hlavici luxmetru bylo nezbytné následně přivést na úroveň hlavy testovaného subjektu a vytrvat zhruba 10-15 sekund, alespoň do částečného ustálení hodnot. Výchozí podmínky musí být v mezi 0-100 lx denního osvitů obličej. Pakliže tyto podmínky nebyly vyhovující, bylo potřebné provést výše zmíněnou regulaci okolního denního světla a měření zopakovat. Po změření okolního denního světla v místnosti následovalo změření jednotlivých přísvitů, v odlišných barevných spektrech.

Samotný přísvit byl realizován prostřednictvím šesti RGB LED pásků, napájených nominálním, stejnosměrným napětím 12 V. RGB LED pásky byly umístěny na vrcholu laboratorního panelu. Umístění přísvitu je blíže znázorněno na obr. 50 a způsob osvitů obličej je blíže znázorněn na obr. 51. RGB LED pásky byly zvoleny zejména z důvodu možnosti jednoduché a rychlé volby barevného spektra přísvitu a volby vyzařovaného výkonu osvitů. Přísvit v podobě LED bývá také nejčastější formou přísvitu. RGB LED pásek je schopný vytvořit až 16 odlišných barev a odstínů. Z množství dostupných barev a odstínů bylo nutné učinit výběr takových barevných spekter, ve kterých bylo zastoupeno dostatečně odlišné spektrum svou vlnovou délkou ( $\lambda$ ) a frekvencí ( $f$ ).

Barevné odstíny přísvitu byly vybrány v základních odstínech RGB a bílé, jelikož se jedná o dostatečně rozdílná spektra svou vlnovou délkou a frekvencí. Biometrické čtečky byly testovány v barevných spektrech R – red, červená – dlouhá vlnová délka, nízká frekvence ( $\lambda=625-740$  nm,  $f=480-405$  Thz), G – green, zelená – průměrná vlnová délka, průměrná frekvence ( $\lambda=520-565$  nm,  $f=580-530$  Thz) a B – blue, modrá – krátká vlnová délka, vysoká frekvence ( $\lambda=430-500$  nm,  $f=700-600$  Thz). Výkon jednotlivých RGB LED pásků byl možný stupňovat na stupnici od 1 (nejnižší) do 10 (nejvyšší). Pro zachování stejných podmínek byl výkon pro všechna měření nastaven na stupeň 10 a při tomto nastaveném výkonu docházelo ke změně barevného spektra. Jednotlivé osvitů tváře užitých barevných spekter byly následně opět změřeny luxmetrem a byly zjištěny následující průměrné hodnoty jednotlivých barevných osvitů tváře – R (red, červená) 328 lx, G (green, zelená) 478 lx, B (blue, modrá) 453 lx a W (white, bílá) 850 lx. Hodnoty byly také do jisté míry ovlivněny luxmetrem, jelikož luxmetr je dimenzován na klasické, bílé, okolní, denní světlo.

Po zajištění potřebných světelných podmínek měření a zaznamenání hodnot jednotlivých přísvitů bylo přistoupeno k registraci subjektu do jednotlivých biometrických čteček. Po úspěšném zaregistrování uživatele do všech čtyřech biometrických čteček a otestování korektnosti zaregistrování a funkčnosti čteček bylo přistoupeno k vysvětlení způsobu přístupu měření subjektu (zaclonění čtečky, vyčkání do ustálení čtečky, přistoupení ke čtečce).

Kamerový systém čtečky se před každým měřením zaclonil (clonkou) a bylo vyčkáno do ustálení čtečky do výchozího stavu. Následně bylo provedeno přistoupení ke čtečce ze strany (nakloněním) v požadovaném místě a vzdálenosti, aby byl do jisté míry simulován pohyb ke čtečce, jako v praxi. Tento pohyb a následné měření bylo opakováno 10x pro každý jednotlivý pokus – pro měření bez přísvitů, pro měření v jednotlivých barevných spektrech (červené, zelené, modré, bílé).

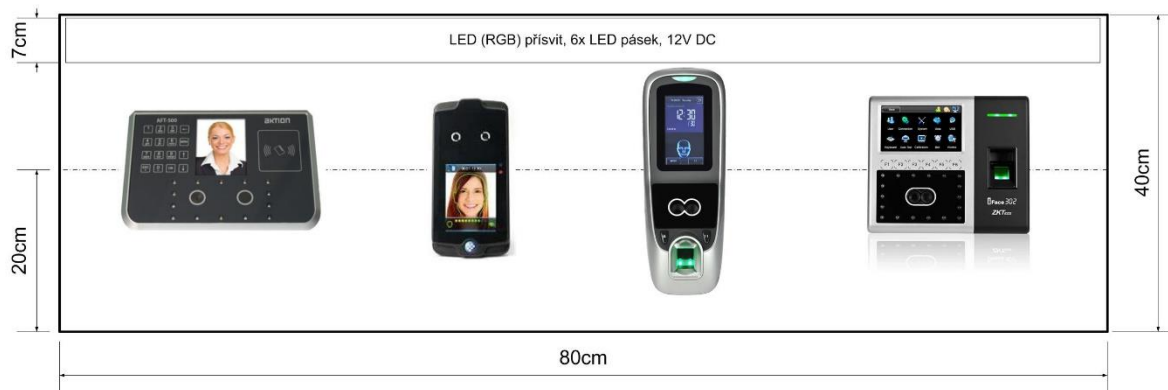
Velmi důležitým prvkem měření bylo stanovení maximální hodnoty délky času ponechání čtečky k identifikaci uživatele v podmínkách bez přísvitů i v podmínkách přísvitů. Tato hodnota byla stanovena na 30 sekund. Jestliže došlo k překročení této doby, byl tento identifikační pokus vyhodnocen jako nevyhovující – osoba neidentifikována (falešné odmítnutí uživatele) a pokus ukončen. Při procesu vyhodnocování procentuální spolehlivosti identifikace byly následně brány v potaz dvě omezující hodnoty a to 10 sekund (benevolentnější varianta) a 5 sekund (přísnější varianta), u novějších čteček hodnota 3s a 2s. V dnešní době dosahují moderní biometrické čtečky, dle specifikací výrobce, velmi rychlých časů vyhodnocení – hodnota se samozřejmě liší, dle čtečky, ale většinou se tato hodnota pohybuje rámcově kolem 1-2 sekundy.

Při měření byly použity 2 čtečky zcela nové, u kterých výrobce specifikuje dobu vyhodnocení kolem 1-2 sekundy (AccuFace EFR-T1 a Aktion AFT-500) a 2 čtečky starší, u kterých výrobce nspecifikuje dobu vyhodnocení (iFace 302 a Multibio 700).

Umístění všech čtyř biometrických čteček bylo zajištěno s ohledem na podmínky výrobce. Čtečky mají být instalovány do výšky v rozmezí 110-120 cm. Všechny čtečky byly namontovány do stejné výšky, na jednotný testovací panel, který byl určen k měření. Tento testovací panel s instalovanými biometrickými čtečkami je schematicky znázorněn na obr. 50. Panel disponuje rozměry 80 x 40 cm, čtečky byly instalovány do jednotné výšky.



Obrázek 50 - Schematické znázornění laboratorního panelu

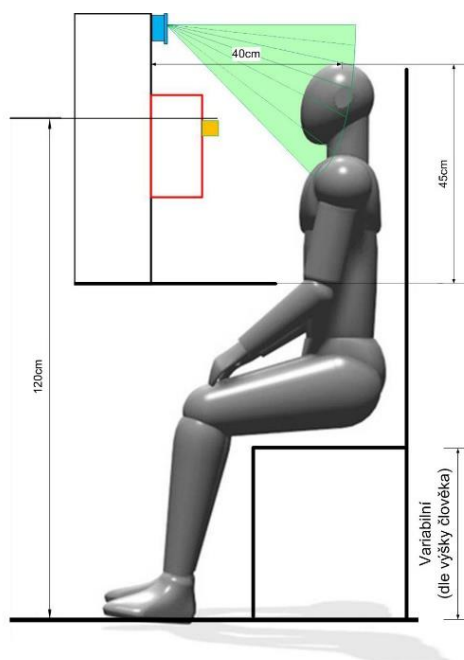


[45] [47] [50] [53]

Všechny čtečky byly instalovány do výšky 120 cm, dle doporučení výrobce. Vzdálenost subjektu mezi čtečkou a testovaným subjektem je výrobcí stanovena na rozmezí 30-80 cm. Výsledná vzdálenost subjektů mezi čtečkou a subjektem v laboratorním prostředí byla 40 cm. Schematické znázornění měření z profilu je znázorněno na obr. 51.

Velmi důležitým krokem u měření bylo také korektní přizpůsobení pozice testovaného subjektu vzhledem k pozici biometrické čtečky. Tento krok byl realizován prostřednictvím nastavitelné úrovně výšky testovacího křesla a přizpůsobením vzdálenosti křesla od čtečky, aby byly dodrženy obdobné podmínky u všech subjektů.

Obrázek 51 - Schematické znázornění měření z profilu



[64]

Měření bylo realizováno v průběhu semestru a testovanými subjekty byli studenti a pracovníci Technické fakulty ČZU v Praze. Měření bylo relativně časově náročné a měření jednoho subjektu trvalo průměrně mezi 60-75 minutami. Měření se zúčastnilo celkem 11 subjektů a s každým subjektem byla provedena série měření na všech čtyřech biometrických čtečkách. Samotnému měření předcházelo měření hodnot denního, okolního světla v místnosti (případná regulace) a následně osvětlení obličejů při jednotlivých barevných spektrech. Následně byla realizována registrace uživatelů (enrollment) do jednotlivých čteček.

Samotné měření se skládalo ze 4 částí (4 čtečky) a 5 dílčích částí (bez přísvitu, s červeným přísvitem, se zeleným přísvitem, s modrým přísvitem a s bílým přísvitem). V každém spektru bylo provedeno 10 opakujících se měření. Při procesu měření byly zaznamenávány jednotlivé časy – doby identifikace a případná falešná odmítnutí či falešná přijetí. Z těchto měření bylo následně celkem získáno 2200 naměřených hodnot a následně vyhodnoceno (4 (čtečky) x 5 (spekter) x 10 (opakování) x 11 (subjektů) = 2200 hodnot). Při měření mohlo dojít k následujícím vyhodnocujícím stavům.

### 5.2.1 Vyhodnocovací stavy

**Stav korektní identifikace** – Jedná se o vyžadovaný stav. Identifikace probíhá ve vymezeném čase a rozpoznání uživatele je korektní.

**Stav falešného odmítnutí (FRR)** – Nedochozí k identifikaci, rozpoznání uživatele. K tomuto stavu dochází, když je skóre naměřeného subjektu příliš nízké a nedochází tak ke korektnímu ztotožnění aktuálního uživatele s uloženým uživatelem v databázi systému.

Tato hodnota byla při měření zaznamenána v případě, kdy nedošlo ke korektní identifikaci uživatele do 30 sekund. Při vyhodnocování výsledků je následně tato hodnota ještě zohledňována v odlišném přístupu tolerance k identifikaci na základě doby identifikace (10s – benevolentnější varianta, 5s – přísnější varianta u starších čteček a 3s, 2s u novějších čteček).

**Stav falešného přijetí (FAR)** – Jedná se o stav, kdy dochází k záměně identifikovaného uživatele za jiného – jedná se o nevyžádaný stav, který silně snižuje bezpečnost celého systému.

## 5.2.2 Bodový souhrn jednotlivých kroků měření

1. Korektní přizpůsobení pozice subjektu (nastavení výšky a vzdálenosti subjektu)
2. Změření okolního, denního světla luxmetrem v laboratorní místnosti
3. Regulace (případná) denního světla v místnosti na stanovenou výchozí mez (0-100 lx)
4. Změření osvitů obličeje v jednotlivých barevných spektrech luxmetrem
5. Registrace (enrollment) uživatele do všech čtyř biometrických čteček
6. Otestování korektního zaregistrování uživatele v jednotlivých čtečkách
7. Měření na biometrické čtečce č.1 v prostředí – bez přísvitu 10x, v přísvitu R (červeném) 10x, v G (zeleném) 10x, v B (modrém) 10x a v W (bílém) 10x.
8. Měření na biometrické čtečce č.2 v prostředí – bez přísvitu 10x, v přísvitu R (červeném) 10x, v G (zeleném) 10x, v B (modrém) 10x a v W (bílém) 10x.
9. Měření na biometrické čtečce č.3 v prostředí – bez přísvitu 10x, v přísvitu R (červeném) 10x, v G (zeleném) 10x, v B (modrém) 10x a v W (bílém) 10x.
10. Měření na biometrické čtečce č.4 v prostředí – bez přísvitu 10x, v přísvitu R (červeném) 10x, v G (zeleném) 10x, v B (modrém) 10x a v W (bílém) 10x.

## 5.2.3 Registrace nových uživatelů u čtečky iFace 302 a Multibio 700

Postup registrace u biometrické čtečky č.1 (iFace 302) a č.2 (Multibio 700) je velmi podobný, jelikož se jedná o systémy, které jsou vyvíjeny totožnou firmou (ZKTeco) a využívají obdobné algoritmy (v jiných verzích) a podobné operační systémy. Celé uživatelské prostředí je v grafické podobě a obsahuje kompletně českou lokalizaci.

