

Česká zemědělská univerzita v Praze

Technická fakulta

**Spolehlivost systémů identifikující osoby na základě skenu  
krevního řečiště za ztížených podmínek**

bakalářská práce

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

Autor práce: Viktorija Miščenko

Praha 2020

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Viktorija Miščenko

Informační a řídicí technika v agropotravinářském komplexu

Název práce

**Spolehlivost systémů identifikující osoby na základě skenu krevního řečiště za ztížených podmínek**

Název anglicky

**Reliability of systems identifying a person based on the scan bloodstream under difficult conditions**

---

### Cíle práce

Cílem bakalářské práce je určit spolehlivost systémů identifikující osobu na základě krevního řečiště za ztížených podmínek.

### Metodika

Bakalářská práce se bude věnovat biometrickému identifikačnímu systému, který identifikuje osoby na základě skenu jejich krevního řečiště ruky. Budou stanoveny nejčastější nepříznivé podmínky, které mohou nastat v praxi, a za těchto podmínek bude probíhat testování.

Práce bude zpracována dle osnovy:

- 1 Úvod
- 2 Cíl a metodika práce
- 3 Přehled řešené problematiky
- 4 Praktická část práce
- 5 Závěr
- 6 Seznam použitých zdrojů
- 7 Přílohy

### **Doporučený rozsah práce**

30–50 str. včetně obrázků, tabulek a grafů

### **Klíčová slova**

krvní řečiště, biometrie, ztížené podmínky, čtečka

---

### **Doporučené zdroje informací**

Advances in user authentication. New York, NY: Springer Berlin Heidelberg, 2017. ISBN 9783319588063.

DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 9788025489796.

KANICH, Ondřej. Fingerprint damage simulation: a simulation of fingerprint distortion, damaged sensor, pressure and moisture. Saarbrücken: Lambert academic publishing, 2014. ISBN 9783659639425

MATYÁŠ, V. – RAK, R. – ŘÍHA, Z. *Biometrie a identita člověka ve forezních a komerčních aplikacích*. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

RATHGEB, Christian, Andreas UHL a Peter WILD. Iris biometrics: from segmentation to template security. New York: Springer, [2013]. ISBN 9781461455707.

---

### **Předběžný termín obhajoby**

2019/2020 LS – TF

### **Vedoucí práce**

Ing. Veronika Hartová, Ph.D.

### **Garantující pracoviště**

Katedra vozidel a pozemní dopravy

---

Elektronicky schváleno dne 21. 1. 2019

**Ing. Martin Kotek, Ph.D.**

Vedoucí katedry

---

Elektronicky schváleno dne 15. 2. 2019

**doc. Ing. Jiří Mašek, Ph.D.**

Děkan

V Praze dne 18. 12. 2019

### Čestné prohlášení

*„Prohlašuji, že jsem diplomovou/bakalářskou práci na téma: **„Spolehlivost systémů identifikující osoby na základě skenu krevního řečiště za ztížených podmínek“** vypracoval/a samostatně a použil/a jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.*

*Jsem si vědom/a, že odevzdáním bakalářské 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/a, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.*

*Jsem si vědom/a že, na moji bakalářskou 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.“*

V Praze dne .....

.....

Viktorija Miščenko

## Poděkování

*Mé poděkování patří Ing. Veronice Hartové, Ph.D. za odborné vedení práce, věcné připomínky a vstřícnost při konzultacích a vypracování. Dále bych ráda poděkovala pracovníkům Fujitsu Technology Solutions s.r.o. za poskytnutí odborných informací týkajících se této práce. Také chci poděkovat všem, kdo se zúčastnil měření praktické části práce.*

**Abstrakt:** Bakalářská práce je zaměřena na testování spolehlivosti systémů identifikujících osoby pomocí krevního řečiště ruky, konkrétně dlaně. Na začátku je práce věnována definování a vysvětlení důležitých pojmů v oblasti biometrie a biometrických systémů, jako jsou identifikace a verifikace. Také jsou zde popsány bezpečnostní charakteristiky FAR a FRR a definovány jejich výpočty. Dále se práce zabývá základním přehledem a popisem nejvyužívanějších biometrických metod identifikace osob v bezpečnostně-komerční sféře. Konec literární rešerše je věnován metodě identifikace osob pomocí snímání krevního řečiště ruky a také popisu technologie PalmSecure. Praktická část práce je věnována popisu ztížených podmínek měření provedeného za použití technologie PalmSecure, a dále také zpracováním a vyhodnocením výsledků tohoto měření.

**Klíčová slova:** krevní řečiště; biometrie; ztížené podmínky; čtečka

***Reliability of systems identifying persons based on a palm vein scan under difficult conditions***

**Summary:** The bachelor thesis is focused on testing the reliability of the systems of identification of persons using the blood circulation of the hand, specifically the palm. In the beginning, the thesis is devoted to the definition and explanation of important terms in the field of biometry and biometric systems such as identification and verification. Also, the safety characteristics FAR and FRR are described and their calculations are defined. Furthermore, the thesis deals with the basic overview and description of the most commonly used biometric methods of identification of persons in the commercial security sphere. The conclusion of the literary research is devoted to the method of person identification by scanning the blood circulation of the hand and also to the description of PalmSecure technology. The practical part of the thesis is devoted to the description of difficult conditions of measurement performed using PalmSecure technology, as well as processing and evaluation of the results of this measurement.

**Key words:** *palm vein; biometrics; difficult conditions; reader*

## Obsah

1. Úvod .....	1
2. Cíl práce .....	3
3. Metodika práce .....	4
4. Literární rešerše .....	5
4.1. Identita, identifikace a verifikace.....	5
4.2. Biometrie a biometrický systém .....	6
4.2.1. FRR a FAR.....	8
4.3. Identifikace na základě behaviorálních biometrických charakteristik.....	9
4.3.1. Hlas.....	9
4.3.2. Podpis a písmo.....	10
4.3.3. Chůze.....	11
4.4. Identifikace na základě anatomicko-fyziologických charakteristik.....	12
4.4.1. Tvář .....	12
4.4.2. Oko.....	12
4.4.3. Ruka.....	13
4.4.3.1. Geometrie ruky.....	14
4.4.3.2. Otisk prstu .....	15
4.4.3.3. Otisk dlaně.....	18
4.5. Identifikace na základě skenu krevního řečiště.....	19
4.5.1. Krevní řečiště prstu.....	19

4.5.2.	Krevní řečiště hřbetu ruky .....	20
4.5.3.	Krevní řečiště dlaně .....	20
4.5.4.	PalmSecure .....	21
5.	Praktická část práce.....	24
5.1.	Podmínky měření .....	24
5.2.	Popis použitých nástrojů .....	24
5.3.	Postup měření a získávání dat .....	28
5.4.	Popis ztížených podmínek .....	28
5.5.	Popis zpracování získaných dat.....	29
6.	Zhodnocení výsledků .....	30
6.1.	Sensor Lifebook U747.....	30
6.2.	Sensor V2 s vodítkem U-Guide .....	32
7.	Závěr .....	35
8.	Seznam použitých zdrojů .....	38
8.1.	Seznam obrázků .....	42
8.2.	Seznam tabulek.....	43
8.3.	Seznam vzorců .....	43
8.4.	Seznam použitých zkratk .....	43
9.	Seznam příloh.....	44



## 1. Úvod

Informace jsou v současné době velice hodnotnou komoditou ve všech oblastech. Ochrana médií, na kterých se tyto informace ukládají, je ze strany vlastníka velice žádaná, proto se požadavky ke správě přístupů k informacím, systémům a fyzickým přístupům stále zpřísňují. Tyto přístupy se dělí podle způsobu identifikace na základě vlastnictví, znalostí a biometrických charakteristik.

Mezi nejrozšířenější způsoby patří ověření identity na základě vlastnictví získaných či přidělených charakteristik. Do této sféry patří osobní doklady, přístupové karty a čipy, biočipy atp., na jejichž základě se ověřuje identita člověka.

Dalším běžně používaným způsobem identifikace je ověření pomocí znalostí dané osoby. Nejrozšířenější jsou metody s použitím hesla či PIN kódu, dále také rodným číslem, číslem ID apod.

Dnes většina organizací používá hesla, karty a jejich kombinace, aby lidé pomocí těchto zabezpečovacích metod prokázali svou totožnost a oprávnění na přístup k zabezpečeným objektům. Tyto znalostní metody a metody založené na vlastnictví čelí hned několika rizikům – může dojít ke ztrátě či poškození karty/čipu, prozrazení či prolomení hesla/PIN kódu.

Biometrické systémy jsou dnes proto nedílnou součástí zabezpečení a ochrany dat a řadí se mezi standardní ochranné prvky. Přístupy na základě biometrických charakteristik mají výhodu v tom, že nemohou být odcizeny či zapomenuty. Avšak některé biometrické systémy se stále setkávají s nedokonalostmi, jako je například falzifikace biometrických identifikačních údajů.

Metody identifikace na základě biometrických charakteristik se dělí na behaviorální a anatomicko-fyziologické. Behaviorální biometrické charakteristiky jsou založeny na specifických znacích chování dané osoby, nejsou tedy příliš objektivní oproti anatomicko-fyziologickým charakteristikám, která jsou časově stálá a jedinečná.

Mezi nejběžnější behaviorální biometrické charakteristiky z pohledu použití v praxi se dnes řadí podpis a písmo, hlas a chůze. Mezi nejrozšířenější vrozené charakteristiky patří otisk prstu, oční duhovka a sítnice, tvář, geometrie ruky a krevní řečiště dlaně či prstu.

Biometrické systémy založené na charakteristice krevního řečiště dlaně se postupem času začínají dostávat do popředí biometrických metod používaných v praxi. Důvodem je jednoduché použití a velice obtížné prolomení tohoto systému, tedy větší míra bezpečnosti.

Jedna z technologií používající tuto metodu identifikace je technologie PalmSecure. Jelikož tato technologie stále není dostatečně rozšířená, lidé se s ní nesečkají příliš často. Cílem této práce je zjistit, zda je tato technologie univerzální a mohla by nahradit jiné více rozšířené biometrické. Výsledku se dosáhne pomocí měření a nastaveným podmínkám, které by mohly nastat během užívání této metody v praxi. Od výsledků testování je očekáváno, že systém bude velice spolehlivý i navzdory ztížených podmínek a potvrdí se jeho všestrannost použití.

## 2. Cíl práce

Cílem této bakalářské práce je otestování spolehlivosti biometrického systému skenu krevního řečiště dlaně za ztížených podmínek, které mohou být překážkou při použití této biometrické metody v praxi. Budou otestovány dva různé sensory za pomoci technologie PalmSecure.

Mezi teoretické cíle práce patří vymezení zásadních pojmů z oblasti identifikace a biometrie, provedení rešerše a vypracování přehledu nejrozšířenějších biometrických metod identifikace osob a popis identifikace na základě skenu krevního řečiště dlaně.

### 3. Metodika práce

Práce bude provedena dle zadání následujícím způsobem:

Literární rešerše bude zaměřena na vysvětlení důležitých pojmů v oblasti biometrických systémů, dále se bude věnovat přehledu zásadních biometrických identifikačních systémů, jejich principů, výhod a nevýhod. Poté bude provedeno zpracování problematiky identifikace pomocí skenu krevního řečiště ruky a technologie PalmSecure.

V praktické části práce budou zpracovány výsledky systematického měření, která budou provedena na dvou odlišných čtečkách snímajících krevní řečiště ruky při použití technologie PalmSecure. Pro klíčové měření bude použit sensor s lepšími vlastnostmi snímání. Při měření na základě prvotního načtení a uložení datové mapy krevního řečiště ruky při podmínkách normálního použití čtečky se ověří identifikace a verifikace za ztížených podmínek pomocí testovací aplikace a bude porovnána úspěšnost prokázání identity. Tyto ztížené podmínky budou vyvolány pomocí změn teploty, záměrným zašpiněním a vytvořením překážky mezi povrchem dlaně a sensoru.

Výsledky měření budou zpracovány pomocí programu Statistica metodou ANOVA, konkrétně Fisherovým LSD testem diferencí a bude vypočítána směrodatná odchylka měření za daných ztížených podmínek.

## 4. Literární rešerše

V současném značně mobilním světě se člověk dokáže během krátké chvíle setkat s obrovským počtem neznámých osob. Je tedy stále problematičtější prověřit identitu dané osoby, a proto jsou využívány různé systémy identifikace osob. V posledních letech roste aplikování biometrických systémů identifikace osob kvůli větší míře zabezpečení.