### Shrnuté kroky k registraci nového uživatele do čtečky č.1 a č.2:

1. Provést autentizaci do systému z pozice administrátora
2. Zvolit záložku MENU, provést potvrzující, opětovnou autentizaci z pozice administrátora
3. Zvolit volbu Přidat nového uživatele
4. Zavést identifikační údaje uživatele do systému (jméno, identifikační číslo)
5. Zahájit sken obličeje, případně sken otisku prstu
6. Dodržet požadované instrukce čtečky v procesu skenu
  - a. Pohled přímý
  - b. Pohled mírně vlevo
  - c. Pohled mírně vpravo
  - d. Pohled do kamery
7. Uložit uživatele do systému
8. Otestovat uživatele, zda byl korektně přidán do systému, případně proces opakovat

## 5.2.4 Registrace nových uživatelů u čtečky AccuFace EFR-T1

Postup registrace u biometrické čtečky č.3 (AccuFace EFR-T1) se provádí buďto prostřednictvím síťového přístupu (prostřednictvím PC a propojením pomocí sběrnice ethernet) nebo prostřednictvím tzv. standalone módu (soběstačného módu) a pomocí dálkového IR ovladače. Registrace prostřednictvím standalone módu probíhá prostřednictvím textového, černobílého, uživatelského prostředí, které není dostupné v české lokalizaci. Potvrzení se provádí na dálkovém ovladači stisknutím znaku \* a smazání, případně zrušení se provádí na dálkovém ovladači stisknutím znaku #.

### Shrnuté kroky k registraci nového uživatele do čtečky č.3:

1. Provést autentizaci do systému z pozice administrátora
  - a. Prostřednictvím dálkového IR ovladače zmáčknout klávesovou sekvenci znaků 1-2-3-4-\*
  - b. Provést autentizaci administrátora prostřednictvím obličeje
2. Zvolit záložku s označením User (volba 3\*)
3. Zvolit záložku s označením Enroll (2\*)
4. Zvolit záložku s označením Input User ID (číslo\*)
5. Zvolit záložku (dle privilegií uživatele) s označením (1\* - normal user, 2\* - root user)
6. Zvolit záložku s příslušným označením, zda uživatel nosí brýle (1\*- ano, 2\* - ne)
7. Zvolit hodnotu, dle patřičného zařazení uživatele do skupiny (rozsah 1-9), (číslo\*)
8. Dodržet požadované instrukce čtečky v procesu skenu
  - a. Přímý pohled
  - b. V případě, že uživatel je nositelem brýlí, v polovině skenovacího procesu bude čtečkou vyžádán o odložení brýlí
9. Uložení uživatele do systému
10. Otestovat uživatele, zda byl korektně přidán do systému, případně proces opakovat

## 5.2.5 Registrace nových uživatelů u čtečky Aktion AFT-500

Postup registrace u biometrické čtečky č.4 (Aktion AFT-500) se provádí opět buďto prostřednictvím síťového přístupu (prostřednictvím PC a propojením pomocí sběrnice ethernet) nebo prostřednictvím lokálního, zjednodušeného menu, dostupného přímo na čtečce. Volba jednotlivých možností probíhá prostřednictvím dotykové klávesnice na terminálu obsahující 4x4 klávesy. Pohyb v menu je realizován prostřednictvím šipek (nahoru, dolů) a potvrzení tlačítkem OK, případně zrušení, smazání tlačítkem ESC. Psaní je realizováno prostřednictvím metody T9, které je známé zejména ze starších mobilních telefonů. Celé uživatelské prostředí je v textové, barevné podobě a je dostupné kompletně v české lokalizaci.

### Shrnuté kroky k registraci nového uživatele do čtečky č.4:

1. Provést autentizaci do systému z pozice administrátora
  - a. Prostřednictvím dotykové klávesnice na terminálu zvolit položku MENU
  - b. Provést autentizaci administrátora prostřednictvím obličeje
2. Zvolit z nabídky záložku Správa osob (potvrdit OK)
3. Zavést identifikační jméno uživatele do systému (potvrdit OK)
4. Zavést identifikační číslo uživatele do systému (potvrdit OK)
5. Zahájit skenování obličeje
  - a. Uživatelé, kteří jsou nositeli brýlí musí po celý proces registrace i identifikace odložit brýle. Čtečka nepodporuje brýle.
  - b. Přímý pohled
6. Uložení uživatele do systému
7. Otestovat uživatele, zda byl korektně přidán do systému, případně proces opakovat

### 5.3 Měřené hodnoty – příklad záznamu z měření

Při měření, které bylo realizováno na 11 testovaných subjektech byl prováděn záznam z měření, který byl rozdělen do následujících 4 tabulek. Tyto tabulky byly rozdělené dle biometrické čtečky, na které bylo prováděno aktuální měření. Každá tabulka obsahovala 10 řádků – dle 10 opakovaných měření na každé použité spektrum. V tabulce se nacházelo 5 sloupců, kde každý sloupec odpovídal použitému spektru přísvitu – bez přísvitu, v červeném, v zeleném, v modrém a v bílém přísvitu. Celkový počet zaznamenaných hodnot byl 200 na jeden testovaný subjekt (4 čtečky x 5 spekter x 10 opakování = 200).

Do tabulky byl zaznamenáván čas identifikace, který byl pořízen digitálními stopkami. Čas v tabulce je udáván v sekundách. Následně byly spočítány průměrné časy identifikace v jednotlivých spektrech přísvitu. Příklad záznamu z měření je zobrazen v tabulkách číslo 3, 4, 5 a 6. V těchto tabulkách se nachází záznam z měření jednoho subjektu.

Hodnota, která v tabulce odpovídá 30 sekundám (30:00s) byla stanovena jako horní mez času identifikace. Pakliže testovaný subjekt nebyl rozpoznán do 30s, byl tento pokus vyhodnocen jako neidentifikování subjektu – falešné odmítnutí subjektu. Tato hodnota falešného odmítnutí subjektu byla následně využita ve výsledném vypočítání hodnoty FRR – false rejection rate (míra falešného odmítnutí). Tato maximální časová hranice (časové rozmezí pro identifikaci) byla následně posunována, měněna pro zjištění, v jakých časových hranicích jednotlivé čtečky dosahují spolehlivosti, jakou mírou spolehlivosti disponují jednotlivé čtečky (starší a novější) v hranici 10s, 5s a novější v hranici 2s (dle specifikací výrobce).

Na základě stanovení této meze hranice bylo následně z naměřených hodnot spočítáno, v kolika případech jednotlivé čtečky v konkrétních spektrech vyhověly zadání (identifikace do 10s a do 5s u starších čteček a do 3s a 2s u novějších čteček). Na tomto základě byla následně spočtena hodnota FRR, která určuje míru spolehlivosti jednotlivých biometrických čteček. Míra spolehlivosti FRR byla počítána následujícím vztahem.

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

$N_{FR}$  = počet chybných odmítnutí

$N_{EIA}$  = počet pokusů oprávněných osob o identifikaci

Tabulka 3 - Hodnoty z měření jednoho testovaného subjektu na č. iFace 302

č.1 - iFace 302					
Číslo měření	bez přívitu	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
	[s]	[s]	[s]	[s]	[s]
1.	30:00	5:10	8:65	3:57	30:00
2.	30:00	4:79	3:20	4:02	6:16
3.	7:70	3:05	3:86	3:84	5:45
4.	5:13	4:22	4:20	3:26	7:06
5.	4:14	5:51	3:76	7:15	4:15
6.	5:37	5:30	2:99	3:78	5:44
7.	30:00	2:99	3:90	3:65	7:76
8.	4:02	4:26	8:88	6:72	30:00
9.	8:04	4:80	3:52	3:98	5:23
10.	30:00	5:58	4:25	3:73	4:01
<b>Průměr</b>	<b>15,44s</b>	<b>4,56s</b>	<b>4,72s</b>	<b>4,37s</b>	<b>10,53s</b>

Tabulka 4 - Hodnoty z měření jednoho testovaného subjektu na č. MultiBio 700

č.2 - MultiBio 700					
Číslo měření	bez přívitu	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
	[s]	[s]	[s]	[s]	[s]
1.	9:45	3:28	1:93	2:66	5:28
2.	14:75	3:35	4:60	7:68	5:23
3.	5:45	3:71	2:05	3:36	3:68
4.	8:65	2:16	1:76	3:18	4:13
5.	5:46	2:15	4:20	3:20	4:11
6.	6:15	3:05	1:53	3:80	3:75
7.	9:82	2:93	4:80	6:05	4:30
8.	13:43	3:10	2:15	3:62	5:02
9.	5:05	3:02	2:00	3:19	5:17
10.	9:33	2:88	4:30	3:33	4:01
<b>Průměr</b>	<b>8,75s</b>	<b>2,96s</b>	<b>2,93s</b>	<b>4,01s</b>	<b>4,47s</b>

Tabulka 5 - Hodnoty z měření jednoho testovaného subjektu na č. AccuFace EFR-T1

č.3 - AccuFace EFR-T1					
Číslo měření	bez přívitu	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
	[s]	[s]	[s]	[s]	[s]
1.	2:89	0:72	1:13	1:11	1:32
2.	1:52	0:91	0:63	0:75	0:81
3.	1:03	1:08	0:65	0:78	0:73
4.	1:05	1:02	0:70	0:93	1:13
5.	2:08	0:71	0:61	1:12	1:22
6.	1:07	0:97	0:66	1:06	1:15
7.	1:11	1:12	0:68	0:92	0:80
8.	2:32	0:68	0:74	0:76	1:24
9.	2:08	0:69	1:09	0:74	0:82
10.	1:90	1:01	0:65	1:08	1:16
<b>Průměr</b>	<b>1,71s</b>	<b>0,89s</b>	<b>0,75s</b>	<b>0,93s</b>	<b>1,04s</b>

Tabulka 6 - Hodnoty z měření jednoho testovaného subjektu na č. Aktion AFT-500

č.4 - Aktion AFT - 500					
Číslo měření	bez přívitu	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
	[s]	[s]	[s]	[s]	[s]
1.	1:89	1:80	1:43	1:51	1:32
2.	1:75	1:26	0:98	1:34	1:68
3.	1:71	1:28	0:76	1:56	1:60
4.	1:98	1:78	1:11	0:93	1:88
5.	2:11	1:05	1:05	1:58	1:90
6.	1:67	1:42	0:86	1:47	1:42
7.	1:66	1:33	0:81	1:14	1:47
8.	1:90	1:59	1:18	1:32	1:82
9.	1:90	1:47	1:16	1:43	1:52
10.	2:30	1:31	1:23	1:31	1:66
<b>Průměr</b>	<b>1,89s</b>	<b>1,43s</b>	<b>1,06s</b>	<b>1,36s</b>	<b>1,63s</b>



## 6 Výsledky

V kapitole výsledky se nachází všechny naměřené výsledné, zprůměrované hodnoty, vypočítané hodnoty a následně všechny vytvořené grafy plynoucí z těchto hodnot.

### 6.1 Naměřené hodnoty osvitů jednotlivých barevných přísvitů

Samotnému měření jednotlivých biometrických čteček předcházelo měření okolního přirozeného denního světla v místnosti. Stanovená pracovní měřicí mez byla v rozmezí 0-100 lx. Pakliže míra okolního přirozeného světla nevyhovovala stanovenému kritériu, byla provedena regulace tohoto množství vstupu přirozeného světla do místnosti. Po změření okolního přirozeného osvitů docházelo ke změření jednotlivých přísvitů v rozdílných spektrech. Všechna měření přísvitů byla realizována prostřednictvím luxmetru CEM-DT 8809A. Naměřené hodnoty jednotlivých osvitů jsou znázorněny v následující tabulce 7. Z těchto hodnot následně byla spočítána průměrná hodnota osvitů bez použití umělého přísvitů a následně míra osvitů jednotlivých barevných spekter. Z těchto hodnot byly následně zjištěny průměrné hodnoty jednotlivých barevných spekter přísvitů – červená 328 lx, zelená 478 lx, modrá 453 lx a bílá 850 lx.

Tabulka 7 - Naměřené hodnoty osvitu jednotlivých přísvitů

Průměrné osvětlení (lx)					
Číslo testovaného subjektu	bez přísvitu	R (red, červená)	G (green, zelená)	B (blue, modrá)	W (white, bílá)
	(zregulované denní světlo v místnosti)				
	[lx]	[lx]	[lx]	[lx]	[lx]
1.	90	347	497	489	866
2.	75	330	476	456	848
3.	75	330	476	456	848
4.	85	338	489	483	859
5.	80	329	478	458	850
6.	80	329	478	458	850
7.	75	327	474	452	845
8.	60	305	465	401	838
9.	60	305	465	401	838
10.	80	332	482	463	852
11.	80	332	482	463	852
<b>Průměrná hodnota</b>	<b>76 lx</b>	<b>328 lx</b>	<b>478 lx</b>	<b>453 lx</b>	<b>850 lx</b>

## 6.2 Test rozpoznání subjektů po měření po 3 letech na starších čtečkách (č.1 a č.2)

Samotnému měření ještě předcházela test, který byl zaměřen na rozpoznání testovaných subjektů po 3 letech. Většina testovaných subjektů (9 subjektů z 11 celkových subjektů) se již s biometrickými čtečkami setkala v rámci výuky Elektronických zabezpečovacích systémů (EVS). Tyto testované osoby se již v minulosti účastnily odlišného měření, které bylo realizováno před 3 roky na starších čtečkách (č.1 - iFace 302 a č.2 - Multibio 700). Subjekty byly ponechány v databázi, v biometrických čtečkách a v aktuálním měření byl proveden test, zda tyto biometrické systémy rozeznají testované subjekty i po 3 letech. Tento test byl proveden nad rámec této diplomové práce a byl proveden pouze z orientačních důvodů. Všem subjektům byla následně vytvořena nová registrace do biometrických systémů (enrollment), aby měly všechny subjekty podobné výchozí podmínky a nebyly ovlivněny neaktuální registrací.

Z celkových 9 testovaných subjektů čtečky rozpoznaly pouze 2 osoby, které byly korektně identifikovány. Úspěšnost obou biometrických čteček tohoto testu byla shodná - 22,22 %. Průměrné dosažené skóre v procesu identifikace jednotlivých subjektů, které nebylo možno rozpoznat, se pohybovalo v rozmezí 25–55 %. Zjištěné hodnoty jsou zobrazeny v následující tabulce 8. Z těchto orientačních hodnot vyplývá, že úspěšnost těchto starších biometrických systémů v rozpoznávání subjektů po 3 letech může způsobovat značné problémy. Tento jev může indikovat značné problémy v budoucnosti v procesu samotné identifikace ve společnostech, firmách, kde jsou tyto čtečky zastoupeny.