### 4.1. Identita, identifikace a verifikace

Identita je dnes velice rozšířený pojem nejen v biometrii, ale i v ostatních vědních oborech. Jedná se o určitou nezaměnitelnou charakteristiku daného objektu. Obecně se mohou objekty popisovat různými způsoby. Některé charakteristiky mohou být naprosto stejné i u ostatních objektů, proto je potřeba volit charakteristiku takovou, která bude sama o sobě jedinečná a nezaměnitelná u každého objektu. [1]

Příkladem je například sériová výroba zařízení, která jsou naprosto identická z hlediska výroby. Každému takovému zařízení je přiděleno unikátní sériové číslo, které právě dodává jedinečnost neboli identitu zařízení. Z toho vyplývá, že každý objekt je jedinečný a totožný sám se sebou.

Identita osoby je velice mnohoznačný pojem, který může být určen z několika hledisek. Identita v sobě nese pouze vrozené biologické charakteristiky, ale také psychologické, filozofické a sociální vlastnosti osoby. Člověk, jakožto bytost, má od narození vlastní jedinečné a nezaměnitelné tělesné charakteristiky. Také nabývá vědomí o sobě samém neboli své osobnosti. Je zařazen do určité společnosti se specifickými rysy. Každý člověk vnímá svou identitu po svém, a i jeho identita je jinak vnímána okolím. [1]

S konceptem prokázání identity jsou spojeny dva pojmy – verifikace a identifikace (obr. 1).

Identifikace je proces, při kterém osoba sdělí svou určitou biometrickou charakteristiku, na jejímž základě se ověří identita osoby. Při tomto procesu dochází k porovnání rozpoznávaného vzorku se všemi vzorky v databázi (1 : N). Nevýhodou identifikace je časová náročnost u obzvláště rozsáhlých databází [1, 2].

Verifikace je prokázání shodnosti identity uvedené s identitou fyzickou. Při verifikaci osoba, která chce prokázat svou totožnost, musí poskytnout informaci o tom, jaká je její identita, a potvrdit tuto skutečnost požadovanou biometrickou charakteristikou (1 : 1). Podmínkou úspěšné verifikace je záznam, který je obsažen v databázi. [1, 2]

Obr. 1 Identifikace a verifikace



Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 9788025489796.

Je mnoho způsobů, jak člověk může prokázat svou identitu. Karty, čipy, průkazy totožnosti a podobné způsoby založené na vlastnictví jsou dnes stále často využívány, avšak začínají pomalu ustupovat kvůli integraci spolehlivějších biometrických systémů. [3]

#### 4.2. Biometrie a biometrický systém

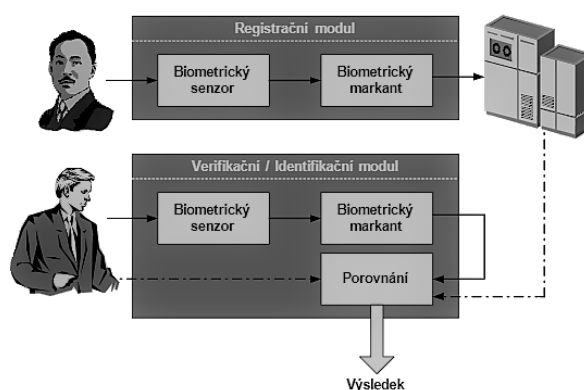
Biometrie je vědní obor, který se zabývá měřitelnými charakteristikami objektů a osob – tzv. biometrikami, s cílem jejich využití v praxi při prokazování identity. Identifikační metody založené na biometrických charakteristikách mají oproti ostatním metodám ověření hned několik výhod:

- Obtížná falzifikace/odcizení
- Časová stálost a jedinečnost
- Nedá se zapomenout či ztratit
- Uživatelský komfort
- Vyšší míra zabezpečení

Biometrické systémy jsou dnes vzhledem ke svým výhodám velice žádané a jsou na ně kladeny vysoké nároky z bezpečnostní stránky. Každý biometrický systém musí mít odpovídající strukturu, která je zobrazena na obr. 2. Skládá se ze dvou modulů – modul registrační a ověřovací modul. [2, 4]

Registrační modul slouží k prvotnímu načtení biometrické charakteristiky uživatele pomocí sensoru a zanesení referenční šablony – biometrického markantu do databáze či zařízení, kde jsou markanty uchovávány. K tomuto výkonu by mělo docházet pod dohledem oprávněné osoby. Modul ověřovací neboli identifikační/verifikační slouží k porovnání snímaných charakteristik s již uloženými markanty. V praxi oba dva moduly používají stejný hardware, avšak z hlediska software se jedná o dva různé objekty. [2, 4]

Obr. 2 Biometrický systém



Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Dražanský], 2011. ISBN 9788025489796.

K bezpečnostním rizikům může dojít hned na několika místech biometrického systému. Mezi zranitelná místa patří sensor, databáze či zařízení, na kterém jsou uloženy šablony, a samotná aplikace. Při snímání biometrických charakteristik senzorem může dojít k použití falzifikátu (např. uměle vyrobený otisk prstu). Samotná aplikace/software může být předmětem hackingu. A ačkoliv z markantů (šablon) uložených v databázi je obtížné získat zpět originální biometrickou charakteristiku, není to zcela nemožné. Je proto velice důležité řídit se pokyny a pravidly při registraci nových uživatelů a zamezit přístup neověřených osob k systémům a databázím. [2, 4]

Žádný biometrický systém není optimální, každý má své výhody i nevýhody, proto je při výběru systémů velice důležité vědět, kde bude aplikován. [5]

#### 4.2.1. FRR a FAR

V praxi při identifikaci či verifikaci je použito statistické vyhodnocení shodnosti mezi šablonou a snímanou biometrickou charakteristikou. Míra této shodnosti se nazývá skóre, jenž musí při prokazování identity převyšovat určitý práh citlivosti biometrické aplikace pro úspěšné přijetí. [2, 5]

Při výběru správné biometrické metody se posuzuje zejména její spolehlivost, která úzce souvisí se skóre. Nejdůležitějšími ukazateli jsou:

- FRR (False Rejection Rate)
- FAR (False Acceptance Rate)

FRR neboli pravděpodobnost chybného odmítnutí udává pravděpodobnost situace, kdy osoba oprávněná ke vstupu nebude rozpoznána. Z hlediska bezpečnosti se nejedná o rozhodující ukazatel, avšak pro uživatele je tato vlastnost nepříjemná, jelikož vyžaduje opětovné prokázání identity. [1]

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}} = \frac{\text{počet chybných odmítnutí}}{\text{počet pokusů oprávněných osob o identifikaci/verifikaci}} \quad (4.1)$$

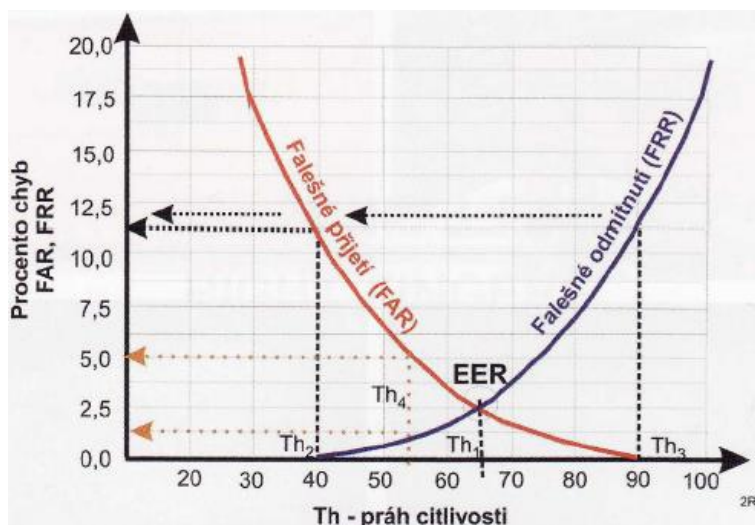
FAR neboli pravděpodobnost chybného přijetí udává pravděpodobnost, kdy systém povolí přístup neoprávněné osobě. Při vysoké hodnotě FAR se jedná o veliké bezpečnostní riziko [1, 6].

$$FAR = \frac{N_{FA}}{N_{IIA}} = \frac{N_{FA}}{N_{IVA}} = \frac{\text{počet chybných přijetí}}{\text{počet pokusů neoprávněných osob o identifikaci/verifikaci}} \quad (4.2)$$

Bohužel v praxi u reálných biometrických aplikací se nedá dosáhnout ideálního výsledku  $FAR = FRR = 0$ , je tedy potřeba nastavit takový práh citlivosti, aby bylo zamezeno vysokých hodnot FAR a FRR (obr. 3). [1, 6]



Obr. 3 Reálná biometrická aplikace



Zdroj: 1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

#### 4.3. Identifikace na základě behaviorálních biometrických charakteristik

Behaviorální biometrické charakteristiky se řadí mezi dynamické, založené na charakteristickém jednání osoby. Do této skupiny patří například hlas, podpis, chůze a dynamika stisku kláves. Oproti anatomicko-fyziologickým metodám, nejsou tak často využívány. [2]

##### 4.3.1. Hlas

Princip této metody spočívá v rozboru řečového signálu v časovém průběhu. Při mluvení ze sebe člověk vydává tzv. fonémy (zjednodušeně řečeno slova) různé rychlosti a frekvence. Při výdechu vzduchu procházejícího hlasovým ústrojím dochází k rozkmitání hlasivek. Řečový signál je poté zaznamenán mikrofonom, jsou analyzovány specifické akustické charakteristiky, a nakonec porovnány s uloženým vzorem. Po porovnání se vyčte skóre shodnosti a porovná s prahovou hodnotou. [1, 2]

Analýza hlasu, a především řeči do sebe zahrnuje mnoho aspektů. Může se provádět analýza obsahu řeči (porozumění, textově závislé), stav osoby (fyzický/psychický stav) a analýza hlasu pro identifikaci/verifikaci. [1, 2]

Systémy identifikující osoby na základě hlasu se dělí na závislé na obsahu textu a nezávislé na obsahu textu. Textově závislé systémy požadují heslo buď předem nastavené uživatelem, či heslo přednastavené samotným systémem. Více spolehlivé jsou systémy používající textovou výzvu, o které uživatel předem neví. Potenciální útok je tak složitější na provedení. Textově nezávislé systémy bývají méně přesné z důvodu malého množství vzorků při registraci uživatele, se kterými může systém porovnávat. [1, 2]

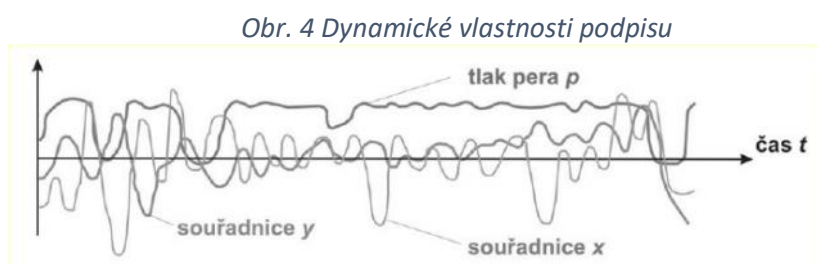
Takové systémy našly největší uplatnění ve sféře policejně-soudní, ale dnes jsou také využívány při telefonickém bankovníctví a obecně telekomunikacích. [2]

#### 4.3.2. Podpis a písmo

Další behaviorální metodou identifikace osob je rozbor ručně psaného písma. Systémy identifikace osob pomocí podpisu se dělí na off-line a on-line systémy.

Off-line systémy jsou statické systémy založeny na podpisu či písmu na papírové médium, které je poté oskenováno a uloženo jako referenční šablona. Autentičnost podpisu je určována podle jeho trajektorie a porovnání bodů (křížení, začátky a konce podpisu) v souřadnicovém systému  $x, y$ . [1, 6]

On-line dynamické systémy využívají speciálního zařízení pro automatickou digitalizaci a uložení podpisu (tablety, PDA záznamníky) a zaznamenávají nejen formu podpisu, ale i dynamické vlastnosti (obr. 4) jako jsou tlak pera ( $p$ ), rychlost tahu (souřadnice  $x$ ) a směr tahu (souřadnice  $y$ ) v čase ( $t$ ). [2, 6]



Zdroj: 1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

Tato biometrická metoda je spíše využívána při verifikaci uživatele z důvodu většího množství porovnávaných charakteristik podpisu. První fází je učení, kdy se vytváří referenční šablona pomocí extrahování charakteristik z co největšího možného počtu vzorků. Každé vytvořené šabloně je přiděleno ID číslo, které uživatel zadá při verifikaci. Druhá fáze je testovací, kdy je ze vstupního zařízení přijat podnět k verifikaci uživatele. Pořízená data jsou porovnána s referenční šablonou a na základě rozhodování podle prahu citlivosti poskytne aplikace výsledek. [1]

Tato biometrická metoda je dnes využívána v oblasti elektronických podpisů.

#### 4.3.3. Chůze

Identifikace na základě chůze spočívá na odlišné dynamice pohybu každého jedince. Chůze může být ovlivněna mnoha faktory: fyzický a psychický stav osoby, obuv, oblečení, a také vnější faktory okolí jako například osvětlení, dav či povrch, po kterém osoba jde. S rozvojem záznamových technologií se tato biometrická metoda využívá víc, avšak prozatím nejvíce ve forenzní oblasti. [2, 6]

Existuje několik způsobů identifikace osoby pomocí chůze. První způsob je založen na trajektorii pohybu těžiště nacházejícího se přibližně v oblasti jizvy pupeční, jehož poloha se mění při chůzi a vytváří křivku podobnou vlně. Protože ale těžiště není viditelné, jako záchytný bod bylo zvoleno temeno hlavy. [1]

Dalším způsobem je modelově orientovaný způsob zkoumající dynamiku pohybu celého těla pomocí tří různých modelů: drátěný, cylindrický a oválný. Od volby modelu se odvíjí efektivnost analýzy. Analyzují se rozměry a úhly těla při chůzi. [1]

Třetí způsob identifikace pomocí chůze je založen na zkoumání pohybu siluety osoby a délek kontur siluety. [1]

Výhodami použití této biometrické charakteristiky při ověření identity je bezkontaktnost a možnost ověření na větší vzdálenost. Nevýhodou této metody velké množství charakteristik chůze. Zatím nebyl vyvinut optimální systém pro identifikaci na základě chůze použitelný v bezpečnostně-komerční sféře. [2]

#### 4.4. Identifikace na základě anatomicko-fyziologických charakteristik

Více využívané metody jsou založeny na anatomicko-fyziologických vlastnostech, které jsou v závislosti na lidském chování neměnné. Jedná se o vrozené a jedinečné, z větší části časově stálé biometrické charakteristiky. Nejčastější způsoby ověření identity jsou na základě otisku prstu či ruky, rozpoznání tváře, oční duhovky či sítnice a topografií žil zápěstí. Mezi méně používané metody (např. použití ve sféře policejně-soudní) se řadí identifikaci na základě DNA, rozměrů a váhy těla, geometrie ruky, pach lidského těla a další. Jelikož je takových charakteristik mnoho, v této práci budou popsány pouze metody využívané v bezpečnostně-komerční sféře. [1, 2]

##### 4.4.1. Tvář

Podle tváře člověk intuitivně rozpoznává ostatní každý den a je to jedna z nejpřirozenějších metod identifikace. Strojová identifikace na základě obličeje se dělí na rozpoznání podle 2D snímku, 3D snímku a termosnímku obličeje. Nejvíce rozšířená metoda ve sféře přístupů je metoda rozpoznávání pomocí 2D snímku. [1, 2]

Prvním krokem identifikace je detekování a lokalizace obličeje dané osoby, ze kterého je vyextrahován referenční snímek obličeje. Poté následuje porovnání s údaji v databázi a výpočet shodnosti. Existuje více způsobů, podle kterých se mohou porovnávat tyto snímky: statistická metoda PCA (Principal Component Analysis) a LDA (Linear Discriminant Analysis), neuronové sítě, systémy strojového učení a další. Vyhovující metoda se volí v závislosti na prostředí, kam se takový biometrický systém aplikuje. [2]

Výhodou této metody je bezkontaktnost a poměrně malá cena hardwaru, proto se hojně využívá v mobilních zařízeních, avšak největší zastoupení má v kriminalistice. [1]

##### 4.4.2. Oko

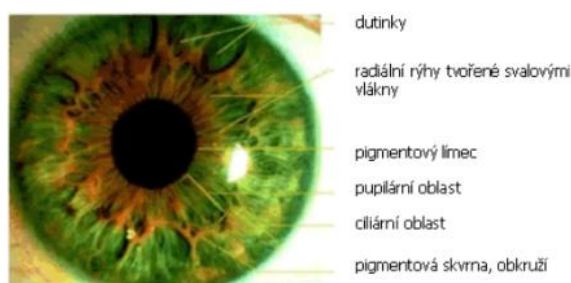
Další rozšířenou metodou identifikace osob je na základě charakteristik oční bulvy – obraz sítnice a oční duhovky.

Sítnice je fotosensitivní vrstva nacházející se v zadní části oční bulvy tvořena fotoreceptory – tyčinkami a čípkami, které vedou informace do mozku. Tato vrstva je zásobována krví pomocí cév vytvářejících specifickou strukturu. [1]

Principem metody je zaměření paprsku světla na sítnici, přičemž se odrazí obraz sítě cév, která je hlavním markantem při identifikaci osob pomocí sítnice. Poté je pomocí CCD kamery pořízen snímek tohoto odrazu (stejný princip je využíván v lékařství u retinoskopu). Z tohoto kruhového snímku je vytvořen referenční záznam, na jehož základě dochází k porovnání při identifikaci či verifikaci. [1, 2]

Oční duhovka je viditelná část oka nacházející se mezi bělimou a zornicí. Její struktura je u každé osoby jedinečná a je tvořena různými charakteristickými rysy (obr. 5). Její funkcí je regulace množství světla vstupujícího dovnitř oka. Barva duhovky je ovlivněna množstvím melaninu. [1, 2]

Obr. 5 Popis struktury duhovky



Zdroj 6. ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. Ostrava, [Online] 2008. [cit. 2020-02-03]

Princip systémů identifikace osob za použití duhovky je založen na snímku oka pomocí CCD kamery s využitím infračerveného světla s vlnovou délkou 700-900 nm. Na tomto snímku je duhovka lokalizována a markanty jsou extrahovány do fázorových diagramů, které jsou následně porovnávány s šablonou uloženou v databázi. [1, 6]

Tyto biometrické systémy se řadí mezi velice spolehlivé metody ověření identity a využívají se v místech, kde je požadována vysoká míra zabezpečení.

#### 4.4.3. Ruka

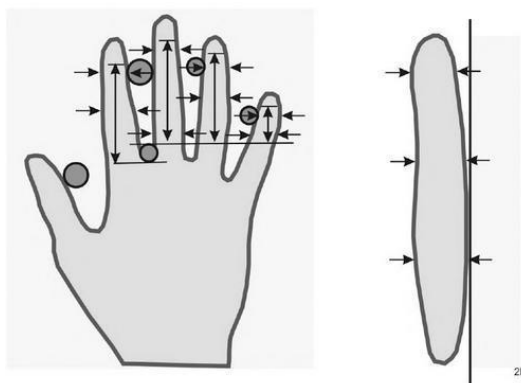
Ruka má hodně biometrických charakteristik, které se dají dnes využít k identifikaci osob: Otisk prstu, otisk dlaně, krevní řečiště hřbetu ruky, krevní řečiště prstu, krevní řečiště dlaně a geometrie ruky. Mezi méně využívané biometrické charakteristiky patří obraz nehtu, 2D a 3D obraz ruky a termální obraz ruky. Tato práce se bude zabývat nejrozšířenějšími charakteristikami a těmi jsou geometrie ruky, otisk prstu a dlaně a krevní řečiště prstu, hřbetu ruky a dlaně. [5]

#### 4.4.3.1. Geometrie ruky

Ruka člověka se od dospělosti nemění a její charakteristiky zůstávají v průběhu života téměř neměnné, nepočítáme-li různé choroby či úrazy. Biometrické systémy identifikace osob na základě geometrie ruky se řadí mezi nejstarší metody strojového rozpoznávání. [1]

Základním principem této metody je měření rozměrů ruky – délka prstů, šířka prstů a výška prstů a dlaně (obr. 6). Osoba identifikující svou totožnost pokládá ruku na desku se speciálními distančními kolíky, které určují správné umístění ruky. Tato deska má světlou barvu a vysokou odrazivost světla z důvodu většího kontrastu a pořízení kvalitního snímku ruky. Černobílý snímek je pořízen CCD kamerou buď přímou optickou cestou, tedy kamera se nachází nad deskou, či nepřímou cestou pomocí zrcadla, čímž se zkrátí vzdálenost potřebná pro umístění kamery, aby celé zařízení bylo kompaktnější. [1, 2]

*Obr. 6 Základní princip metody geometrie ruky. Kombinace jednotlivých geometrických hodnot měřených v desítkách bodů je jedinečná.*



*Zdroj: 1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.*

Existuje několik metod vyhodnocení snímku – metoda přímých měření, zarovnání rukou, analýza šířky prstů a 3D metoda. Nejvyužívanější je metoda přímých měření, která je založena na porovnání rozměrů, která jsou extrahována ze snímku a porovnána s referenční šablonou. [2]

Výhodou této metody je uživatelská akceptovatelnost a poměrně malá cena pořízení. Nevýhodou je proces identifikace, kde dochází k velkému počtu porovnávaných dat, proto se tato metoda spíše využívá při verifikaci osoby. [1]

Tato metoda našla využití v docházkových systémech pracovišť rozličného charakteru.

#### 4.4.3.2. Otisk prstu

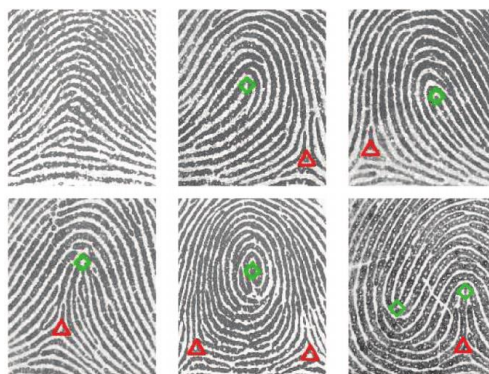
Identifikace osob na základě otisku prstu je dnes nejrozšířenější metodou vůbec. Dnešní společnost v tuto metodu vkládá důvěru zejména kvůli rozšířenému použití v kriminalistice, přestože podle statistik není nejbezpečnějším typem zabezpečení. [1, 2]

Tato metoda je založena na daktyloskopii zkoumající jedinečné uspořádání papilárních linií neboli vyvýšených reliéfů kůže prstu, které se formují v embryonálním stádiu vývoje člověka. Papilární linie jsou přibližně 0,1 – 0,4 mm vysoké a 0,2 – 0,5 mm široké a časově stálé. Pokud nedojde k poškození epidermální vrstvy kůže, papilární linie se obnovují společně s dorůstáním povrchu kůže. [2]

Markanty otisku prstu jsou znázorněny na obr. 7. Mezi relevantní markanty patří delta (červený trojúhelník) a jádro (zelený kruh). Delta je místo, kde dochází k rozdělení papilárních linií do tří různých směrů. Jádro je prostředkem tzv. smyčky, která je tvořena papilárními liniemi tvořící klenbu. [2]

Struktura papilárních linií se dále dělí na šest tříd (obr. 7) [4]:

Obr. 7 Třídy otisku prstu

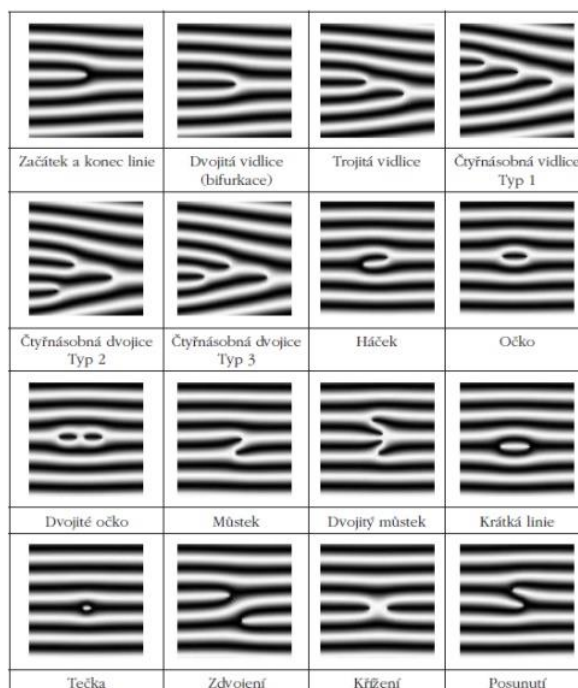


Zdroj 4. LODROVÁ, Dana. *Security of Biometric Systems*. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing, 2017. ISBN 978-3-330-34325-2.