Negativní dopady mohou být zejména z hlediska v čase potřebném k identifikaci uživatelů, snížení míry spolehlivosti, zvýšení případné frustrace z negativního výsledku identifikace a v neposlední řadě také možné zvýšení nákladů společnosti.

Tabulka 8 - Test rozpoznání subjektů po 3 letech na č.1 a č.2

Čtečka	Identifikováno	Neidentifikováno	Úspěšnost [%]
iFace 302	2	7	22,22 %
Multibio 700	2	7	22,22 %

## 6.3 Naměřené hodnoty doby identifikace

Ze všech měření na biometrických čtečkách (celkem 2200 hodnot z měření) byly provedeny výpočty jednotlivých průměrných časů, potřebných k identifikaci na konkrétních čtečkách. Samotné měření bylo odlišeno v měření bez použitého umělého přisvitu (pouze za pomoci denního, přirozeného, okolního světla v rozmezí 0-100 lx) a za pomoci umělého přisvícení v barevném spektru červeném, zeleném, modrém a bílém.

V grafu 1 je zobrazen souhrn všech průměrných časů, potřebných k identifikaci u jednotlivých čteček. Doba identifikace je znázorněna v sekundách a jednotlivé sloupce v grafu reprezentují jednotlivé čtečky v konkrétních barevných spektrech.

**Čtečka č.1 iFace 302** dosahuje hodnot 10,7s bez přisvitu. V barevných spektrech dosahuje následujících hodnot – v červeném 3,23s (zlepšení o 7,47s), v zeleném 3,12s (zlepšení o 7,58s), v modrém 2,71s (zlepšení o 7,99s) a v bílém 4,27s (zlepšení o 6,43s).

**Čtečka č.2 Multibio 700** dosahuje hodnot 9,04s bez přisvitu. V barevných spektrech dosahuje následujících hodnot – v červeném 4,07s (zlepšení o 4,97s), v zeleném 3,12s (zlepšení o 5,92s), v modrém 3,51s (zlepšení o 5,53s) a v bílém 4,11s (zlepšení o 4,93s).

**Čtečka č.3 AccuFace EFR-T1** dosahuje hodnot 1,64s bez přisvitu. V barevných spektrech dosahuje následujících hodnot – v červeném 1,07s (zlepšení o 0,57s), v zeleném 0,95s (zlepšení o 0,69s), v modrém 1,03s (zlepšení o 0,61s) a v bílém 1,33s (zlepšení o 0,31s).

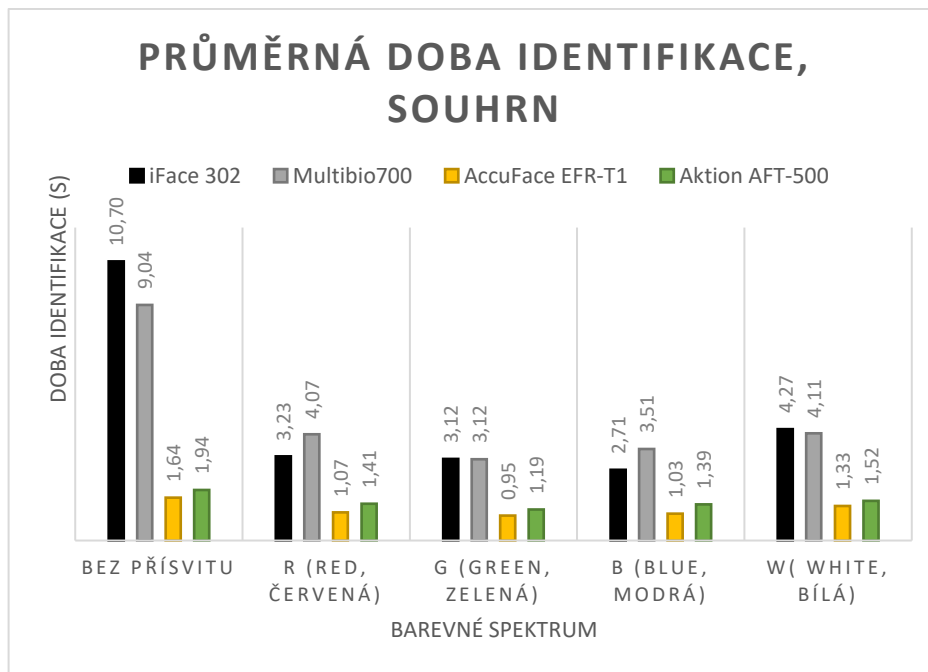
**Čtečka č.4 Aktion AFT-500** dosahuje hodnot 1,94s bez přisvitu. V barevných spektrech dosahuje následujících hodnot – v červeném 1,41s (zlepšení o 0,53s), v zeleném 1,19s (zlepšení o 0,75s), v modrém 1,39s (zlepšení o 0,55s) a v bílém 1,52s (zlepšení o 0,42s).

Z měření jednoznačně vyplývá, že obecně z vlivu dodatečného umělého přisvitu dochází ke zlepšení (snížení) identifikačních časů, potřebných k rozpoznání potenciálních uživatelů. Z měření také vyplývá, že jednotlivé časy jsou také více stabilní a nedochází k tak velké odlišnosti jednotlivých časů jako v případě bez přisvitu, zejména u starších čteček č.1 a č.2.

Z těchto hodnot je možné usuzovat, že u starších čteček dochází k velkému zlepšení v průměrné době potřebné k identifikaci, kdežto u novějších čteček dochází také ke zlepšení, ale pouze v menší, omezené míře.

Nejllepší výsledky z hlediska průměrné doby identifikace, rychlosti, dosahuje zejména zelené a modré barevné spektrum s průměrnou hodnotou osvitů – zelená 478 lx, modrá 453 lx. Největší zlepšení je patrné ve spektrech zejména u č.1 (zelené o 7,58s a modré o 7,99s z původních 10,7s) a u č.2 (zelené o 5,92s a modré o 5,53s z původních 9,04s).

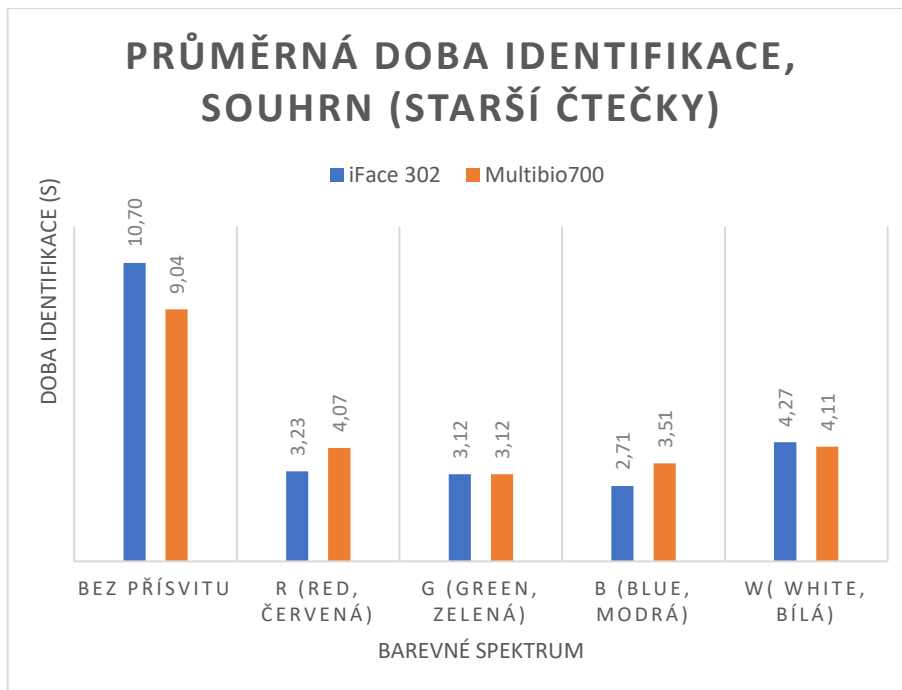
Graf 1- Průměrná doba identifikace (souhrn)



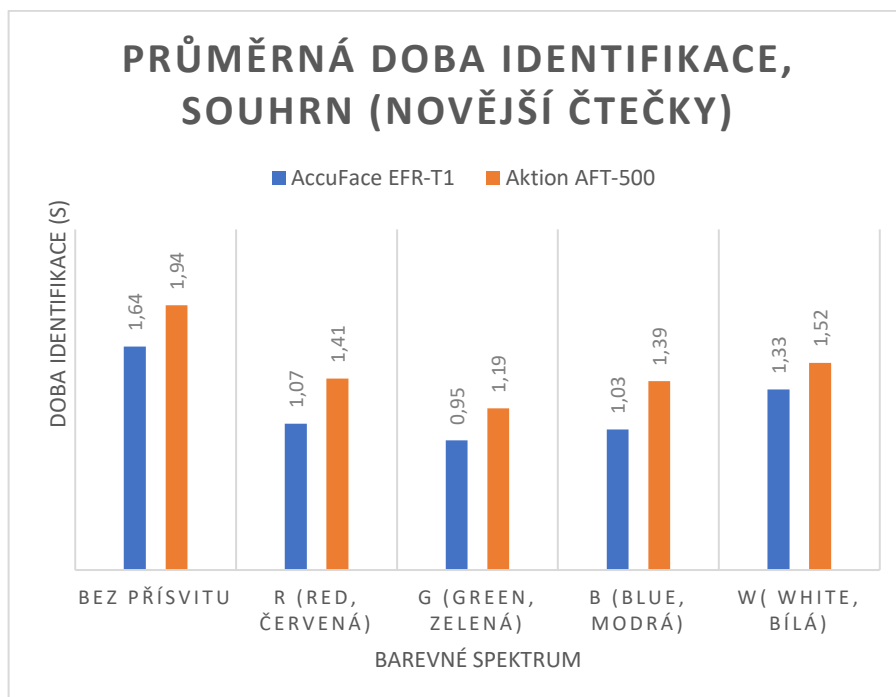
V následujících grafech 2 a 3 je zobrazeno bližší porovnání čteček, které je rozděleno na starší (č.1 a č.2) a novější čtečky (č.3 a č.4). Z těchto grafů je jednoznačně vidět přínos jednotlivých přísvitů v konkrétních barevných spektrech. Z těchto grafů mimo jiné také vyplývá jednoznačný posun v oblasti technologie biometrie obličeje. Jednoznačně je z grafů možné vidět, že ačkoliv přínos u novějších čteček v podobě přísvitů je, není tak významný jako u starších čteček. U nových čteček dochází k nejrychlejším časům identifikace také ve spektru zeleném a modrém, ale zlepšení je v menší míře u č.3 - v zeleném spektru o 0,69s a v modrém spektru o 0,61s z původních 1,64s, u č.4 - v zeleném spektru o 0,75s a v modrém spektru o 0,55s z původních 1,94s.

V příloze s označením 1 - 9 na stranách I - IV jsou dostupné grafy, které zobrazují dobu identifikace jednotlivých čteček, dle jednoho konkrétního barevného spektra s porovnáním vůči jednotlivým čtečkám. Je zde zobrazeno také dodatečné porovnání konkrétních čteček a jednotlivých barevných spekter a jejich vlivu na dobu identifikace.

Graf 2 - Průměrná doba identifikace (souhrn), starší čtečky (č.1 a č.2)



Graf 3 - Průměrná doba identifikace (souhrn), novější čtečky (č.3 a č.4)



## 6.4 Naměřené hodnoty spolehlivosti (FRR)

Celkový počet měření u jedné čtečky, při všech 11 subjektech a po 10 opakováních pro jedno konkrétní spektrum přísvitu je 110. Počet měření u všech pěti spekter jedné čtečky je 550. Počet všech celkových měření pro všechna spektra i čtečky dohromady je 2200. Tabulka 9 obsahuje všechny naměřené hodnoty, kdy nedošlo ke korektní identifikaci ve vytyčeném čase pro jednotlivé čtečky a barevná spektra. Z těchto hodnot byla spočítána procentuální neidentifikovatelnost - hodnota FRR. Na základě těchto hodnot byly následně sestaveny grafy 4, 5, 6 a 7. Pakliže došlo k překročení stanovené hranice (10s, 5s, 3s, 2s) byl čas identifikace považován za nevyhovující a stav byl vyhodnocen jako - neidentifikován pro danou časovou hranici.

Příklad výpočtu hodnoty FRR u č.1, pro spektrum bez umělého přísvitu pro hranici 10s:

$$FRR = \frac{N_{FR}}{N_{EIA}} * 100 = \frac{38}{110} * 100 = 34,55[\%]$$

$N_{FR}$  = počet chybných odmítnutí = počet nevyhovujících pokusů

$N_{EIA}$  = počet pokusů oprávněných osob o identifikaci = 110

Mez identifikovatelnosti byla stanovena odlišně pro starší čtečky (10s benevolentnější a 5s přísnější varianta) a novější čtečky (3s benevolentnější a 2s přísnější varianta). Následně byly tyto čtečky porovnávány odděleně, zejména z důvodu novější, odlišné technologie a očekávaného času potřebného k identifikaci – u novějších čteček č.3 a č.4 do 2s, dle výrobce (starší č.1 a č.2 výrobce čas nestanovuje). Nutné je také zmínit fakt, že u novějších čteček č.3 a č.4 došlo vždy k identifikaci osoby, ale časová mez nebyla vždy ve všech případech dodržena. Celkový počet absolutních neidentifikovatelných pokusů (kdy došlo na ukončení pokusu z důvodu dosažení časového limitu 30s) bylo 12x pro č.1 a 6x pro č.2, vždy v případě bez použití přísvitu. U č.3 a č.4 došlo ve 100 % případech k identifikování osoby, i když ne vždy ve stanovené časové hranici.