- Oblouk – neobsahuje deltu ani jádro
- Levá smyčka – tvořena deltou umístěnou vpravo a jedním jádrem
- Pravá smyčka – tvořena deltou umístěnou vlevo a jedním jádrem
- Klenutý oblouk – tvořen jádrem a deltou umístěnou přibližně pod ním
- Spirála – tvořena jádrem a dvěma deltami z obou stran
- Dvojitá spirála – tvořena dvěma jádry a jednou deltou

Další markanty využívané v klasifikaci otisků prstu jsou zobrazeny na obr. 8. Papilární linie představuje bílá barva. [1]

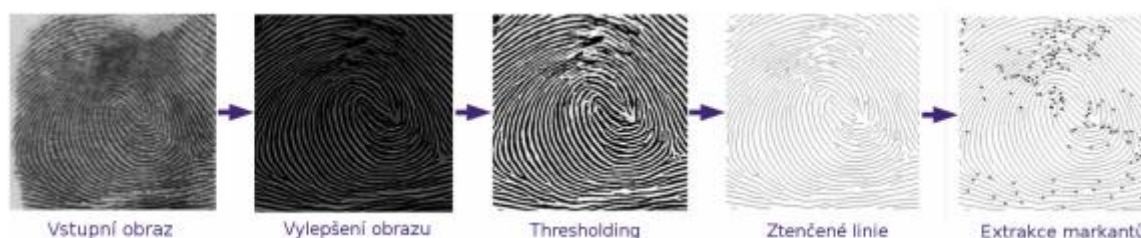
Obr. 8 Přehled základních markantů, pomocí kterých se modelují otisky prstů.



Zdroj: 1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

Samotné strojové zpracování otisku prstu (obr. 9) je založeno na vstupním obrazu, který může být naskenován z papírového média či načten pomocí digitálních čteček. Po načtení obrazu následuje vylepšení obrazu pomocí redukce šumu a oddělení otisku od pozadí. Dále dochází k segmentaci obrazu neboli prahování (thresholding), kdy se zvýrazní papilární linie, jež jsou upraveny a ztenčeny pro konečné zpracování a získání markantů. [4]

Obr. 9 Schéma zpracování otisku prstů



Zdroj: 7. DRAHANSKÝ, M., M. DOLEŽEL a J. URBÁNEK. *Influence of Skin Diseases on Fingerprint Quality and Recognition*. *New Trends and Developments in Biometrics*. BoD – Books on Demand, 2012, s. 275–303. ISBN 9789535108597.



Sensory pro snímání otisků prstu bývají různé a využívají odlišné technologie. Existují sensory optické, elektronické, kapacitní, ultrazvukové, tlakové či teplotní a liší se v závislosti na parametrech jako jsou – rozlišení, velikost, přesnost a plocha snímání. [1]

Optické sensory využívají zdroj LED světla pro osvětlení skleněné plochy, na kterou se přikládá prst. Paprsky odražené od povrchu prstu jsou zaznamenány CCD kamerou. Nevýhodou těchto sensorů je nežádoucí vliv nečistot na povrchu skla či prstu. [1, 2]

Elektronické sensory jsou založeny na změně elektrického pole mezi dvěma povrchy – vodivá vrstva kůže prstu a vodivá deska sensoru. Papilární linie deformují elektrické pole, které je pomocí snímacích antén převedeno do obrazu otisku prstu. Předností těchto sensorů je snímání vodivé vrstvy kůže, která se nachází pod potenciálně znečištěným či poškozeným povrchem prstu. [1]

Kapacitní sensory se řadí mezi nejčastěji používané sensory a jsou tvořeny polem vodivých ploch menších než 0,2 mm. Při doteku prstu dochází k propojení těchto ploch a vzniká přesný obraz papilárních linií. Nevýhodami těchto sensorů je snadné poškození povrchu a při doteku mokrého či suchého prstu je snímek nepřesný. [1, 4]

Ultrazvukové sensory fungují na principu odrazu ultrazvukových vln, které jsou vysílány vysílačem a zachyceny přijímačem. Tento proces trvá několik vteřin, proto je méně uživatelsky akceptovatelný, avšak výhodou je automatická detekce živosti uživatele. [5]

Dalším způsobem snímání je tlaková metoda založená na tlaku papilárních linií na piezoelektrický povrch sensoru, čímž se propojí dvě elektrovodivé vrstvy a vytvoří obraz otisku prstu. Takové sensory bezpečně fungují i při doteku mokrého, suchého či mastného prstu, avšak mají podstatně kratší životnost než jiné typy sensorů. [1, 5]

Teplotní metoda využívá tepelného záření. Pyroelektrický článek snímá teplo vyzařované papilárními liniemi, které vyzařují více světla než prohlubně, čímž se vytvoří snímek otisku prstu. Výhodou těchto sensorů je automatická detekce živosti uživatele právě za pomoci vyzařovaného tepla. [2, 5]

Využití této metody identifikace osob je velice rozšířené a na trhu je dnes k nalezení široká nabídka sensorů snímající otisk prstu ať už externí čtečky či implementované v mobilních zařízeních.

#### 4.4.3.3. Otisk dlaně

Metoda identifikace osob pomocí otisku dlaně je méně rozšířená oproti otisku prstu. Dochází při ní k pořízení většího snímku, což může mít své klady i zápory.

Mezi výhody patří velké množství porovnaných markantů, čímž je tato metoda potenciálně bezpečnější než metoda otisku prstu. Nevýhodou je nutnost větší plochy sensoru a delší doba zpracování výsledku identifikace. [3]

Pořízený snímek dlaně se podle rozlišení dělí na tři úrovně. První úroveň zaznamenává nejvýraznější markanty – linie dlaně a silueta. Druhá úroveň snímá menší papilární linie a markanty popsané na obr. 8. Třetí úroveň rozlišení zaznamenává šířku linií, póry a nejmenší detaily otisku dlaně. [3]

Nejvíce se tato metoda využívá u daktyloskopických karet ve forenzní sféře jako doplňující kontrolní otisk prstů a dlaně (obr. 10). [1]

Obr. 10 Dekadaktyloskopická karta využívaná v ČR



Zdroj: 1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

Na trhu prozatím neexistuje žádné zařízení zaměřené pouze na identifikaci osob pomocí otisku dlaně. [3]

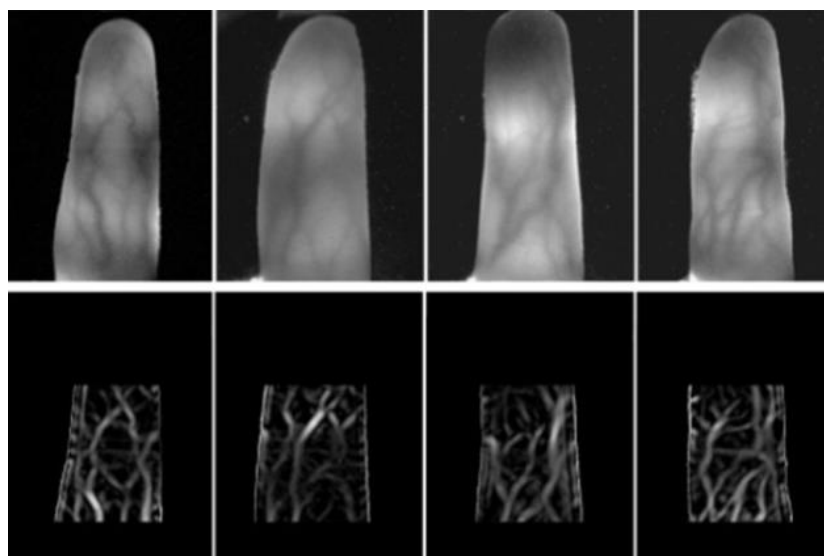
#### 4.5. Identifikace na základě skenu krevního řečiště

Krevní řečiště je u každé osoby jedinečné a nedá se jednoduše zfalšovat. Princip identifikace na základě skenu krevního řečiště spočívá v pořízení snímku pomocí krátkodobého osvětlení ruky IR neboli infračerveným zářením. Odkysličený hemoglobin pohlcuje světlo s vlnovou délkou 760 nm, čímž na snímku vyniknou žíly dlaně, prstů či hřbetu ruky. Aby byl snímek přesnější, používá se ve většině případů záření NIR (Near InfraRed) s vlnovou délkou 850 nm, které prochází kůží. Poté se ze snímku extrahují kontury dlaně, prstů a geometrické rozmístění krevního řečiště, z čehož vzniká binární mapa posléze uložená do databáze uživatelů. [5]

##### 4.5.1. Krevní řečiště prstu

Identifikace na základě skenu krevního řečiště prstu je založena na pořízení snímku prstu pomocí CCD kamery v infračervené oblasti, kdy se zvýrazní žíly prstu, jak je vidět na obr. 11. Po vytvoření se snímek dále zpracovává tak, aby následná extrakce žil byla co nejpřesnější a mohla se vytvořit binární mapa. [2]

*Obr. 11 Snímky otisků krevního řečiště prstu*



*Zdroj: 8 WINCOR NIXDORF a Dalibor PREMUS. Biometrie v bankovníctví [online]. In: 18. května 2015 [cit. 2020-02-25].*

Výhodou této metody oproti krevnímu řečišti dlaně či hřbetu ruky je poměrně malá velikost snímajícího zařízení, a proto je často využívána v kombinaci s otiskem prstu. [2]

Zařízení využívající tuto metodu poskytují na trhu firmy Hitachi (Vein ID) a Sony (Finger Vein Verification Technology). [2]

#### 4.5.2. Krevní řečiště hřbetu ruky

Pro pořízení snímku stromové sktruktury žil hřbetu ruky, která je též u každého jedince jedinečná, se může použít obraz světelné prostupnosti ruky pořízený pomocí světelného zdroje a CCD kamery, avšak spolehlivější metodou je snímek v infračervené oblasti. [6]

Pořízení IR snímku se provádí obdobně jako u skenu krevního řečiště prstu. Po pořízení snímku se odstraní pozadí a zredukuje šum obrazu. Poté se vyextrahují žíly a vytvoří se referenční šablona. [2]

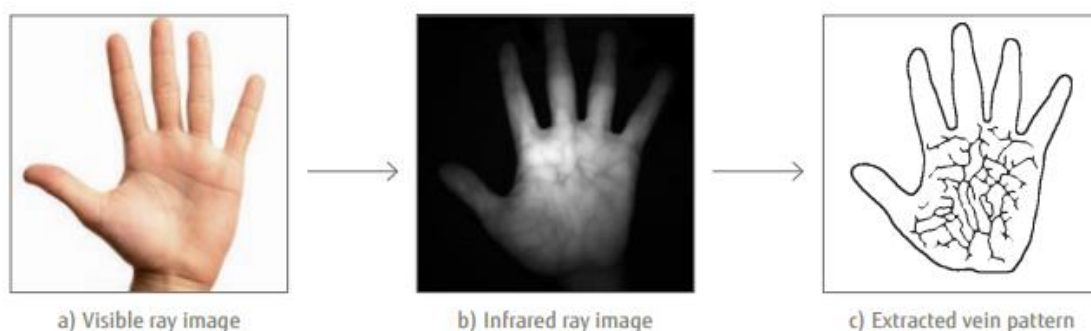
Zařízení snímající krevní řečiště hřbetu ruky nabízí firma Neuscience (Veincheck). [1]

#### 4.5.3. Krevní řečiště dlaně

Nejrozšířenější metodou identifikace na základě krevního řečiště je metoda skenu krevního řečiště dlaně ruky. Z pohledu uživatele je rychlejší a pohodlnější než výše zmíněné metody. [9]

Po pořízení snímku pomocí NIR světla dochází k extrahování referenční šablony (obr. 12) a jejímu uložení do databáze uživatelů. Při identifikaci či verifikaci se porovnává pořízený a zpracovaný snímek právě s touto referenční šablonou. [1, 2]

Obr. 12 Proces extrahování referenční šablony krevního řečiště



Zdroj: 10. FUJITSU LTD. Fujitsu PalmSecure: The solution for user-friendly and reliable authentication – more secure than the competition. [online]. [cit. 2020-02-04]

Biometrická metoda skenu krevního řečiště dlaně je dnes velice slibná a prosperující v bezpečnostně-komerční sféře kvůli řadě výhod:

- Jedná se o jednu z nejbezpečnějších biometrických metod z hlediska velice obtížného získání falzifikátu. Krevní řečiště se totiž nachází uvnitř těla.
- Tato metoda nevyžaduje fyzický kontakt, to znamená určitý komfort a hygienickou nezávadnost pro její uživatele.
- Při identifikaci nelze použít odcizenou šablonu.
- Při prověření identity se zároveň provádí i test živosti, jelikož řečištěm musí proudit krev.
- Krevní řečiště je jedinečné i u jednovaječných dvojčat.
- Krevní řečiště je časově stálé a zhruba od 14 let neměnné.
- U dětí se dá tato ověřovací metoda při častější aktualizaci šablony použít také.
- Oproti otisku prstu může být na dlani menší poranění či znečištění, které nijak neovlivní snímání. [11]

Nevýhodou této metody je výpočetní náročnost vyhledávání při identifikaci. Při použití této metody se také musí přizpůsobit teplotní režim snímače okolí a okolní hladina osvětlení. [9]

Mezi přední výrobce sensorů této biometrické metody patří Fujitsu Ltd., NCLEX® a Hitachi Ltd.