Tabulka 9 - Naměřené hodnoty neidentifikovaných pokusů, přípustné hranice (10s, 5s, 3s, 2s), výpočet FRR

<b>Hranice 10s - neidentifikovatelnost FRR (č.1 - iFace 302)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
38x	2x	2x	0x	6x
<b>34,55%</b>	<b>1,82%</b>	<b>1,82%</b>	<b>0,00%</b>	<b>5,45%</b>
<b>Hranice 5s - neidentifikovatelnost FRR (č.1 - iFace 302)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
82x	10x	14x	4x	20x
<b>74,55%</b>	<b>9,09%</b>	<b>12,73%</b>	<b>3,64%</b>	<b>18,18%</b>
<b>Hranice 10s - neidentifikovatelnost FRR (č.2 - Multibio 700)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
34x	4x	2x	0x	2x
<b>30,91%</b>	<b>3,64%</b>	<b>1,82%</b>	<b>0,00%</b>	<b>1,82%</b>
<b>Hranice 5s - neidentifikovatelnost FRR (č.2 - Multibio 700)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
82x	32x	12x	22x	22x
<b>74,55%</b>	<b>29,09%</b>	<b>10,91%</b>	<b>20,00%</b>	<b>20,00%</b>
<b>Hranice 3s - neidentifikovatelnost FRR (č.3 - AccuFace EFR-T1)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
4x	0x	0x	0x	2x
<b>3,64%</b>	<b>0,00%</b>	<b>0,00%</b>	<b>0,00%</b>	<b>1,82%</b>
<b>Hranice 3s - neidentifikovatelnost FRR (č.4 - Aktion AFT-500)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W(white, bílá)
6x	0x	2x	2x	0x
<b>5,45%</b>	<b>0,00%</b>	<b>1,82%</b>	<b>1,82%</b>	<b>0,00%</b>
<b>Hranice 2s - neidentifikovatelnost FRR (č.3 - AccuFace EFR-T1)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
26x	2x	0x	0x	14x
<b>23,64%</b>	<b>1,82%</b>	<b>0,00%</b>	<b>0,00%</b>	<b>12,73%</b>
<b>Hranice 2s - neidentifikovatelnost FRR (č.4 - Aktion AFT-500)</b>				
bez přísvitů	R (red, červená)	G (green, zelená)	B (blue, modrá)	W( white, bílá)
48x	6x	2x	4x	12x
<b>43,64%</b>	<b>5,45%</b>	<b>1,82%</b>	<b>3,64%</b>	<b>10,91%</b>

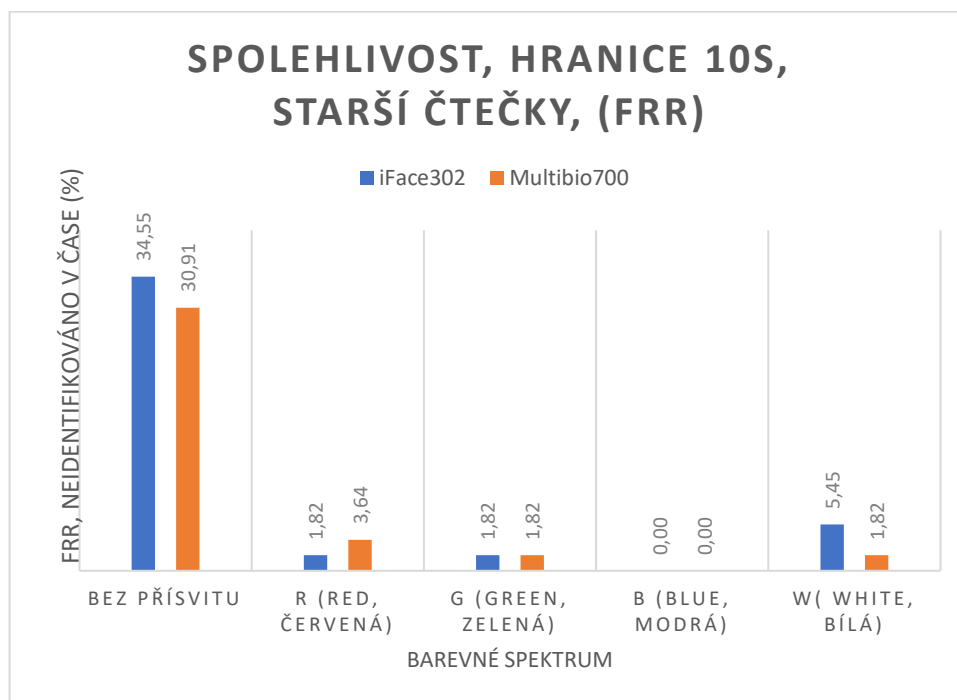


Grafy zobrazující spolehlivost starších čteček (č.1 – iFace 302 a č. 2 Multibio 700) jsou grafy s označením 4 a 5. Tyto grafy jsou rozděleny, dle časové hranice 10s (benevolentnější varianta) a 5s (přísnější varianta). Oba grafy reprezentují spolehlivost čteček, která je vyjádřena hodnotou FRR – false rejection rate (míra chybného odmítnutí). Čím nižší míra FRR, tím lépe (čím nižší hodnota FRR, tím vyšší spolehlivost). Oba grafy obsahují rozdělení naměřených hodnot dle jednotlivých barevných spekter.

Z grafu s označením 4, je možné vyčíst následující údaje, reprezentující spolehlivost čteček č.1. a č.2 do hranice 10s. Čtečky bez užití dodatečného přísvitu dosahují chybovosti, neidentifikovatelnosti (FRR) u č.1 – 34,55 % a u č.2 – 30,91 %. Při užití dodatečného přísvitu ve všech barevných spektrech dochází jednoznačně ke zlepšení spolehlivosti, a to v následující míře. Neidentifikovatelnost FRR klesla na hodnotu u přísvitu červeného u č.1 – na 1,82 %, u č.2 – na 3,64 %, u přísvitu zeleného u č.1 – na 1,82 %, u č.2 – na 1,82 %, u přísvitu modrého u č.1 – na 0,00 %, u č.2 – na 0,00 % a u přísvitu bílého u č.1 – na 5,45 %, u č.2 – na 1,82 %.

Z těchto hodnot jednoznačně vyplývá, že nejvyšší spolehlivosti a zároveň nejnižší hodnotou neidentifikovatelnosti FRR dosahuje spektrum v barvě modré (zlepšení u č.1. o 34,55 % a u č.2 o 30,91%) a zelené (zlepšení u č.1. o 32,73 % a u č.2 o 29,09%). Zlepšení spolehlivosti při užití těchto barevných spekter přísvitů je velmi znatelné.

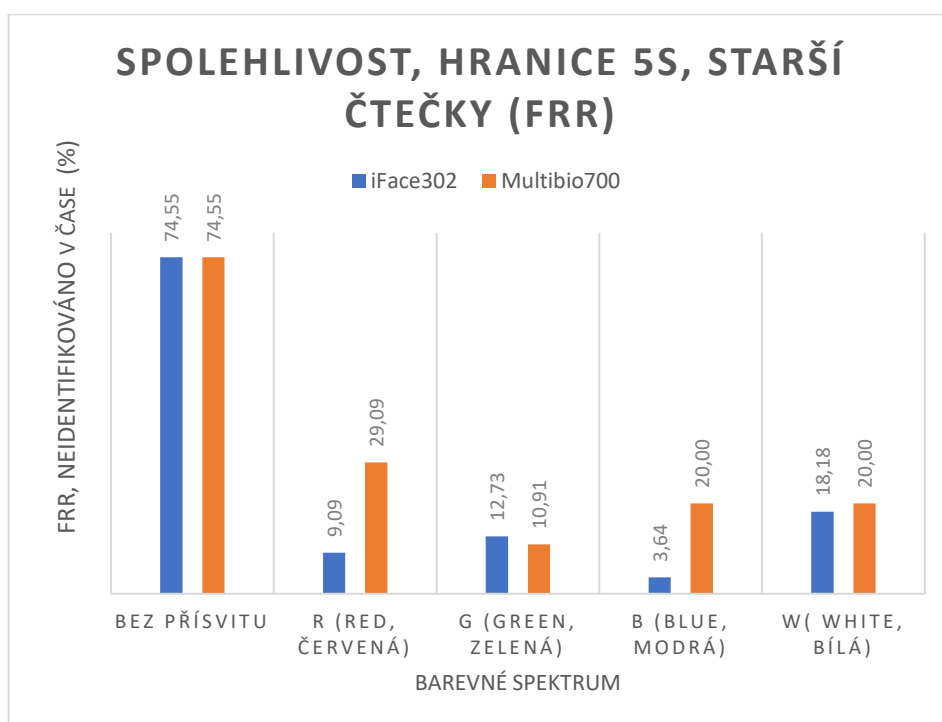
Graf 4 - Spolehlivost, hranice nastavena na 10s, (FRR) starší čtečky (č.1 a č.2)



Z grafu s označením 5 je možné vyčíst následující údaje, reprezentující spolehlivost čteček č.1. a č.2 do hranice 5s. Čtečky bez užití dodatečného přísvitů dosahují totožné chybovosti, neidentifikovatelnosti (FRR) u č.1 i u č.2 – 74,55 %. Tato hodnota FRR je velmi vysoká a v praxi je nepřijatelná. Při užití dodatečného přísvitů ve všech barevných spektrech dochází opět jednoznačně ke zlepšení spolehlivosti, a to v následující míře. Neidentifikovatelnost FRR klesla na hodnotu u přísvitů červeného u č.1 – na 9,09 %, u č.2 – na 29,09 %, u přísvitů zeleného u č.1 – na 12,73 %, u č.2 – na 10,91 %, u přísvitů modrého u č.1 – na 3,64 %, u č.2 – na 20,00 % a u přísvitů bílého u č.1 – na 18,18 %, u č.2 – na 20,00 %.

Z těchto hodnot jednoznačně vyplývá, že nejvyšší spolehlivosti a zároveň nejnižší hodnotou neidentifikovatelnosti FRR dosahuje spektrum opět v barvě modré (zlepšení u č.1. o 70,91 % a u č.2 o 54,55 %) a zelené (zlepšení u č.1. o 61,82 % a u č.2 o 63,64 %). Zlepšení spolehlivosti při užití těchto barevných spekter přísvitů je opět velmi znatelné.

Graf 5 - Spolehlivost, hranice nastavena na 5s, (FRR) starší čtečky (č.1 a č.2)

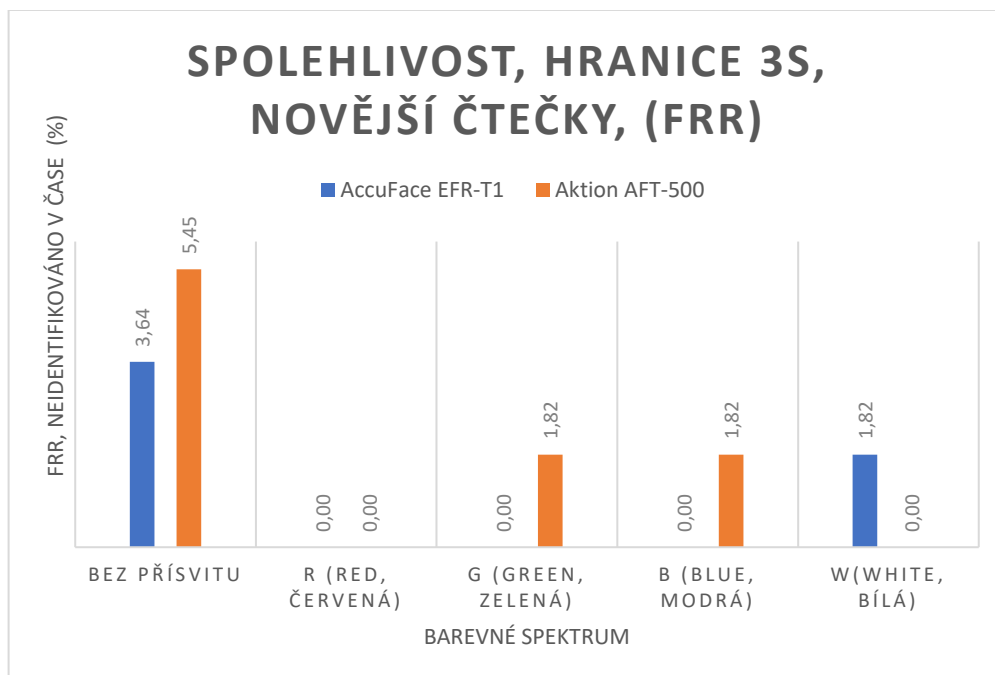


Grafy zobrazující spolehlivost novějších čteček (č.3 – AccuFace EFR-T1 a č.4 Aktion AFT-500), jsou grafy s označením 6 a 7. Tyto grafy jsou rozděleny dle časové hranice 3s (benevolentnější varianta) a 2s (přísnější varianta). Oba grafy reprezentují spolehlivost čteček, která je vyjádřena opět stejnou metodikou - hodnotou FRR (false rejection rate (míra chybného odmítnutí)). Čím nižší míra FRR, tím lépe. Oba grafy obsahují opět rozdělení naměřených hodnot dle jednotlivých barevných spekter.

Z grafu s označením 6 je možné vyčíst následující údaje, reprezentující spolehlivost čteček č.3 a č.4 do hranice 3s. Čtečky bez užití dodatečného přisvitu dosahují chybovosti, neidentifikovatelnosti (FRR) u č.3 – 3,64 % a u č.4 – 5,45 %. Při užití dodatečného přisvitu ve všech barevných spektrech dochází k mírnému zlepšení spolehlivosti, ale ne do takové míry, jako u starších čteček. Neidentifikovatelnost FRR klesla na hodnotu přisvitu červeného u č.3 – na 0,00 %, u č.4 – na 0,00 %, u přisvitu zeleného u č.3 – na 0,00 %, u č.4 – na 1,82 %, u přisvitu modrého u č.3 – na 0,00 %, u č.4 – na 1,82 % a u přisvitu bílého u č.3 – na 1,82 %, u č.4 – na 0,00 %.