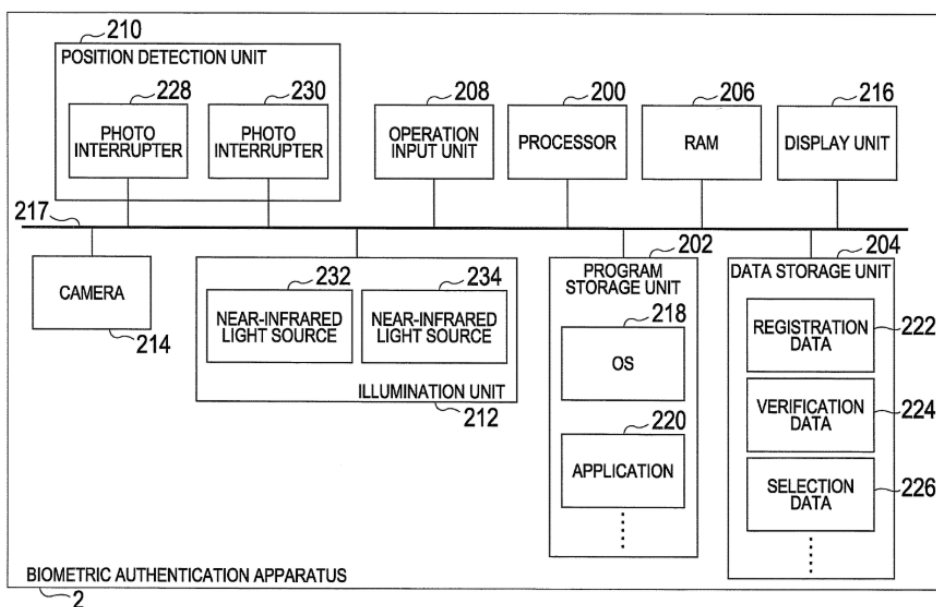
#### 4.5.4. PalmSecure

Nadnárodní společnost Fujitsu představila v roce 2008 patent na technologii PalmSecure poskytující uživatelům vše potřebné pro aplikaci systému identifikující osobu na základě skenu krevního řečiště dlaně (hardware i software). [12]

System se skládá ze speciálně navrženého autentizačního aparátu, který je popsán na obr. 13. Fujitsu PalmSecure senzor (obr. 15) je patentovaná součást s USB 2.0 rozhraním, kombinující funkce osvětlení, snímání, detekci pozice ruky a předzpracování obrazové informace krevního řečiště. Na schématu je senzor reprezentován kamerou (214), iluminační jednotkou (212) a jednotkou detekující pozici dlaně ruky (210). [12]

Další důležité části aparátu jsou databáze (204) pro ukládání referenčních šablon a jednotka (202 - procesor a paměť RAM mohou být obsaženy v této jednotce), na které je spuštěna aplikace (220) přístupná přes periferie a monitor (216). [12]

Obr. 13 Schéma systému technologie PalmSecure



Zdroj 12. HAMA, Soichi, Mitsuaki FUKUDA a Takahiro AOKI. FUJITSU LTD. Authentication apparatus: US20100085151A1. Zapsáno 22. 09. 2009. [online] [cit. 2020-02-05]

Průběh samotného procesu: Dlaň je umístěna přibližně 5-8 cm nad senzorem. Následně je provedena detekce živosti a dlaň je krátce prosvícena NIR zářením, které zvýrazní odkysličenou krev v žilách pohlcující NIR záření. Kamera pořídí snímek. V senzoru je tento snímek zašifrován pomocí standardizovaného algoritmu pro šifrování dat AES. Zašifrovaná data putují do serveru či PC a jsou konvertovány a zkomprimovány do biometrické šablony, která je následně ještě jednou pomocí AES zašifrována. Výsledkem je zašifrovaná biometrická šablona o velikosti 1-3 kB uložená v databázi či na jiném zařízení (SmartCard, mobilní zařízení). [9, 12]

Mezi výhody PalmSecure patří právě malá velikost biometrické šablony a nemožnost přenášet je do jiného systému kvůli šifrování. Dále není ukládán obraz, ale číselný výsledek matematické transformace. Zpětná transformace je velice obtížná, samotný obraz nelze zpětně získat. Tato technologie poskytuje velice přesné výsledky a ve srovnání s jinými biometrickými metodami vysokou míru zabezpečení, o které vypovídají hodnoty FAR a FRR (tab. 1). [9]

Tab. 1 FAR a FRR hodnoty různých biometrických metod

Autentizační metoda	FAR (%) =	If FRR (%) =
Rozpoznání tváře	~ 1.3	~ 2.6
Hlasové vzorky	~ 0.01	~ 0.3
Otisk prstu	~ 0.001	~ 0.1
Cévy v prstu	~ 0.0001	~ 0.01
Duhovka/Sítnice	~ 0.0001	~ 0.01
Krevní řečiště v dlani	<b>&lt; 0.00008</b>	~ 0.01

Zdroj: 9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace.

Technologie PalmSecure je z důvodu velké nabídky periferních přizpůsobení a individuálního řešení (obr. 14) dnes využívána ve zdravotnictví, bankovníctví i letištích. V Turecku je PalmSecure implementován ve více než 1700 privátních nemocnicích a napomáhá k identifikaci pacientů. Dále je tato technologie aplikovaná do bankomatů bank Bradesco Bank v Brazílii, Ziraat Bank v Turecku a BTMU – Bank of Tokyo-Mitsubishi UFJ v Japonsku. Také v německé bance Deutsche Bank byl spuštěn pilotní provoz těchto bankomatů. Poslední známá implementace PalmSecure proběhla na čtrnácti letištích v Koreji. [9, 13]

Obr. 14 Příklady použití sensoru



Zdroj: 14. FUJITSU Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite [online]. [cit. 2020-02-04]

## 5. Praktická část práce

Praktická část práce se věnuje testování skenování krevního řečiště dlaně ruky za ztížených podmínek, ke kterým by mohlo docházet při praktickém použití této biometrické metody ve sféře bezpečnostně-komerční. Při testování bylo použito technologie PalmSecure.

### 5.1. Podmínky měření

Měření se uskutečnilo v průběhu několika měsíců. S osobami, na kterých bylo testování provedeno (dále subjekty), bylo předem domluveno místo a čas měření. Z důvodu lehké manipulace se zařízením a pomůckami potřebnými k měření bylo možné, aby samotné měření probíhalo individuálně v závislosti na vyhovujících podmínkách zúčastněných.

Měření probíhalo za běžných atmosférických podmínek uvnitř budovy. Teplota a vlhkost okolního vzduchu se nevymykaly obvyklým hodnotám. Jako zdroj světla byly použity klasická žárovka se žlutým světlem a zářivka s bílým světlem.

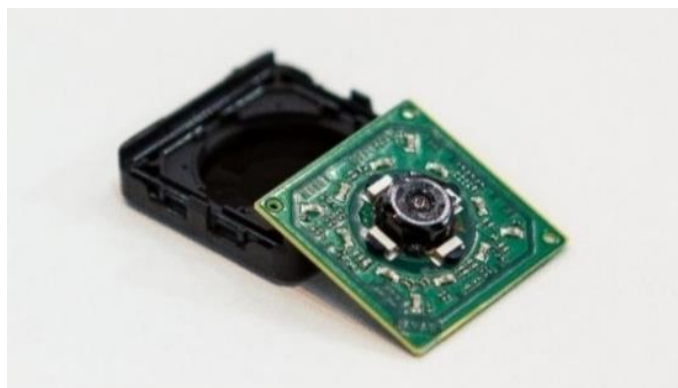
Testování byli podrobena rodina, přátelé a kolegové různého věku, pohlaví a tělesných proporcí. Celkem se testování zúčastnilo 20 subjektů.

### 5.2. Popis použitých nástrojů

Při měření byly použity dva různé sensory. První sensor V2 Sensor (obr. 15) snímající pomocí NIR světla využívá USB 2.0 rozhraní a AES šifrování. Při testování je důležité zamezit přímému slunečnímu světlu v dopadu na sensor. Při snímání musí být dlaň umístěna 4-6 cm nad senzorem. [9, 14]



Obr. 15 PalmSecure V2 Sensor



Zdroj: 9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace.

S tímto senzorem bylo použito speciální vodítko U-Guide určené pro vložení V2 senzoru (obr. 16). Vodítko je doporučováno pro pořizování kvalitních biometrických šablon i pro individuální autentizace subjektu, které lze použít jako stolní zařízení (má protiskluzové nožičky), nebo vestavět do desky stolu či zdi. Toto ergonomické vodítko intuitivně napomáhá subjektu umístit ruku do pozice pro optimální podmínky snímání. Je velice užitečné zejména při hojném provozu. [15]

Obr. 16 PalmSecure V2 U-Guide



Zdroj: 9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace.

Sensor na zařízení Lifebook U747 (obr. 17) nemá stejné technické parametry jako sensor V2 z důvodu zmenšení sensoru pro jednodušší implementace do notebooku, avšak přesnost měření by stále měla odpovídat hodnotám uvedeným v tab. 1. [16]

*Obr. 17 Detail Lifebook U747*

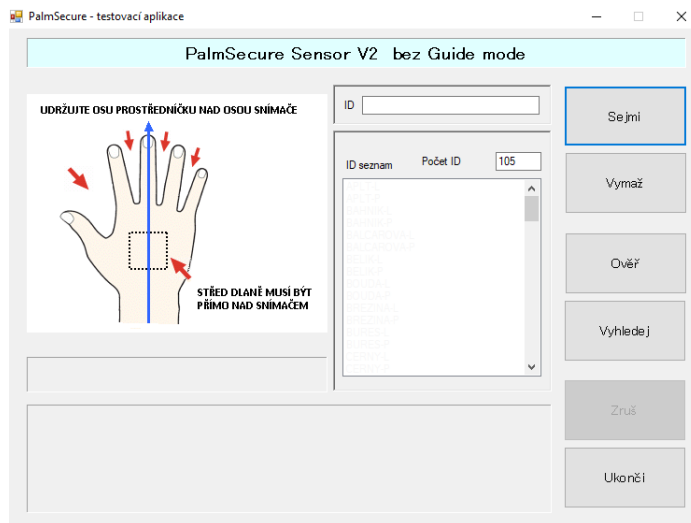


*Zdroj: 9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace*

Při testování sensoru V2 byla použita speciálně vyvinutá testovací aplikace [9], jejíž rozhraní je zobrazeno na obr. 18. Tato aplikace umožňuje rychlou práci se senzorem a záznamy subjektů. Záznamy mohou být načteny a vymazány.

Tlačítko „Ověř“ slouží pro verifikaci, je tedy potřeba označit příslušný záznam subjektu. Tlačítko „Vyhledej“ slouží k identifikaci subjektu. Tlačítkem „Zruš“ se zruší probíhající proces verifikace/identifikace. Tlačítkem „Ukonči“ se aplikace ukončí. Aplikace sama navádí subjekt ke správnému umístění dlaně, dá se tedy použít i bez U-Guide vodička. [9]

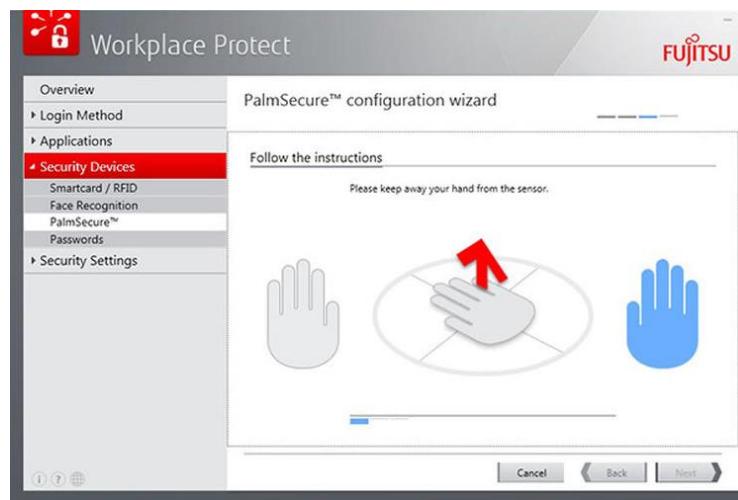
Obr. 18 Testovací aplikace PalmSecure Sensoru V2



Zdroj: 9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace.