Z těchto hodnot vyplývá, že ke zvýšení spolehlivosti dochází v mnohem nižší míře, než u čteček starších. Novější čtečky pracují relativně rychle a spolehlivě, ale dochází zde také k jistému zvýšení míry spolehlivosti. Přínos jednotlivých barevných spekter je víceméně v tomto případě vyvážen.

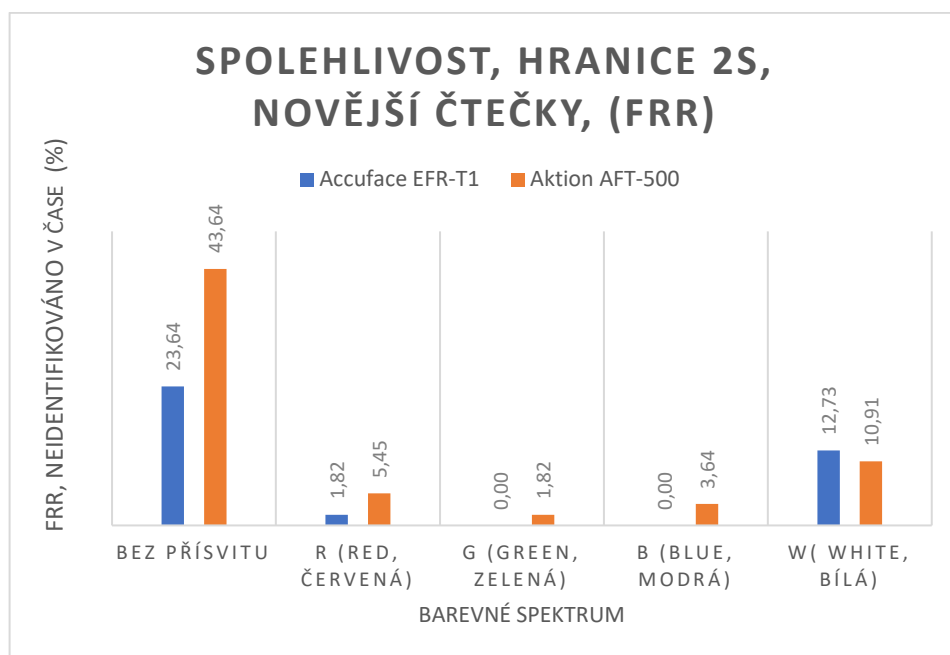
Graf 6 - Spolehlivost, hranice nastavena na 3s, (FRR) novější čtečky (č.3 a č.4)



Z grafu s označením 7 je možné vyčíst následující údaje, reprezentující spolehlivost čteček č.3 a č.4 do hranice 2s. Čtečky bez užití dodatečného přisvitu dosahují chybovosti, neidentifikovatelnosti (FRR) u č.3 – 23,64 % a u č.4 – 43,64 %. Při užití dodatečného přisvitu ve všech barevných spektrech dochází k mírnému zlepšení spolehlivosti, ale opět ne do takové míry, jako u starších čteček, ale při této časové hranici je vliv dodatečného přisvitu již více znát. Neidentifikovatelnost FRR klesla na hodnotu u přisvitu červeného u č.3 – na 1,82 %, u č.4 – na 5,45 %, u přisvitu zeleného u č.3 – na 0,00 %, u č.4 – na 1,82 %, u přisvitu modrého u č.3 – na 0,00 %, u č.4 – na 3,64 % a u přisvitu bílého u č.3 – na 12,73 %, u č.4 – na 10,91 %.

Z těchto hodnot vyplývá, že ke zvýšení spolehlivosti zde dochází, ale v mnohem nižší míře, než u čteček starších, ale zároveň je vliv přisvitu znatelnější v této přísnější časové hranici 2s, než u benevolentnější hranici 3s. Přínos jednotlivých barevných spekter je nejznatelnější u přisvitu zeleného (zlepšení o 23,64 % u č.3 a o 41,82 % u č.4) a modrého (zlepšení o 23,64 % u č.3 a o 40,00 % u č.4). Nejnižší přínos podává bílé spektrum (zlepšení o 10,91 % u č.3 a o 32,73 % u č.4).

Graf 7 - Spolehlivost, hranice nastavena na 2s, (FRR) novější čtečky (č.3 a č.4)



## 7 Diskuse

Mnoho zpracovaných, zdokumentovaných prací, které by se zabývaly problematikou přisvitu u biometrických zařízení a konkrétně se zaměřením na obličej není a s rozbořením jednotlivých barevných spekter a typů přisvitu ještě méně, ať už v zahraničí nebo v ČR. Jednou z mála prací, která se částečně zabývá přisvitem u biometrie obličej je disertační práce Ing. Veroniky Hartové, Ph.D. Tato práce je z roku 2014 a téma práce se nazývá Biometrické identifikační systémy. V této práci je provedena prvotní inovace v podobě využití bílé LED diody u přisvitu a bylo realizováno prvotní orientační měření, zda přisvit jako takový má smysl u biometrických čteček. V této práci bylo zjištěno, že přidáním bílé LED diody opravdu dochází ke zlepšení spolehlivosti jednotlivých čteček, a to v průměru o 40 % u čtečky iFace 302 a o 34 % u čtečky Multibio 700.

V aktuální diplomové práci byla tato prvotní myšlenka rozšířena o další barevná spektra přisvitů a následně bylo zjištěno v prvotním měření těchto čteček při využití přisvitu v podobě 6x LED RGB pásků a nastavení časové meze identifikace na 10s zlepšení spolehlivosti u čtečky iFace 302 o 32,73% (červené spektrum), o 32,73 % (zelené spektrum), o 34,55 % (modré spektrum) a o 29,10 % (bílé spektrum). Zlepšení spolehlivosti u čtečky Multibio 700 o 27,07 % (červené spektrum), o 29,09 % (zelené spektrum), o 30,91 % (modré spektrum) a o 29,09 % (bílé spektrum). Při dalším měření a stanovením odlišných časových hranic doby identifikace bylo vyhodnoceno jako spektrum s nejvyšším zlepšením zelené a modré s tím, že modré spektrum je i nejpřijatelnější z hlediska optického vjemu lidského oka.

Při porovnání výsledků z těchto prací, v bílém spektru je zřejmé, že se hodnoty liší o jednotky procent. Tato odlišnost je způsobena zejména odlišnou skladbou testovaných subjektů, jelikož každý člověk je originál, disponuje více či méně odlišným obličejem, tak i čtečky rozpoznávají jednotlivé obličej lépe či hůře. Dále může být odlišnost způsobena množstvím výchozího přirozeného světla v místnosti, metodikou přístupu k procesu identifikace, kde nelze zajistit vždy 100 % totožné podmínky a zejména ovlivněním lidského faktoru při identifikaci. Každý člověk přistupuje k čtečce mírně odlišně, ačkoliv se snaží po prvotní instruktaži přistupovat totožně, vždy dochází k drobným odchylkám.

Ostatní výsledky, zejména z hlediska spolehlivosti a vlivu na dobu identifikace u ostatních barevných spekter při odlišných časových hranicích identifikace, či rozpoznání uživatelů po 3 letech, či příjemnosti osvětlení barevných přisvitů lidským okem nelze porovnat, jelikož nebyly nalezeny zdokumentované práce, které by se touto problematikou zabývaly.

Obecně se technologie biometrie obličejů neustále vyvíjí. Technologie nasazovaná v praxi je to relativně nová, využívaná zejména v zahraničí. V ČR se teprve relativně nedávno začala využívat, a to zejména ve státním sektoru, ve větších firmách, letištích a u vysoce střežených objektů.

Velký důraz na vývoj je kladen zejména z hlediska softwaru, kde se neustále zlepšují algoritmy rozpoznání jednotlivých obličejů, vyvíjí se odlišné metody rozpoznávání, vytváří se nové licence a patenty na jednotlivé algoritmy, ale vývoj hardwaru, na kterém jsou biometrické čtečky stejně tak závislé není často prioritou do takové míry. Toto je možné vidět zejména u starších čteček iFace 302 či Multibio 700, kde je použit nedostačující IR přísvit v podobě LED, který se využívá pouze ve zhoršených podmínkách a ani v těchto podmínkách nepřináší mnoho užitku, je silně poddimenzován. Z testování při podmínkách 0-100 lx bylo jednoznačně zjištěno zlepšení, při využití dodatečného LED přísvitu. Tento LED přísvit není nikterak finančně náročný a zlepšení z hlediska spolehlivosti a rychlosti identifikace je veliké. Z těchto důvodů je dodatečný přísvit v podobě LED více než vhodný.

Starší čtečky iFace 302 a Multibio 700 jsou stále aktuálními čtečkami, které se ve velké míře používají a jsou stále v nabídce prodejců těchto biometrických systémů. Novější čtečky AccuFace EFR-T1 a Aktion AFT-500 jsou technologicky vyspělejšími čtečkami a je zde vidět evoluční technologický pokrok. Tyto novější čtečky fungují relativně velmi dobře, disponují vhodným soběstačným přísvitem v podobě IR LED. Accuface EFR-T1 se spoléhá zejména na svůj IR LED přísvit, kdežto Aktion AFT-500 využívá svůj IR LED přísvit pouze ve zhoršených podmínkách. U těchto novějších čteček dodatečný přísvit není potřebný a fungují velmi dobře i bez dodatečného přísvitu, avšak k menšímu zlepšení i zde dochází a byl by vhodný zejména u vysoce frekventovaných objektů, kde dochází k velkému množství identifikací a je zde vítané i drobné zlepšení doby identifikace na osobu, které se následně projeví ve velkém měřítku identifikovaných osob.

Novější čtečky nejsou ale zcela bezchybné. Čtečka AccuFace EFR-T1 obsahuje vizuální šablonu (virtuální obličejové bariéry), do které se musí obličej při identifikaci umístit. Z tohoto důvodu může být identifikace mírně nekomfortní. Čtečka Aktion AFT-500 neidentifikuje uživatele, kteří nosí dioptrické brýle, z tohoto důvodu může být opět identifikace mírně nekomfortní (nutné odložení brýlí při identifikaci) a pakliže uživatel nemá volné ruce, může být tato identifikace i mírně frustrující.

Stejně jako u všech technologií, tak i u vývoje biometrických technologií je nutné pamatovat na to, že nejslabší článek celého systému může ve velké míře negativně ovlivnit ve výsledku celý systém – necitlivá kamera s nízkým rozlišením, slabý přísvit, špatně zvolená technologie přísvitu a v tomto případě sebelepší softwarové vybavení v podobě metody či algoritmu rozpoznání obličejů může vysoký potenciál například jinak výborného algoritmu zcela potlačit.

## 8 Závěr

Měření bylo realizováno při průměrném, zregulovaném denním osvětlení místnosti laboratoře v rozsahu 0-100 lx. Naměřená, průměrná hodnota přirozeného osvětlení laboratoře dosahovala hodnoty 76 lx. Při těchto světelných podmínkách byly změřeny následující hodnoty osvětlení jednotlivých přísvitů, které byly následně zprůměrovány. Jednotlivé přísvitů byly nastaveny na stejný vyzařovaný světelný výkon. Nejvyššího přísvitů bylo dosaženo při přísvitů bílém (850 lx), následně při osvětlení zeleném (478 lx), při osvětlení modrém (453 lx) a v neposlední řadě při osvětlení červeném (328 lx).

Při měření byly využity 4 nejpoužívanější biometrické čtečky na českém trhu. Dvě čtečky disponující starší technologií a dvě čtečky disponující novější technologií. Starší čtečky se nazývají iFace 302 a Multibio 700. Novější čtečky se nazývají AccuFace EFR-T1 a Aktion AFT-500.

Měření se účastnilo celkem 11 testovaných subjektů. Testování bylo realizováno v jednotlivých barevných spektrech přísvitů na jednotlivých čtečkách. Samotné měření jednoho subjektů bylo provedeno na 4 čtečkách v 5 barevných přísvitů a při 10 opakováních ( $4 \times 5 \times 10 = 200$  hodnot / subjekt). Celkový počet naměřených hodnot byl 2200 ( $200 \times 11 = 2200$ ).

Hlavním cílem měření bylo zjištění vlivu přísvitů, případného přínosu jednotlivých spekter ovlivnění spolehlivosti a rychlosti doby identifikace. V neposlední řadě byla zohledněna vhodnost barevného spektra také z hlediska příjemnosti vnímání světla lidským okem.

Ze všech naměřených hodnot vyplývá, že největší přínos přísvitů jako takového je u starších čteček č.1 a č.2, přínos u novějších čteček č.3 a č.4 je v menší míře, ale stále je znatelný. Ze všech barevných přísvitů podávají nejlepší výkon, jak z hlediska doby samotného procesu identifikace, tak i spolehlivosti barevné spektrum – zelené a modré. S přihlédnutím z hlediska příjemnosti vnímání jednotlivých barev lidským okem, vychází jako nejlepší volba modrá.

Ze zjištěných hodnot vychází, že starší čtečky se jednoznačně vyplatí provozovat s dodatečným přísvitů, kde zlepšení je velmi znatelné. U novějších čteček se vyplatí používat dodatečný přísvit, pakliže je využití velmi vysoké a je proces identifikace velmi frekventovaný. Tyto případy mohou nastat zejména v případech velkých společností, kde se provádí velké množství identifikací za den a je zde znatelný efekt takzvaných „motýlích křídel“, kde velmi malé změny na vstupu procesu (drobné ušetření času jedné identifikace) tvoří velké změny na výstupu (velké ušetření času ve výsledku, ze všech identifikací).

Z hlediska vnímání jednotlivých barevných spekter lidskýma očima bylo vyhodnoceno jako nejpříznivější spektrum modré a červené. Jako velmi rušivé spektrum až nepříjemné lidským vnímáním bylo vyhodnoceno spektrum zelené a bílé.

Ze samotného měření jednoznačně lze usuzovat, že vliv dodatečného přísvitu u biometrických čteček je. U starších čteček je přínos vysoký, u novějších čteček je přínos nižší, ale stále do jisté míry znatelný.

U starších čteček iFace 302 (č.1) a Multibio 700 (č.2) dosahuje nejlepších výsledků z hlediska průměrné doby identifikace, rychlosti, zejména zelené a modré barevné spektrum. Největší zlepšení je patrné ve spektrech zejména u č.1 (zelené o 7,58s a modré o 7,99s z původních 10,7s (bez přísvitu) na hodnoty v zeleném spektru 3,12s a modrém spektru 2,71s) a u č.2 (zelené o 5,92s a modré o 5,53s z původních 9,04s (bez přísvitu) na hodnoty v zeleném spektru 3,12s a modrém spektru 3,51s).

U novějších čteček AccuFace EFR-T1 (č.3) a Aktion AFT-500 (č.4) dosahuje nejlepších výsledků z hlediska průměrné doby identifikace, rychlosti, také zejména zelené a modré barevné spektrum. Největší zlepšení je patrné ve spektrech zejména u č.3 (zelené o 0,69s a modré o 0,61s z původních 1,64s (bez přísvitu) na hodnoty v zeleném spektru 0,95s a modrém spektru 1,03s) a u č.4 (zelené o 0,75s a modré o 0,55s z původních 1,94s (bez přísvitu) na hodnoty v zeleném spektru 1,19s a modrém spektru 1,39s).

Spolehlivost v odlišných spektrech přísvitu je velmi ovlivnitelná opět zejména u starších biometrických čteček a mírně znatelná u novějších biometrických čteček. Spolehlivost je vyjádřena chybovostí nekorektního nepřijetí oprávněných uživatelů – hodnota FRR (false rejection rate, míra falešného odmítnutí). Tato hodnota je vypočítána ze vztahu, která je přímo závislá na naměřených časových údajích jednotlivých identifikací a zároveň stanovení přijatelného času identifikace. Z hlediska odlišné technologie byly čtečky porovnávány odděleně, opět na starší a novější. Výrobce udává u novějších čteček identifikaci do 2s, výrobce u starších čteček dobu identifikace obličeje neudává. Z tohoto důvodu byly při vyhodnocování naměřených údajů zohledněny hranice přísnější a benevolentnější. U starších čteček byly užity časové hranice 10s (benevolentnější) a 5s (přísnější) a u novějších čteček byly užity časové hranice 3s (benevolentnější) a 2s (přísnější). Mimo jiné byl také stanoven maximální časový limit pokusu identifikace na 30s (při překročení času, je pokus vyhodnocen jako absolutní neidentifikování subjektu). Je nutné zmínit, že u novějších čteček došlo vždy ve 100 % případů k identifikaci uživatele a nedošlo k absolutní neidentifikaci uživatele (nebyl překročen čas 30s). U starších čteček bylo zaznamenáno 12 případů u čtečky iFace 302 a 6 případů u čtečky Multibio 700 absolutní neidentifikace, vždy v případě neuzítí přísvitu.



Chybovost či neidentifikovatelnost u starších čteček při časové hranici 10s dosahovala hodnot při neužití přisvitu u č.1 34,55 % a u č.2 30,91 %. Nejnížší míru neidentifikovatelnosti bylo dosaženo v modrém a zeleném přisvitu. Naměřené hodnoty v barvě modré jsou následující - zlepšení u č.1. o 34,55 % na hodnotu 0,00 % a u č.2 o 30,91 % na hodnotu 0,00 %. Zlepšení v zeleném přisvitu - u č.1. o 32,73 % na hodnotu 1,82 % a u č.2 o 29,09 % na hodnotu 1,82 %. Zlepšení spolehlivosti při užití těchto barevných spekter přisvitů je velmi znatelné.

Chybovost či neidentifikovatelnost u starších čteček při časové hranici 5s dosahovala hodnot při neužití přisvitu u č.1 i č.2 74,55 %. Nejnížší míru neidentifikovatelnosti bylo dosaženo opět v modrém a zeleném přisvitu. Naměřené hodnoty v barvě modré jsou následující - zlepšení u č.1. o 70,91 % na hodnotu 3,64 % a u č.2 o 54,55 % na hodnotu 20,00 %. Zlepšení v zeleném přisvitu - u č.1. o 61,82 % na hodnotu 12,73 % a u č.2 o 63,64 % na hodnotu 10,89 %. Zlepšení spolehlivosti při užití těchto barevných spekter přisvitů je velmi znatelné.

Chybovost či neidentifikovatelnost u novějších čteček při časové hranici 3s dosahovala hodnot při neužití přisvitu u č.3 3,64 % a u č.4 5,45 %. Při užití dodatečného přisvitu ve všech barevných spektrech dochází k mírnému zlepšení spolehlivosti, ale ne do takové míry, jako u starších čteček. Neidentifikovatelnost klesla na hodnotu u přisvitu červeného u č.3 i č.4 na 0,00 %, u přisvitu zeleného u č.3 – na 0,00 %, u č.4 – na 1,82 %, u přisvitu modrého u č.3 – na 0,00 %, u č.4 – na 1,82 % a u přisvitu bílého u č.3 – na 1,82 %, u č.4 – na 0,00 %. Z těchto hodnot vyplývá, že ke zvýšení spolehlivosti dochází v mnohem nižší míře než u čteček starších. Novější čtečky pracují relativně rychle a spolehlivě, ale dochází zde také k jistému zvýšení míry spolehlivosti. Přínos jednotlivých barevných spekter je víceméně v tomto případě vyvážen.

Chybovost či neidentifikovatelnost u novějších čteček při časové hranici 2s dosahovala hodnot při neužití přisvitu u č.3 23,64 % a u č.4 43,64 %. Při užití dodatečného přisvitu ve všech barevných spektrech dochází ke znatelnějšímu zlepšení spolehlivosti, ale opět ne do takové míry, jako u starších čteček. Neidentifikovatelnost klesla na hodnotu u přisvitu červeného u č.3 na 1,82 % a u č.4 na 5,45 %, u přisvitu zeleného u č.3 – na 0,00 %, u č.4 – na 1,82 %, u přisvitu modrého u č.3 – na 0,00 %, u č.4 – na 3,64 % a u přisvitu bílého u č.3 – na 12,73 %, u č.4 – na 10,91 %. Z těchto hodnot vyplývá, že ke zvýšení spolehlivosti dochází v mnohem nižší míře než u čteček starších. Z těchto hodnot vyplývá, že ke zvýšení spolehlivosti zde dochází, ale v mnohem nižší míře než u čteček starších, ale zároveň je vliv přisvitu znatelnější v této přísnější časové hranici 2s, než v benevolentnější hranici 3s. Přínos jednotlivých barevných spekter je nejznatelnější u přisvitu zeleného (zlepšení o 23,64 % u č.3 a o 41,82 % u č.4) a modrého (zlepšení o 23,64 % u č.3 a o 40,00 % u č.4). Nejnížší přínos podává bílé spektrum (zlepšení o 10,91 % u č.3 a o 32,73 % u č.4).

Z celkových 11 subjektů bylo 9 subjektů otestováno také nad rámec diplomové práce z hlediska identifikace po 3 letech, od doby prvotní registrace. Testování z hlediska identifikace po 3 letech od prvotní registrace (rozpoznání) bylo umožněno díky seznámení se s staršími čtečkami v předmětu Elektronické zabezpečování budov a možnosti zanešení některých subjektů do databáze biometrických systému již před 3 lety. Tento test byl pouze orientační a byl realizován na starších čtečkách iFace 302 a Multibio 700. Z naměřených hodnot vyplývá, že z 9 testovaných subjektů bylo rozpoznáno pouze 22,22 % subjektů (pouze 2 z 9 lidí). Hranice míry ztotožnění se pohybovala v rozmezí 25–55 %. Tato nízká míra rozpoznání uživatelů u těchto starších čteček po 3 letech je velmi znepokojivá. Případné negativní dopady mohou být zejména z hlediska v čase potřebném k identifikaci uživatelů, snížení míry spolehlivosti, nekorektní neidentifikování uživatelů, zvýšení případné frustrace z negativního výsledku identifikace a v neposlední řadě také možné zvýšení nákladů domácnosti/společnosti.

## Reference

- [1] Biometrie. *WikiPedia*. [Online] 4. 1 2017. [Citace: 6. 3 2017.] <https://cs.wikipedia.org/wiki/Biometrie>.
- [2] Romar Rak, Václav Matyáš, Zdeněk Říha a kolektiv. *Biometrie a identita člověka*. místo neznámé : GRADA, 2008. ISBN 8024723654.
- [3] Mgr. Ing. Radomír Ščurek, Ph.D. *Biometrické metody identifikace osob v bezpečnostní praxi*. 2008.
- [4] Doc. Mgr. Ing. Radomír Ščurek, Ph.D. *Biometrické technologie, technické prostředky bezpečnostních služeb*. 2015.
- [5] SRI. Face Recognition. *creativetechno.wordpress.com*. [Online] 18. 2 2012. [Citace: 6. 3 2017.] <https://creativetechno.wordpress.com/2012/02/18/face-recognition/>.
- [6] Beneš, R. Autentizační metody založené na biometrických informacích. *AccessServer*. [Online] 18. 11 2010. [Citace: 6. 3 2017.] <http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>.
- [7] Bureš, Jiří. Základní jednotky SI soustavy. *Converter.cz*. [Online] [Citace: 4. 3 2017.] <http://www.converter.cz/prevody/jednotky-si.htm>.
- [8] Face Recognition White Paper Technology. *fingertec.com*. [Online] [Citace: 6. 3 2017.] <http://www.fingertec.com/whatsnew/face-recognition-white-paper-technology-2>.
- [9] R., Vanaman E. Biometric facial recognition database systems“. *eforensicsmag.com*. [Online] 4. 9 2014. [Citace: 6. 3 2017.] <https://eforensicsmag.com/biometric-facial-recognition-database-systems/>.
- [10] Victor, Lavrenko. Basics of machine learning, PCA 10: eigen faces. *Basics of machine learning*. [Online] [Citace: 6. 3 2017.] <http://homepages.inf.ed.ac.uk/vlavrenk/iaml.html>.
- [11] Eigenface. *WikiPedia*. [Online] 9. 1 2017. [Citace: 6. 3 2017.] <https://en.wikipedia.org/wiki/Eigenface>.
- [12] Fjura. Neuronové sítě – vývoj a testování. *Shrimphood.net*. [Online] [Citace: 6. 3 2017.] <http://www.shrimphood.net/neuronove-site-vyvoj-a-testovani.html>.
- [13] Militello C., Rundo L., Gilardi C.M. Applications of image processing. *TCR*. [Online] 10 2014. [Citace: 6. 3 2017.] <http://tcr.amegroups.com/article/view/3200/html>.

- [14] Tan, Tamara Kisha. Mathematical portraits . *DesignTaxi*. [Online] 6. 4 2013. [Citace: 6. 3 2017.] <http://designtaxi.com/news/356912/Mathematical-Portraits-Of-Famous-People-Plus-A-Cat/advertise.html/>.
- [15] WON O. L., YEONG G.K., HYUNG G.H., KANG R.P. Face recognition system for set-top box-based intelligent TV. *MDPI- sensors*. [Online] 18. 11 2014. [Citace: 6. 3 2017.] <http://www.mdpi.com/1424-8220/14/11/21726Despite>.
- [16] J.E., Orthod. Three-dimensional quantification of facial symmetry. *Oxford Academics*. [Online] 27. 7 2011. [Citace: 7. 3 2017.] <https://academic.oup.com/ejo/article/36/2/125/453590/Three-dimensional-quantification-of-facial>.
- [17] Yosart. Lips geometric carcass polygonal line abstract. *Shutterstock*. [Online] [Citace: 7. 3 2017.] <https://image.shutterstock.com/z/stock-vector-lips-geometric-carcass-polygonal-line-abstract-313110416.jpg>.
- [18] Frederick G. Haibach, Ph.D. Lighting for Facial Biometrics. *visiononline.org*. [Online] 27. 9 2004. [Citace: 7. 3 2017.] [http://www.visiononline.org/vision-resources-details.cfm/vision-resources/Lighting-for-Facial-Biometrics/content\\_id/318](http://www.visiononline.org/vision-resources-details.cfm/vision-resources/Lighting-for-Facial-Biometrics/content_id/318).
- [19] Mrinal Kanti Bhowmik, Kankan Saha, Sharmistha Majumder a kolektiv. Thermal infrared face recognition. *InTech*. [Online] 27. 7 2011. [Citace: 7. 3 2017.] <http://www.intechopen.com/books/reviews-refinements-and-new-ideas-in-face-recognition/thermal-infrared-face-recognition-a-biometric-identification-technique-for-robust-security-system>.
- [20] Voženílek, Jan. Elektromagnetické spektrum. *jan.gfxs.cz*. [Online] 11 2006. [Citace: 7. 3 2017.] <http://jan.gfxs.cz/studium/files/optika/spektrum.pdf>.
- [21] Elektromagnetické spektrum. *WikiPedia*. [Online] 10. 2 2016. [Citace: 7. 3 2017.] [https://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9\\_spektrum](https://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_spektrum).
- [22] Jaroslav Reichl, Martin Všetíčka. Světlo jako elektromagnetické vlnění. *Encyklopedie fyziky*. [Online] [Citace: 7. 3 2017.] <http://fyzika.jreichl.com/main.article/view/434-svetlo-jako-elektromagneticke-vlneni>.
- [23] Teplota chromatičnosti. *is.mendelu.cz*. [Online] [Citace: 7. 3 2017.] [https://is.mendelu.cz/eknihovna/opory/zobraz\\_cast.pl?cast=9104](https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=9104).
- [24] Typy světelných zdrojů. *WikiSkripta*. [Online] 11. 1 2016. [Citace: 7. 3 2017.] [http://www.wikiskripta.eu/index.php/Typy\\_sv%C4%9Bteln%C3%BDch\\_zdroj%C5%AF](http://www.wikiskripta.eu/index.php/Typy_sv%C4%9Bteln%C3%BDch_zdroj%C5%AF).