Při měření se zařízením Lifebook U747 byla použita aplikace Workplace Protect, která umožňuje autentizaci do operačního systému Windows. Aplikace subjekt navádí do správné polohy dlaně pro co nejefektivnější záznam šablony (obr. 19). Tato aplikace také umožňuje využití více faktorové verifikace uživatele pomocí kombinací SmartCard, RFID karty, otisku prstu i rozpoznání obličeje. [17]

Obr. 19 Aplikace Workplace Protect



Zdroj: 17. FUJITSU, Ltd. Workplace Protect [počítačový program]. Ver. 3.1.L.3.7\_3.1.L.4.7 [online] [cit. 2020-02-07].

Pomůcky pro navození ztížených podmínek byly následující: gumová světlá rukavice, hydratační krém, rostlinný olej, lihový fix, voda a prostředky pro očištění dlaně ruky.

### 5.3. Postup měření a získávání dat

Testování sensoru V2 probíhalo jednotlivě pomocí testovací aplikace. Subjekty byly obeznámeny s podmínkami měření. Nejdříve byl 3x sejmout vzorek pro vytvoření referenční šablony krevního řečiště obou dlaní subjektu. Poté byl proveden kontrolní sken krevního řečiště za neztížených podmínek, tedy běžných provozních podmínek. Následující dílčí části měření probíhaly za ztížených podmínek (viz kapitola 5.4.) obou dlaní subjektu, a to za podmínky dvojnásobné verifikace a dvojnásobné identifikace každé dlaně. Výsledné hodnoty byly tři: přístup povolen (úspěšné ověření), žádost o opakování skenu a v případě třetího neúspěšného skenu (2x žádost o opakování) došlo k zamítnutí přístupu. Výsledky každého skenu byly vyhodnoceny a zapsány do tabulky. U jednoho subjektu bylo naměřeno z pohledu úspěšné i neúspěšné verifikace a identifikace 64 výsledků.

U sensoru integrovaného v zařízení Lifebook U747 se pomocí aplikace Workplace Protect nahrála referenční šablona obou dlaní subjektu. Každá šablona vyžadovala 3 skeny krevního řečiště dlaně. Po uložení šablony a odhlášení z operačního systému, které bylo nutné provést po každém měření, byla nejdříve provedena verifikace subjektu pro seznámení se se správnou polohou dlaně ruky. Poté se každý výsledek měření zaznamenal do tabulky výsledků. Prvním zaznamenaným měřením byla verifikace za pomoci obou dlaní za běžných (neztížených) podmínek. Následující dílčí části měření probíhaly za ztížených podmínek (viz kapitola 5.4.) obou dlaní subjektu. Výsledek skenu byl hodnocen buď povolením přístupu či zamítnutím přístupu. Na konci měření byly z aplikace Workplace Protect odstraněny všechny záznamy subjektu. Takovým způsobem bylo otestováno 5 subjektů. U jednoho subjektu bylo naměřeno 32 výsledků.

### 5.4. Popis ztížených podmínek

- První sken probíhal bez ztížených podmínek pro vyzkoušení správného načtení šablony obou dlaní.
- Druhý sken krevního řečiště dlaně byl proveden v hygienických rukavicích světlé matné barvy.
- Třetí sken proběhl po nanesení hydratačního krému na ruce.
- Čtvrtý sken byl zatížen nanesením kapek rostlinného oleje nepravidelného vzoru a částečně rozetřen na dlaní.

- Při pátém skenu bylo využito mokré dlaně (po omytí oleje).
- Při šestém skenu byly dlaně ohřáty pomocí horké vody.
- Při sedmém skenu byly dlaně naopak ochlazený ledovou vodou.
- Poslední osmý sken byl proveden po nakreslení mřížky lihovým fixem na povrch dlaně.

### 5.5. Popis zpracování získaných dat

Získané výsledky z testování sensorů byly zapsány do tabulky. Vyhodnocení celkové úspěšnosti verifikace obou sensorů bylo provedeno za pomoci softwaru Statistica [25]. Byla použita statistická metoda Anova neboli analýza rozptylu ověřující, zdali hodnota proměnné má statisticky významný vliv na pozorování. Tato metoda zkoumá proměnné různých faktorů, přičemž tyto faktory (ztížené podmínky) třídí proměnné do skupin. Počet těchto proměnných je závislý na počtu měření a nabývá hodnot 0 či 1 (úspěšná verifikace, neúspěšná verifikace). [26]

Pro vyhodnocení dat byl použit Fisherův LSD test diferencí, který vyhodnocuje statisticky významné difference při hladině významnosti  $\alpha = 0,05$ , tedy zda dochází k zamítnutí nulové hypotézy. [27]

Směrodatná odchylka byla zpracována u výsledků verifikace obou sensorů a značí rozptyl hodnot od průměru. Směrodatná odchylka ( $\sigma$ ) se vypočítá za pomoci rozptylu (průměr druhých mocnin vzdáleností od průměru). [28]

$$\sigma = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}} = \sqrt{\frac{\text{součet druhých mocnin vzdáleností od průměru}}{\text{počet prvků statistického souboru}}} \quad (5.1)$$

## 6. Zhodnocení výsledků

Výsledky měření spolehlivosti systémů identifikující osoby na základě skenu krevního řečiště prokázaly, že tyto systémy jsou vcelku spolehlivé i při uměle vyvolaných ztížených podmínkách oproti jiným systémům identifikace (např. otisk prstu).

### 6.1. Sensor Lifebook U747

Výsledky měření subjektu při použití sensoru zařízení Lifebook U747 prokázaly větší počet neúspěšné verifikace. Průměrná chybovost z celkového počtu měření nabyla přibližné hodnoty 24,4 %. Celkový počet provedených dílčích měření je 160.

Hodnoty v tab. 2 reprezentují výsledky měření verifikace subjektu.

Při podmínce bez jakéhokoli zatížení (Normální) byla hodnota FRR 5 %, která mohla být způsobena nesprávným umístěním dlaně nad senzorem. Nanesení krému na dlaň ovlivnilo úspěšnost verifikace přibližně o 20 %. Znečištění dlaně mastnotou či lihovým fixem mělo podobné výsledky neúspěšných pokusů verifikace, tedy přibližně jedna třetina všech měření byla neúspěšná. Nejvíce bylo měření ovlivněno při použití hygienické rukavice, kdy docházelo z 85 % k negativnímu ovlivnění výsledku verifikace subjektu.

Odpovídající míra FRR (uvedená v tab. 1) při testování tohoto sensoru byla splněna pouze u jedné podmínky. Vysoká míra FRR mohla být způsobena nekorektním umístěním dlaně ruky nad senzorem.

Statisticky významné hodnoty jsou v tab. 2 vyznačeny červeně.

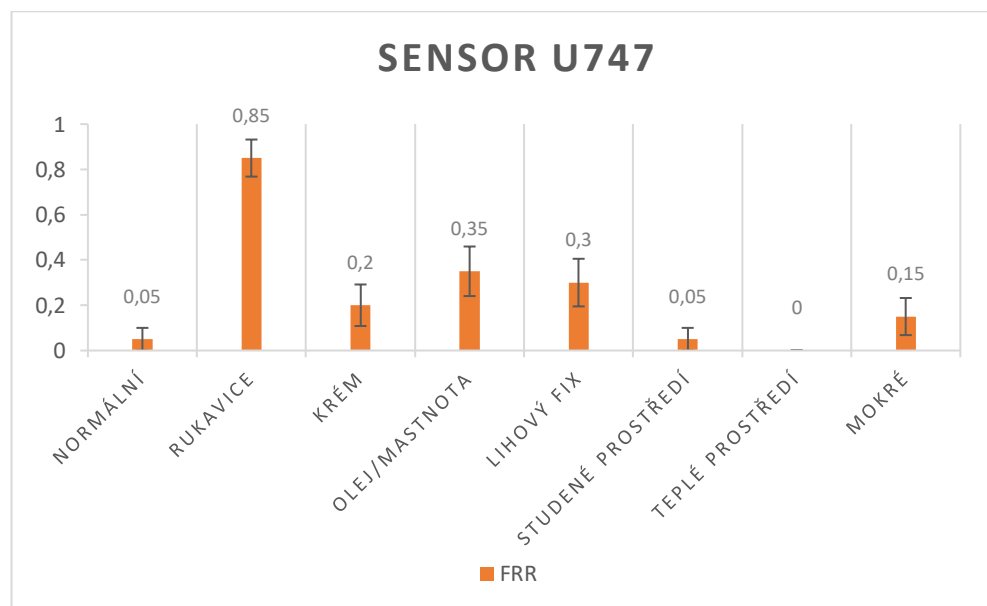
Tab. 2 Výsledky U747 – Verifikace

	Neúspěšné	Neúspěšnost	FRR	Shodnost FRR (0,01 %)	LSD test diferencí	Směrodatná odchylka
1. Normální	1/20	0,05	5 %	ne	-	0,050000
2. Rukavice	17/20	0,85	85 %	ne	0,000000	0,081918
3. Krém	4/20	0,2	20 %	ne	0,181142	0,091766
4. Olej/mastnota	7/20	0,35	35 %	ne	0,008017	0,109424
5. Lihový fix	6/20	0,3	30 %	ne	0,026607	0,105131
6. Studené prostředí	1/20	0,5	5 %	ne	1,000000	0,050000
7. Teplé prostředí	0/20	0	0 %	ano	0,654933	0,000000
8. Mokrý	3/20	0,15	15 %	ne	0,371879	0,081918

Zdroj: Výsledky měření

Na obr. 20 (Graf sensoru U747) jsou zobrazeny hodnoty FRR a také směrodatné odchylky měření při daných ztížených podmínkách. Největší rozptyl byl naměřen při použití lihového fixu či znečištění dlaně olejem.

Obr. 20 Graf sensoru U747 – FRR, směrodatná odchylka



Zdroj: Výsledky měření

Při větším počtu jednotlivých měření by hodnoty chybovosti nejspíše klesaly pomalým tempem.

## 6.2. Sensor V2 s vodítkem U-Guide

Výsledky měření verifikace subjektu za pomoci sensoru V2 prokázaly, že tento sensor je více spolehlivý než sensor implementovaný v zařízení Lifebook U747 z důvodu použití pomocného vodítka U-Guide pro správné umístění dlaně nad sensor. Průměrná chybovost všech měření nabyla přibližné hodnoty 8,6 %.

Tento sensor byl testován při procesu verifikace i identifikace, avšak z důvodu porovnání sensorů jsou uváděny pouze výsledky verifikačního procesu. Výsledné hodnoty identifikačního procesu jsou k nalezení v příloze č. 1 - Výsledky měření. Celkový počet provedených dílčích měření verifikace subjektu je 640.

Hodnoty v tab. 3 reprezentují výsledky měření verifikace subjektu za pomoci sensoru V2.

Podmínky studeného a teplého prostředí, tedy ochlazená či ohřátá dlaň, nijak neovlivnily průběh verifikace. Nulová chybovost byla též prokázána při nanesení oleje či vody na dlaň, hodnoty tedy byly stejné, jako za neztížených podmínek.

Nanesení krému na dlaň ruky ovlivnilo proces verifikace v malé míře (FRR 2,5 %).

Neúspěšné pokusy verifikace při použití hygienické rukavice a lihového fixu nabyly vyšších hodnot. Ve srovnání se senzorem zařízení U747 jsou tyto hodnoty menší, což mohlo být způsobeno větším počtem dílčích měření.

Odpovídající míra FRR (uvedená v tab. 1) při testování sensoru V2 byla splněna u pěti podmínek (z toho 4 ztížené podmínky).

Statisticky významné hodnoty jsou v tab. 3 vyznačeny červeně.