- [25] Valušík, Jan. Světlo, nasvícení scény. *fi.muni.cz*. [Online] [Citace: 7. 3 2017.] <http://www.fi.muni.cz/lemma/referaty/10/11.pdf>.
- [26] Princip fungování bílé LED. *WireliLed*. [Online] [Citace: 7. 3 2017.] <http://www.wireliled.cz/aplikacni-poznamky/princip-bile-led/>.
- [27] Niesig, Petr. LED světelné diody. *Elkovo-Cepelik*. [Online] [Citace: 7. 3 2017.] <http://www.elkovo-cepelik.cz/led-svetelne-diody-light-emitting-diodes>.
- [28] Brightest 5mm white LED. *ElectronicGoldmine*. [Online] [Citace: 7. 3 2017.] <http://www.goldmine-elec-products.com/prodinfo.asp?number=G17802>.
- [29] Requirements for a biometric passport photo. *idPhoto*. [Online] 26. 1 2017. [Citace: 7. 3 2017.] <https://www.idphoto.ch/help/passport-photo/requirements/>.
- [30] Přisvícení kamer. *kamerove-systemy-cplusplus.cz*. [Online] [Citace: 7. 3 2017.] <https://www.kamerove-systemy-cplusplus.cz/prisviceni-kamer>.
- [31] Agarval, Tarun. How to build a simple infrared illuminator. *ElProCus.com*. [Online] [Citace: 7. 3 2017.] <https://www.elprocus.com/simple-infrared-illuminator/>.
- [32] How night vision works. *sofradir-ec.com*. [Online] [Citace: 7. 3 2017.] <http://sofradir-ec.com/hownightvisionworks/#NII>.
- [33] A., TARHINI. Face Recognition: A introduction. *alitarhini.wordpress.com*. [Online] 5. 12 2010. [Citace: 7. 3 2017.] <https://alitarhini.wordpress.com/2010/12/05/face-recognition-an-introduction/>.
- [34] Infračervené záření. *WikiPedia*. [Online] 2. 3 2017. [Citace: 7. 3 2017.] [https://cs.wikipedia.org/wiki/Infra%C4%8Derven%C3%A9\\_z%C3%A1r%C5%99en%C3%AD](https://cs.wikipedia.org/wiki/Infra%C4%8Derven%C3%A9_z%C3%A1r%C5%99en%C3%AD).
- [35] Mainguet, Jean Francois. Biometrics - Facial thermogram. [Online] 4. 3 2016. [Citace: 7. 3 2017.] <http://biometrics.mainguet.org/types/face.htm>.
- [36] Infrared camera enables reliable facial recognition. [Online] 24. 11 2015. [Citace: 7. 3 2017.] <https://www.alliedvision.com/en/news/detail/news/infrared-camera-enables-reliable-facial-recognition.html>.
- [37] Tariq Manzur, Aravinda Kar. Infrared imaging at high temperatures. *SPIE.org*. [Online] 27. 12 2012. [Citace: 7. 3 2017.] <http://spie.org/newsroom/4553-infrared-imaging-at-high-temperatures>.
- [38] K., Kadlec. Měřící a řídicí technika. *docplayer.cz*. [Online] 23. 2 2016. [Citace: 7. 3 2017.] <http://docplayer.cz/18201081-80-400-sirokopasmove-zachyceni-veskereho-teplotniho.html>.

- [39] Termografie. *WikiPedia*. [Online] 11. 10 2016. [Citace: 7. 3 2017.]  
<https://cs.wikipedia.org/wiki/Termografie>.
- [40] Infračervené přisvícení. *huntermann.com*. [Online] [Citace: 7. 3 2017.]  
<http://www.hutermann.com/eshop/001/produkty/infracervene-prisviceni>.
- [41] INFRAČERVENÝ LED REFLEKTOR KINGBRIGHT . *fonetip.cz*. [Online] [Citace: 7. 3 2017.] <http://www.fonetip.cz/infracerveny-led-reflektor-kingbright-bl0106-15-28-940-n-p14871?gclid=CLPUIInfxNICFY4GwodKM8HSA>.
- [42] GE Hardglass infrared reflector with ruby filter. *lamptech.co.uk*. [Online] 4. 1 2017. [Citace: 7. 3 2017.] <http://www.lamptech.co.uk/Spec%20Sheets/IN%20R%20120-250R40IRR-E26%20GE.htm>.
- [43] Laser. *WikiPedia*. [Online] 7. 2 2017. [Citace: 7. 3 2017.] <https://cs.wikipedia.org/wiki/Laser>.
- [44] Laserová dioda IR 780nm 5mW. *laser-shop.cz*. [Online] [Citace: 7. 3 2017.] <http://laser-shop.cz/cs/laser-diody/790-laserova-dioda-ir-780nm-5mw-.html?gclid=CPy7ob7gxNICFQ4TGwodjNIPjw>.
- [45] iFace302. *ZKteco.com*. [Online] [Citace: 5. 3 2017.]  
[https://www.zkteco.com/product/iFace302\\_218.html](https://www.zkteco.com/product/iFace302_218.html).
- [46] iFace Series User Manual. *eattendance.net*. [Online] 1 2010. [Citace: 6. 3 2017.]  
<https://www.eattendance.net/Iface302-facial-time-attendance-device-user-manual.pdf>.
- [47] Multibio700. *ZKteco.com*. [Online] [Citace: 5. 3 2017.]  
[https://www.zkteco.com/product/MultiBio700\\_241.html](https://www.zkteco.com/product/MultiBio700_241.html).
- [48] Multibio 700 User Manual. *etas.ro*. [Online] 11 2010. [Citace: 6. 3 2017.]  
<http://www.etas.ro/docs/AccessControl/ZK/Manuale/Multi-Bio700-User-Manual.pdf>.
- [49] Multibio 700 - product description. *masterbc.co.rs*. [Online] [Citace: 6. 3 2017.]  
[http://www.masterbc.co.rs/dokumenta/2731\\_2.pdf](http://www.masterbc.co.rs/dokumenta/2731_2.pdf).
- [50] AccuFACE EFR-T1 Series Facial Recognition System. *PSPsecurity.com*. [Online] [Citace: 5. 3 2017.] [http://www.pspsecurity.com/products\\_contents.php?products\\_id=2](http://www.pspsecurity.com/products_contents.php?products_id=2).
- [51] AccuFace - Series Features. *PSPsecurity.com*. [Online] [Citace: 6. 3 2017.]  
<http://www.pspsecurity.com/download/AccuFACE%20EFR&FS%20Series%20DM.pdf>.
- [52] AccuFace EFR-T1x - User Guides (Quick Start Guide, QSG). *PSPsecurity*. [Online] [Citace: 6. 3 2017.] <http://www.pspsecurity.com/support.php>.

- [53] Aktion AFT-500. *shop.efg.cz*. [Online] [Citace: 5. 3 2017.] <http://shop.efg.cz/z19476-aft-500>.
- [54] AFT-500 - katalogový list (PDF). *shop.efg.cz*. [Online] [Citace: 6. 3 2017.] <http://shop.efg.cz/z19476-aft-500>.
- [55] Luxmetr. *ET-pocitacovesystemy*. [Online] 2017. [Citace: 4. 3 2017.] [http://www.et-pocitacovesystemy.wz.cz/elektronicke\\_pristroje/luxmetr.html](http://www.et-pocitacovesystemy.wz.cz/elektronicke_pristroje/luxmetr.html).
- [56] Ing. Henrietta PŘIBÁŇOVÁ, MUDr. Ariana LAJČÍKOVÁ, CSc. Umělé osvětlení vnitřního prostředí. *TZB-info.cz*. [Online] 3. 1 2003. [Citace: 4. 3 2017.] <http://elektro.tzb-info.cz/osvetleni/1303-umele-osvetleni-vnitriho-prostredi>.
- [57] Jednotka svítivosti - kandela. *Fyzmatik.pise.cz*. [Online] 27. 9 2009. [Citace: 4. 3 2017.] <http://fyzmatik.pise.cz/45-jednotka-svitivosti-kandela.html>.
- [58] Digitální luxmetr CEM DT-8809. *GME.cz*. [Online] [Citace: 4. 3 2017.] <https://www.gme.cz/digitalni-luxmetr-cem-dt-8809>.
- [59] DT-8808/8809A. *CEM-instruments*. [Online] [Citace: 4. 3 2017.] <http://www.cem-instruments.com/en/Product/detail/id/799/pid/808;/pids/1312>.
- [60] LED PÁSEK 5M RGB 30 LED/M, 36W. *smdLEDzarovky.cz*. [Online] [Citace: 6. 3 2017.] <https://www.smdledzarovky.cz/led.pasky.a.moduly/led.pasky.sady/led.pasek.5m.rgb.30.ledm.36w.i.p20.44.tlacitek.sada?gclid=CJanjbHbwdICFTAz0wodX7YHdQ>.
- [61] Ovládání třibarevné LED – RGB. *ELUC.kr-olomoucky.cz*. [Online] [Citace: 6. 3 2017.] <https://eluc.kr-olomoucky.cz/verejne/lekce/921>.
- [62] SMD led flexible light strip . *wayjun.com*. [Online] [Citace: 6. 3 2017.] [http://www.wayjun.com/index.php?main\\_page=product\\_info&cPath=45&products\\_id=697&zenid=c58558e799a29867ca83c44089445511](http://www.wayjun.com/index.php?main_page=product_info&cPath=45&products_id=697&zenid=c58558e799a29867ca83c44089445511).
- [63] Ing. Veronika Hartová, Ph.D. Biometrické identifikační systémy. *Disertační práce*. Praha, 2014.
- [64] Vinson, Dano. CAD Sitting Figure. *GrabCad.com*. [Online] 11. 12 2012. [Citace: 5. 3 2017.] <https://grabcad.com/library/sitting-figure>.

## Seznam příloh

Příloha 1 - průměrná doba identifikace – bez přísvitu .....	I
Příloha 2 - průměrná doba identifikace – v červeném přísvitu .....	I
Příloha 3 - průměrná doba identifikace – v zeleném přísvitu .....	I
Příloha 4 - průměrná doba identifikace – v modrém přísvitu .....	II
Příloha 5 - průměrná doba identifikace – v bílém přísvitu.....	II
Příloha 6 - průměrná doba identifikace na č.1 (dle užitého spektra).....	III
Příloha 7 - průměrná doba identifikace na č.2 (dle užitého spektra).....	III
Příloha 8 - průměrná doba identifikace na č.3 (dle užitého spektra).....	III
Příloha 9 - průměrná doba identifikace na č.4 (dle užitého spektra).....	IV



## Seznam obrázků

Obrázek 1 - Základní biometrické markanty tváře.....	6
Obrázek 2 - Princip biometrického porovnávání .....	7
Obrázek 3 - Proces vytvoření šablony tváře .....	7
Obrázek 4 - Proces identifikace .....	8
Obrázek 5 - Proces verifikace .....	9
Obrázek 6 - Charakteristiky FAR, FRR, ERR a ideální ERR.....	10
Obrázek 7 - Obecný přístup zpracování tváří 2D technikou .....	11
Obrázek 8 - Obecný přístup zpracování tváří 3D technikou .....	12
Obrázek 9 - Markanty na obličejích.....	14
Obrázek 10 - Analyticko-statistická metoda .....	15
Obrázek 11 - Grafická metoda .....	16
Obrázek 12 - PCA, Eigenface .....	19
Obrázek 13 - Eigenhead .....	19
Obrázek 14 – Model neuronu.....	21
Obrázek 15 - Neuronová síť.....	22
Obrázek 16 - Detekce obličeje na principu rozložení šedi.....	23
Obrázek 17 - Pohyb na scéně .....	24
Obrázek 18 - Odhadnutí výsledné tváře při změně pohybu na základě optického toku .....	25
Obrázek 19 - Kontury obličeje, vyjádřitelné matematickými funkcemi .....	25
Obrázek 20 - Příklad histogramu obličeje.....	26
Obrázek 21 - Symetrie obličeje.....	27
Obrázek 22 - Porovnávané markanty obličeje .....	28
Obrázek 23 - Deformační model rtů .....	28
Obrázek 24 - Deformační modely .....	29
Obrázek 25 - Rozdíl mezi využitím a nevyužitím přisvitu .....	30
Obrázek 26 - Elektromagnetické spektrum.....	30
Obrázek 27 - Viditelné spektrum, barvy .....	31
Obrázek 28 - Viditelné spektrum, barva světla v závislosti na teplotě .....	31
Obrázek 29 - Schématická značka, PN přechod, LED dioda.....	33
Obrázek 30 - LED, RGB barvy a bílá barva .....	34
Obrázek 31 - Ukázky špatného a správného nasvícení .....	35
Obrázek 32 - Orientace stínů.....	35
Obrázek 33 - Ideální podmínky nasvícení .....	36
Obrázek 34 - Obecný princip IR snímání .....	38

Obrázek 35 - Detailnější postup IR snímání (short-wave IR kamera), vč. synchronizace.....	38
Obrázek 36 - Zobrazení obličeje při odlišném IR spektru .....	39
Obrázek 37 - Emisivita .....	40
Obrázek 38 - Termogram.....	40
Obrázek 39 - Přisvit IR LED.....	42
Obrázek 40 - Přisvit IR lampy/žárovky .....	42
Obrázek 41 - Přisvit IR laser.....	43
Obrázek 42 - Rozpoznání živé kůže.....	44
Obrázek 43 - Biometrická čtečka - iFace 302.....	46
Obrázek 44 - Biometrická čtečka - Multibio 700.....	47
Obrázek 45 - Biometrická čtečka - AccuFace EFR-T1.....	48
Obrázek 46 - Biometrická čtečka - Aktion AFT-500.....	49
Obrázek 47 – Luxmetr, CEM-DT 8809A .....	50
Obrázek 48 - Přisvit - LED RGB pásek .....	51
Obrázek 49 a) dálkový ovladač přisvitu b) IR čidlo dálkového ovladače.....	51
Obrázek 50 - Schematické znázornění laboratorního panelu.....	55
Obrázek 51 - Schematické znázornění měření z profilu .....	55

## Seznam tabulek

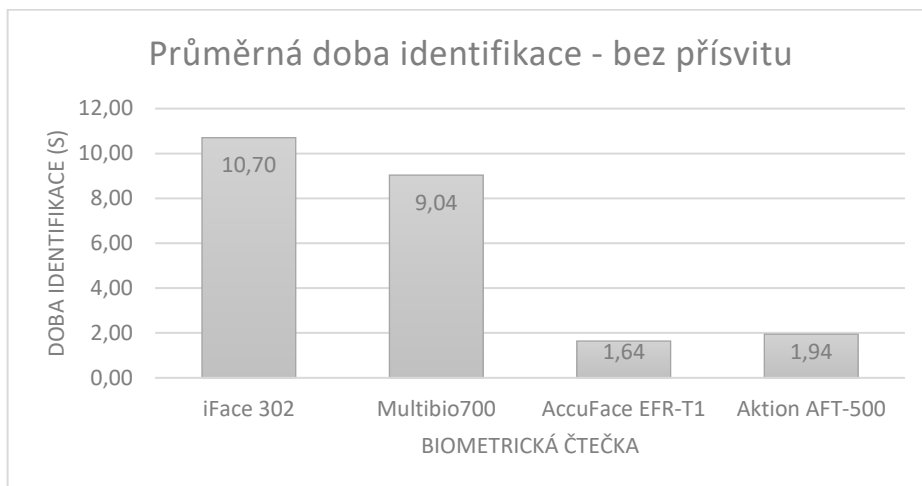
Tabulka 1 - Klady/Zápory 2D technologie zpracování tváří.....	12
Tabulka 2 - Klady/Zápory 3D technologie zpracování tváří.....	13
Tabulka 3 - Hodnoty z měření jednoho testovaného subjektu na č. iFace 302 .....	61
Tabulka 4 - Hodnoty z měření jednoho testovaného subjektu na č. Multibio 700.....	61
Tabulka 5 - Hodnoty z měření jednoho testovaného subjektu na č. AccuFace EFR-T1.....	62
Tabulka 6 - Hodnoty z měření jednoho testovaného subjektu na č. Aktion AFT-500.....	62
Tabulka 7 - Naměřené hodnoty osvitů jednotlivých přísvitů .....	64
Tabulka 8 - Test rozpoznání subjektů po 3 letech na č.1 a č.2.....	65
Tabulka 9 - Naměřené hodnoty neidentifikovaných pokusů, přípustné hranice (10s, 5s, 3s, 2s), výpočet FRR .....	70

## Seznam grafů

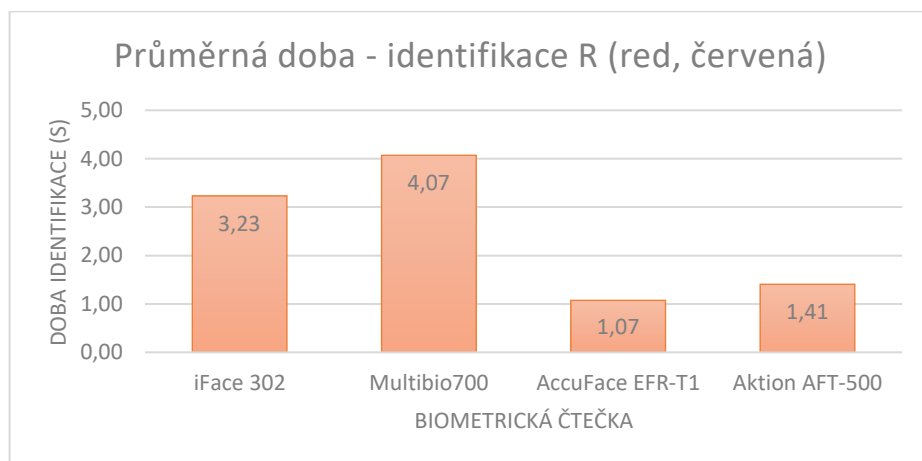
Graf 1 - Průměrná doba identifikace (souhrn) .....	67
Graf 2 - Průměrná doba identifikace (souhrn), starší čtečky (č.1 a č.2).....	68
Graf 3 - Průměrná doba identifikace (souhrn), novější čtečky (č.3 a č.4).....	68
Graf 4 - Spolehlivost, hranice nastavena na 10s, (FRR) starší čtečky (č.1 a č.2) .....	71
Graf 5 - Spolehlivost, hranice nastavena na 5s, (FRR) starší čtečky (č.1 a č.2) .....	72
Graf 6 - Spolehlivost, hranice nastavena na 3s, (FRR) novější čtečky (č.3 a č.4) .....	73
Graf 7 - Spolehlivost, hranice nastavena na 2s, (FRR) novější čtečky (č.3 a č.4) .....	74

# Přílohy

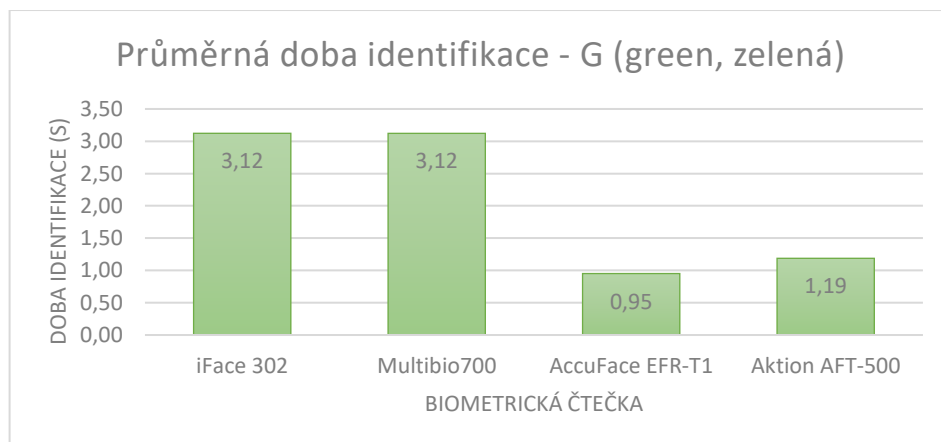
*Příloha 1 - průměrná doba identifikace – bez přisvitu*



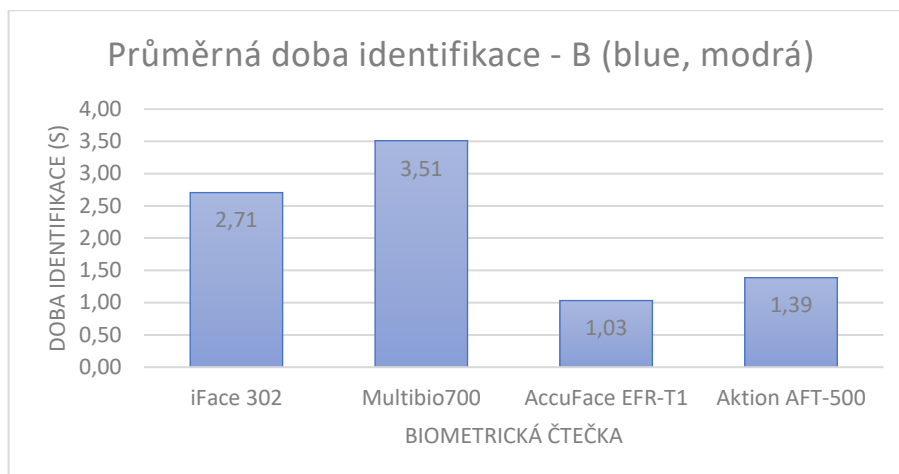
*Příloha 2 - průměrná doba identifikace – v červeném přisvitu*



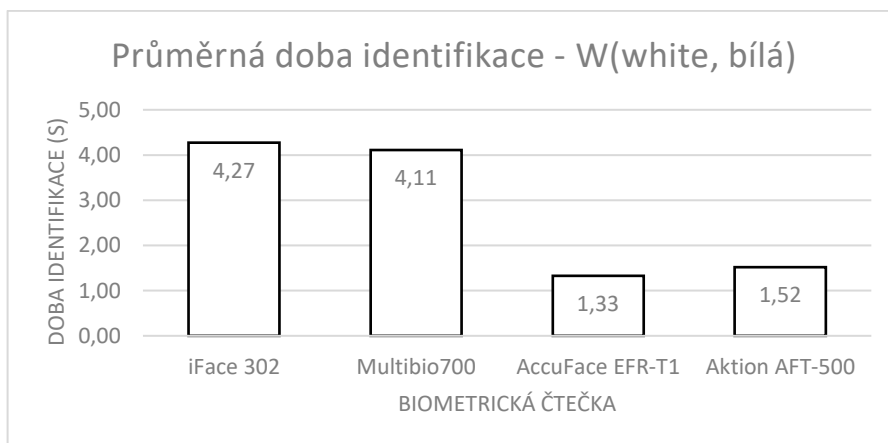
*Příloha 3 - průměrná doba identifikace – v zeleném přisvitu*



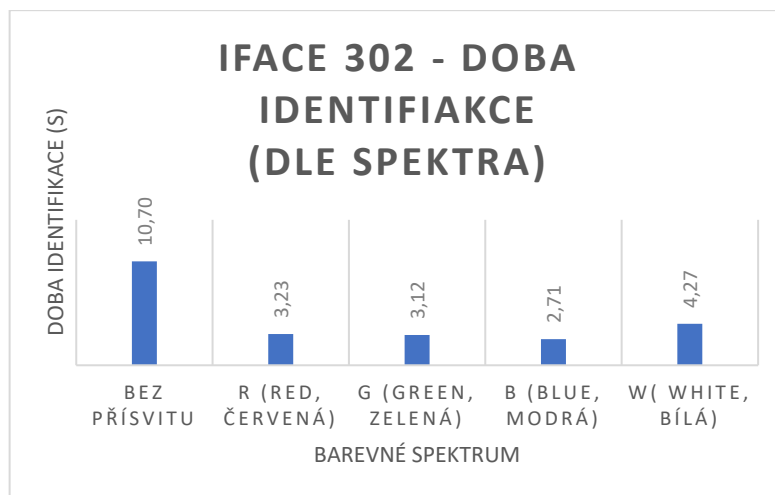
Příloha 4 - průměrná doba identifikace – v modrém přisvitu



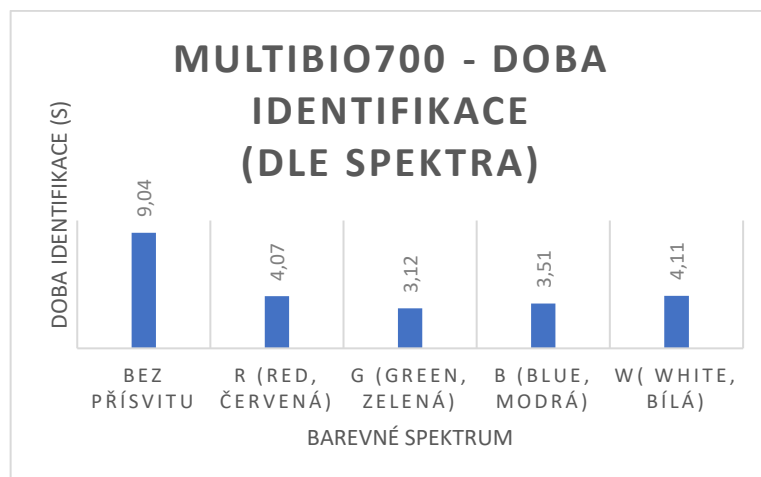
Příloha 5 - průměrná doba identifikace – v bílém přisvitu



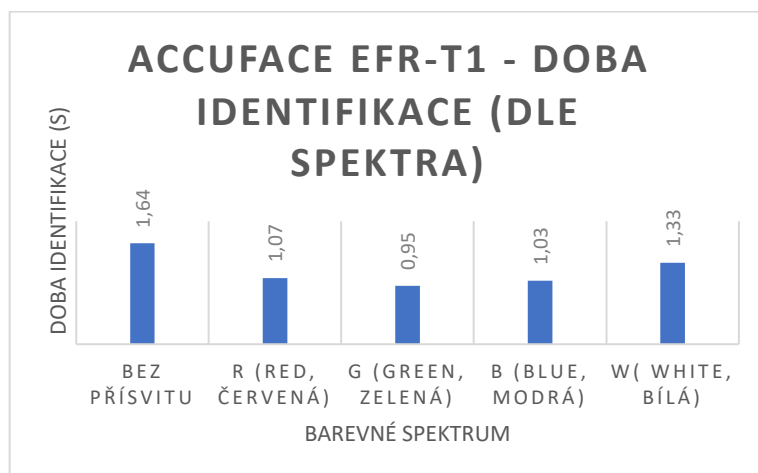
Příloha 6 - průměrná doba identifikace na č.1 (dle užitého spektra)



Příloha 7 - průměrná doba identifikace na č.2 (dle užitého spektra)



Příloha 8 - průměrná doba identifikace na č.3 (dle užitého spektra)



Příloha 9 - průměrná doba identifikace na č.4 (dle užitého spektra)