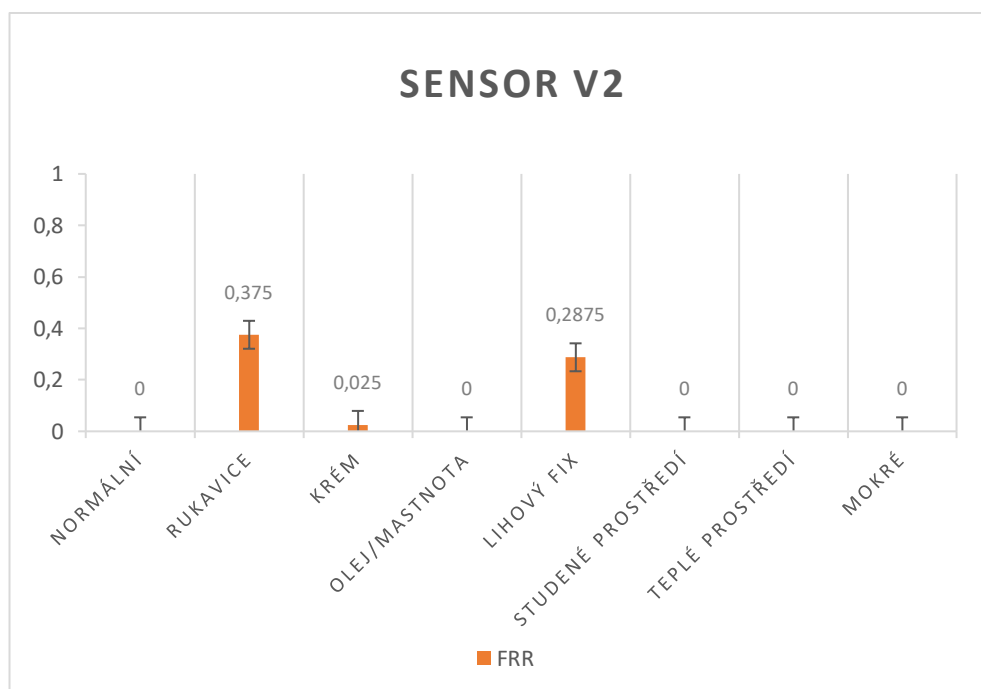
Tab. 3 Výsledky sensor V2 – Verifikace

	Neúspěšné	Neúspěšnost	FRR	Shodnost FRR (0,01 %)	LSD test diferencí	Směrodatná odchylka
1. Normální	0/80	0	0,00 %	ano	-	0,000000
2. Rukavice	30/80	0,375	37,50 %	ne	0,000000	0,054468
3. Krém	2/80	0,025	2,50 %	ne	0,514186	0,017565
4. Olej/mastnota	0/80	0	0,00 %	ano	1,000000	0,000000
5. Lihový fix	23/80	0,2875	28,75 %	ne	0,000000	0,050921
6. Studené prostředí	0/80	0	0,00 %	ano	1,000000	0,000000
7. Teplé prostředí	0/80	0	0,00 %	ano	1,000000	0,000000
8. Mokrý	0/80	0	0,00 %	ano	1,000000	0,000000

Zdroj: Výsledky měření

Na obrázku 21 (Graf sensoru V2) jsou graficky zobrazeny hodnoty FRR a také směrodatné odchylky měření při daných ztížených podmínkách. Největší rozptyl byl naměřen při použití lihového fixu a hygienické rukavice.

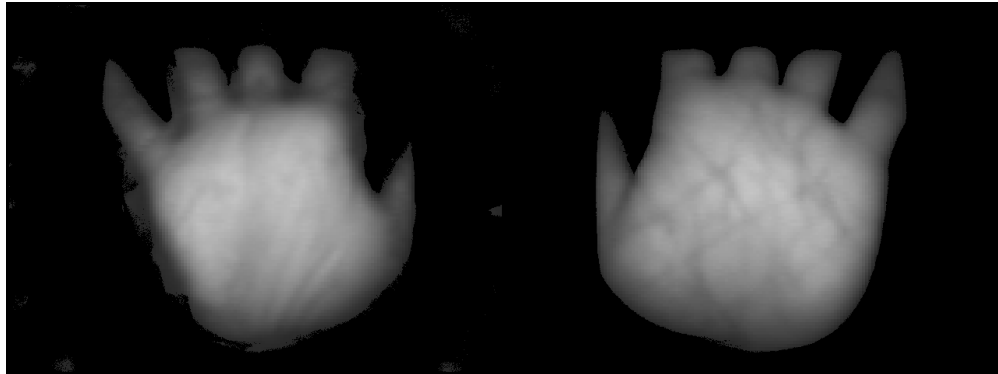
Obr. 21 Graf sensoru V2 – FRR, směrodatná odchylka



Zdroj: Výsledky měření

Při měření bylo vyzorováno, že menší dlaně (zejména u ženského pohlaví) prokazovaly větší míru chybovosti verifikace a identifikace při použití lihového fixu a hygienické rukavice. Důvodem mohla být menší testovaná plocha (obr. 22).

*Obr. 22 Vlevo snímek dlaně v rukavici, vpravo ruka popsaná lihovým fixem*



*Výsledky testovací aplikace*

Výše okomentované výsledky měření poukazují na vysokou míru spolehlivosti systému identifikace na základě skenu krevního řečiště, avšak při některých podmínkách je spolehlivost omezená.

## 7. Závěr

V teoretické části práce byly definovány základní pojmy v oblasti biometrie jako je identita, identifikace a verifikace, a také výpočty základních bezpečnostních charakteristik biometrických systémů – pravděpodobnost chybného odmítnutí a pravděpodobnost chybného přijetí. Dále byla praktická část věnována základnímu rozdělení biometrických metod a stručnému popisu nejvyužívanějších metod identifikace na základě behaviorálních charakteristik – rozpoznání na základě hlasu, podpisu a chůze – a anatomicko-fyziologických charakteristik – tváře, oka a ruky. Biometrické metody různých charakteristik ruky byly popsány detailněji, konkrétně se jednalo o metodu geometrii ruky, otisk prstu, tisk dlaně a krevní řečiště prstu, hřbetu ruky a dlaně. Poslední kapitola teoretické části se věnovala popisu technologie PalmSecure.

Identifikace osob na základě krevního řečiště má řadu výhod. Při identifikaci dochází k automatickému testu živosti uživatele z důvodu nutnosti proudění krve krevním řečištěm, které je časově stálé. Identifikace je provedena bez fyzického kontaktu, uživatel se tedy nemusí přímo dotýkat sensoru. Tato metoda toleruje menší znečištění a poškození ruky. Dalším podstatným přínosem je velice obtížná falzifikace. Přestože má tato metoda vysokou úroveň bezpečnosti, není příliš rozšířená, jelikož je poměrně novou metodou v oblasti biometrických systémů.

V praktické části práce byly popsány a vyhodnoceny výsledky měření spolehlivosti systémů identifikace osob na základě krevního řečiště dlaně za ztížených podmínek. Toto měření bylo provedeno za pomoci technologie PalmSecure od firmy Fujitsu, Ltd., která nabízí lehce aplikovatelný systém, tedy hardware i software. Při měření byly testovány dva typy sensorů – první integrovaný do notebooku Lifebook U747 a druhý externí sensor V2 s USB rozhraním a speciálním vodítkem V2 U-Guide. Cílem tohoto měření bylo zjistit, zda je tato metoda spolehlivá i za nepříznivých vlivů při identifikaci a verifikaci uživatele.

U integrovaného sensoru se provádělo měření za pomoci aplikace Workplace Protect, která umožňuje pouze verifikaci uživatele. S tímto typem sensoru byly testovány obě dlaně pěti subjektů, přičemž každá dlaň byla testována dvakrát za daných podmínek. Druhý typ sensoru s vodítkem byl aplikován pomocí speciálně vyvinuté testovací aplikace umožňující proces verifikace i identifikace. S tímto senzorem byly testovány obě dlaně dvaceti subjektů, přičemž každá dlaň byla podrobena dvakrát identifikaci a dvakrát verifikaci za daných podmínek.

Prvním krokem měření bylo prvotní načtení a uložení referenční šablony, na jejímž základě docházelo k porovnání za ztížených podmínek, které byly uměle vyvolány v následujícím pořadí:

1. Kontrolní měření bez jakéhokoli zatížení
2. Měření v hygienické rukavici
3. Měření při nanesení hydratačního krému
4. Měření při nanesení rostlinného oleje
5. Měření mokré dlaně
6. Měření zahřáté dlaně
7. Měření ochlazené dlaně
8. Měření dlaně pokreslené lihovým fixem

Výsledky měření byly zpracovány za pomoci programu Statistica metodou Anova, konkrétně Fisherovým LSD testem diferencí a byla vypočítána směrodatná odchylka výsledků měření za jednotlivých ztížených podmínek.

Celkem bylo provedeno dílčích 1440 měření a bylo prokázáno, že spolehlivost snímání krevního řečiště ruky při odlišných teplotách se nemění. Výsledky měření při použití oleje a hydratačního krému vykazovaly ojedinělé chyby. Znečištění dlaně lihovým fixem a použití hygienické rukavice negativně ovlivňují výsledky identifikace, avšak při větších rozměrech dlaně ruky je možné provést identifikaci subjektu.

Při měření probíhajícím pomocí integrovaného sensoru byly výsledky přibližně totožné, avšak byla prokázána větší míra FRR neboli pravděpodobnost chybného odmítnutí. Důvodem mohla být nepřesná poloha umístění dlaně nad senzorem.

Celkově může být tento biometrický systém hodnocen jako spolehlivý i při ztížených podmínkách. Doporučením do budoucna je lepší přizpůsobení podmínek měření z hlediska zajištění vždy stejné polohy dlaně nad senzorem u integrovaného sensoru. Také je možné testovat za ztížených podmínek jiného charakteru.

## 8. Seznam použitých zdrojů

1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.
2. DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 9788025489796.
3. ГАФНЕР, Василий Викторович, СПИВАК, А. М., ed. *Информационная безопасность*. Ростов-на-Дону: Феникс, 2010г., 324 с. ISBN 978-5-222-17389-3.
4. LODROVÁ, Dana. *Security of Biometric Systems*. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing, 2017. ISBN 978-3-330-34325-2.
5. *Hand-based biometrics: methods and technology*. Editor Martin DRAHANSKÝ. London: The Institution of Engineering and Technology, 2018. IET book series in advanced biometrics. ISBN 978-1-78561-224-4.
6. ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. Ostrava, [Online] 2008. [cit. 2020-02-03] Dostupné také z: [https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke\\_metody.pdf](https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf).
7. DRAHANSKÝ, M., M. DOLEŽEL a J. URBÁNEK. Influence of Skin Diseases on Fingerprint Quality and Recognition. *New Trends and Developments in Biometrics*. BoD – Books on Demand, 2012, s. 275–303. ISBN 9789535108597.
8. WINCOR NIXDORF a Dalibor PREMUS. *Biometrie v bankovníctví* [online]. In: 18. května 2015 [cit. 2020-02-25]. Dostupné z: <https://slideplayer.cz/slide/4874671/>

9. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. *PalmSecure a Palm Vein Sensory* [online]. leden 2020; [cit. 2020-02-05]. Osobní komunikace.
10. FUJITSU LTD. *Fujitsu PalmSecure: The solution for user-friendly and reliable authentication – more secure than the competition.* [online]. [cit. 2020-02-04] Dostupné také z: [https://www.fujitsu.com/id/Images/PalmSecure%20Global%20Solution%20Catalogue\\_tcm114-1594497.pdf](https://www.fujitsu.com/id/Images/PalmSecure%20Global%20Solution%20Catalogue_tcm114-1594497.pdf)
11. *Compare Fingerprint Recognition and Palm Vein Technology* [online]. [cit. 2020-02-04]. Dostupné z: <https://www.bayometric.com/compare-fingerprint-recognition-and-palm-vein-technology/>
12. HAMA, Soichi, Mitsuaki FUKUDA a Takahiro AOKI. FUJITSU LTD. *Authentication apparatus: US20100085151A1.* Zapsáno 22. 09. 2009. [online] [cit. 2020-02-05]. Dostupné také z: <https://patents.google.com/patent/US20100085151A1/>
13. *Fujitsu's PalmSecure Deployed in World's First Palm Vein Authentication System at Korean Airports* [online]. [cit. 2020-02-04]. Dostupné z: <https://www.fujitsu.com/global/about/resources/news/pressreleases/2019/0327-01.html>
14. *FUJITSU Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite* [online]. [cit. 2020-02-04]. Dostupné z: [https://www.fujitsu.com/us/Images/Fujitsu\\_DS-F-Pro\\_103017.pdf](https://www.fujitsu.com/us/Images/Fujitsu_DS-F-Pro_103017.pdf)
15. *Datasheet Příslušenství FUJITSU PalmSecure U Guide: Zabezpečení přístupu* [online]. [cit. 2020-02-07]. Dostupné z: <https://sp.ts.fujitsu.com/dmsp/Publications/public/ds-PalmSecure-U-Guide-cz.pdf>
16. *Fact Sheet FUJITSU PalmSecure for mobile devices* [online]. [cit. 2020-02-07]. Dostupné z: [https://www.shopfujitsu.com/pdf/notebooks/Fujitsu-Palm-Secure-mobile-devices\\_factsheet.pdf](https://www.shopfujitsu.com/pdf/notebooks/Fujitsu-Palm-Secure-mobile-devices_factsheet.pdf)

17. FUJITSU, Ltd. *Workplace Protect* [počítačový program]. Ver. 3.1.L.3.7\_3.1.L.4.7 [online] [cit. 2020-02-07]. Dostupné z: <https://support.ts.fujitsu.com/IndexDownload.asp?lng=COM&ln=no&LC=yes>
18. *Age factors in biometric processing*. Editor Michael FAIRHURST. London, UK: The institution of engineering and technology, 2014. ISBN 978-1-84919-502-7.
19. *PalmSecure™, Palm Vein Authentication System* [online]. [cit. 2020-02-04]. Dostupné z: [https://www.fujitsu.com/downloads/COMP/fcpa/biometrics/palmsecure\\_datasheet.pdf](https://www.fujitsu.com/downloads/COMP/fcpa/biometrics/palmsecure_datasheet.pdf)
20. *Fujitsu steps up biometric offerings with PalmSecure* [online]. [cit. 2020-02-04]. Dostupné z: <https://www.techcentral.ie/fujitsu-steps-up-biometric-offerings-with-palmsecure/>
21. *Datasheet Fujitsu PalmSecure Contactless Biometrics Authentication* [online]. [cit. 2020-02-04]. Dostupné z: [https://www.fujitsu.com/global/Images/PalmSecure\\_Datasheet.pdf](https://www.fujitsu.com/global/Images/PalmSecure_Datasheet.pdf)
22. *PalmSecure A new level of Biometric Technology Solutions* [online]. [cit. 2020-02-04]. Dostupné z: [https://www.fujitsu.com/pt/Images/Palm\\_Secure\\_tcm72-630557.pdf](https://www.fujitsu.com/pt/Images/Palm_Secure_tcm72-630557.pdf)
23. *Data Sheet FUJITSU Notebook LIFEBOOK U747* [online]. [cit. 2020-02-08]. Dostupné z: <https://sp.ts.fujitsu.com/dmsp/Publications/public/ds-LIFEBOOK-U747.pdf>
24. BOURGET, Denis a Denis Jean-Claude SIEW. *Biometric authentication system and method: WO2012083456A1*. Zapsáno 21.12.2011. [online] [cit. 2020-02-05]. Dostupné z: <https://patents.google.com/patent/WO2012083456A1/>



25. STATSOFT. *STATISTICA 13.3: Input data and analyze it with a built-in visualization module* [online]. [cit. 2020-03-22]. Dostupné z: <https://statistica.software.informer.com/>
26. NEUBAUER, Jiří. *Analýza rozptylu: Statistika II* [online]. Katedra ekonometrie FVL UO Brno [cit. 2020-03-22]. Dostupné z: <https://k101.unob.cz/~neubauer/pdf/anova.pdf>
27. DUBJAKOVÁ, Eva. *Metody mnohonásobného porovnávání pro jednoduché třídění*. Brno, 2009. Diplomová práce. Masarykova univerzita. Vedoucí práce RNDr. Marie Budíková, Dr. Dostupné také z: [https://is.muni.cz/th/151390/prif\\_m/diplomova\\_prace\\_ed.pdf](https://is.muni.cz/th/151390/prif_m/diplomova_prace_ed.pdf).
28. VACHTOVÁ, Jitka. *Statistika: Směrodatná odchylka  $\sigma$*  [online]. [cit. 2020-03-22]. Dostupné z: <https://www.ekovyp.cz/smerodatna-odchylka/>

## 8.1. Seznam obrázků

Obr. 1 Identifikace a verifikace.....	6
Obr. 2 Biometrický systém .....	7
Obr. 3 Reálná biometrická aplikace .....	9
Obr. 4 Dynamické vlastnosti podpisu .....	10
Obr. 5 Popis struktury duhovky .....	13
Obr. 6 Základní princip metody geometrie ruky. Kombinace jednotlivých geometrických hodnot měřených v desítkách bodů je jedinečná. ....	14
Obr. 7 Třídy otisku prstu .....	15
Obr. 8 Přehled základních markantů, pomocí kterých se modelují otisky prstů. ....	16
Obr. 9 Schéma zpracování otisku prstů .....	16
Obr. 10 Dekadaktyloskopická karta využívaná v ČR .....	18
Obr. 11 Snímky otisků krevního řečiště prstu .....	19
Obr. 12 Proces extrahování referenční šablony krevního řečiště .....	20
Obr. 13 Schéma systému technologie PalmSecure .....	22
Obr. 14 Příklady použití sensoru.....	23
Obr. 15 PalmSecure V2 Sensor .....	25
Obr. 16 PalmSecure V2 U-Guide.....	25
Obr. 17 Detail Lifebook U747 .....	26
Obr. 18 Testovací aplikace PalmSecure Sensoru V2.....	27

Obr. 19 Aplikace Workplace Protect.....	27
Obr. 20 Graf sensoru U747 – FRR, směrodatná odchylka .....	31
Obr. 21 Graf sensoru V2 – FRR, směrodatná odchylka.....	33
Obr. 22 Vlevo snímek dlaně v rukavici, vpravo ruka popsaná lihovým fixem.....	34

## 8.2. Seznam tabulek

Tab. 1 FAR a FRR hodnoty různých biometrických metod.....	23
Tab. 2 Výsledky U747 – Verifikace.....	31
Tab. 3 Výsledky sensor V2 – Verifikace.....	33

## 8.3. Seznam vzorců

Výpočet FRR (4.1).....	8
Výpočet FAR (4.2) .....	8
Výpočet směrodatné odchylky (5.1).....	29

## 8.4. Seznam použitých zkratk

PIN	Personal Identification Number
ID	Identity Document
FRR	False Rejection Rate
FRA	False Acceptance Rate
PDA	Personal Digital Assistant
CCD	Charge-Coupled Device

LED	Light-Emitting Diode
IR	Infrared Radiation (Infrared light)
NIR	Near-Infrared Radiation
USB	Universal Serial Bus
RAM	Random-Access Memory
AES	Advanced Encryption Standard
PC	Personal Computer
kB	kiloByte
LSD	Least Significant Difference

## 9. Seznam příloh

Příloha č. 1 – Výsledky měření

## **Příloha č. 1 – Výsledky měření**

### Výsledky měření – Sensor U747

Měření č. 1	Verifikace	
	Levá	Pravá
Podmínky		
1. Normální	VV	VV
2. Rukavice	XX	XX
3. Krém	VV	VV
4. Olej/masnota	XX	XV
5. Lihový fix	XX	VV
6. Studené prostředí	VV	VV
7. Teplé prostředí	VV	VV
8. Mokrý	VV	VX

Měření č. 2	Verifikace	
	Levá	Pravá
Podmínky		
1. Normální	VV	VV
2. Rukavice	XX	XX
3. Krém	VV	XX
4. Olej/masnota	VV	XX
5. Lihový fix	XV	XX
6. Studené prostředí	VV	VV
7. Teplé prostředí	VV	VV
8. Mokrý	VV	VV

Měření č. 3	Verifikace	
	Levá	Pravá
Podmínky		
1. Normální	VV	VV
2. Rukavice	XX	XX
3. Krém	VV	VV
4. Olej/masnota	VV	VV
5. Lihový fix	VV	VV
6. Studené prostředí	VV	VV
7. Teplé prostředí	VV	VV
8. Mokrý	VV	VV

Měření č. 4	Verifikace	
	Levá	Pravá
Podmínky		
1. Normální	VV	VV
2. Rukavice	VX	VV
3. Krém	VV	VV
4. Olej/masnota	XV	VV
5. Lihový fix	VV	VV
6. Studené prostředí	VV	VV
7. Teplé prostředí	VV	VV
8. Mokrý	VV	VV

Měření č. 5	Verifikace	
	Levá	Pravá
Podmínky		
1. Normální	VV	XV
2. Rukavice	XX	XX
3. Krém	VV	XX
4. Olej/masnota	VV	XV
5. Lihový fix	VV	VX
6. Studené prostředí	VV	VX
7. Teplé prostředí	VV	VV
8. Mokrý	VX	XV

Vysvětlivky	
X	Přístup zamítnut
V	Přístup povolen

### Výsledky měření – Sensor V2

Měření č. 1	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIXIIX	IIXIIX	IIXIIX	IIXIIX
3. Krém	IVIV	VV	VIV	IVV
4. Olej/masnota	VV	IIVV	VV	VV
5. Lihový fix	IIXIV	VIIIV	IIXIV	IVIIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Vysvětlivky	
X	Přístup zamítnut
I	Opětovné snímání
V	Přístup povolen

Měření č. 2	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VIV	VV
5. Lihový fix	VV	VV	VV	VV
6. Studené prostředí	VV	VV	VIV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 3	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IVV	IVIIX	IVIIX	IIXV
3. Krém	VV	IVV	VV	IVIIX
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	IVV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 4	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIXV	IIXIIX	IVV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VIV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 5	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	IIXV	VV	IIXV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 6	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	IIXIX	IIXIX	IIXIX	IIXIX
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	IVV	VV	IVIV
5. Lihový fix	IIXIX	IIXIX	IIXIX	IIXIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VIV	VV	VV

Měření č. 7	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	IVV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VIV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 8	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	VV	VIV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV



Měření č. 9	Identifikace		Verifikace	
Podmínky	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	IIIX	IVIX	IIIX	IIIX
3. Krém	VV	IIIX	VV	VIIX
4. Olej/masnota	VV	VIV	VV	IVIV
5. Lihový fix	IVIX	IIIX	IIIX	IIIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 10	Identifikace		Verifikace	
Podmínky	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VIV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	IVV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 11	Identifikace		Verifikace	
Podmínky	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	IIIX	IIIX	IIIX	IIIX
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	IIIX	IIIX	IVIX	IIIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VIV	VV	IVV	VV

Měření č. 12	Identifikace		Verifikace	
Podmínky	Levá	Pravá	Levá	Pravá
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VIV	VV	VIV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	IVV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 13	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIIXIX	IIIXIV	IIIXIX	IVIXIX
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VIV
5. Lihový fix	IVIXIX	IIIXIX	IIIXIX	IIIXIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 14	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	IVV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 15	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIIXIX	IIIXIX	IIIXIX	IIIXIX
3. Krém	VV	IIIXIV	VV	IVV
4. Olej/masnota	IVV	VV	VIV	VV
5. Lihový fix	IIIXIX	IIIXIX	IIIXIX	IIIXIX
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 16	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	IVV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VIV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 17	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIXIIX	IIXIIX	IIXIV	IVV
3. Krém	IVV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	IVV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 18	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	IVV	VV	VV	VV
2. Rukavice	IIXIIX	IVIIX	IIXIV	IIXIV
3. Krém	IIXV	VV	VV	VV
4. Olej/masnota	IIXIV	VV	IVIV	VV
5. Lihový fix	IIXIV	VV	IIXIIX	IVV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Měření č. 19	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	VV	VV	VV	VV
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	VV	VV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	IVV	VV	VV

Měření č. 20	Identifikace		Verifikace	
	Levá	Pravá	Levá	Pravá
Podmínky				
1. Normální	VV	VV	VV	VV
2. Rukavice	IIXIIX	IIXIIX	IIXIIX	IVIIX
3. Krém	VV	VV	VV	VV
4. Olej/masnota	VV	VV	VV	VV
5. Lihový fix	VV	VV	IVV	VV
6. Studené prostředí	VV	VV	VV	VV
7. Teplé prostředí	VV	VV	VV	VV
8. Mokrý	VV	VV	VV	VV

Výsledky sensor V2 IDENTIFIKACE	Neúspěšné	Opakované snímání při úspěšné identifikaci	Neúspěšnost	FRR	Shodnost FRR (0,01%)
1. Normální	0/80	2	0	0,00%	ano
2. Rukavice	37/80	6	0,4625	46,25%	ne
3. Krém	3/80	7	0,0375	3,75%	ne
4. Olej/masnota	1/80	6	0,0125	1,25%	ne
5. Lihový fix	20/80	13	0,25	25,00%	ne
6. Studené prostředí	0/80	0	0	0,00%	ano
7. Teplé prostředí	0/80	0	0	0,00%	ano
8. Mokrý	0/80	3	0	0,00%	ano

Výsledky sensor V2 VERIFIKACE	Neúspěšné	Opakované snímání při úspěšné verifikaci	Neúspěšnost	FRR	Shodnost FRR (0,01%)
1. Normální	0/80	0	0	0,00%	ano
2. Rukavice	30/80	11	0,375	37,50%	ne
3. Krém	2/80	5	0,025	2,50%	ne
4. Olej/masnota	0/80	9	0	0,00%	ano
5. Lihový fix	23/80	10	0,2875	28,75%	ne
6. Studené prostředí	0/80	1	0	0,00%	ano
7. Teplé prostředí	0/80	0	0	0,00%	ano
8. Mokrý	0/80	1	0	0,00%	ano