Využití krevního řečiště prstu pro biometrickou identifikaci osob

Bc. Roman Baroň

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Roman Baroň**
Osobní číslo:	**A12289**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití krevního řečiště prstu pro biometrickou identifikaci osob**
Téma anglicky:	**Using Finger Bloodstreams for the Biometric Identification of Individuals**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na biometrickou identifikaci osob.**
2. **V rámci literární rešerše se zaměřte na možnosti využití krevního řečiště pro identifikaci osob.**
3. **Proveďte základní měření identifikace osob pomocí krevního řečiště, při měření se zaměřte na spolehlivost použité metody.**
4. **Ověřte podobnost krevního řečiště rodinných příslušníků.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Vyd. 1. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**
2. **RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka: ve forenzních a komerčních aplikacích. Vyd. 1. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.**
3. **BLAŽEK, Vladimír a Radek TRNKA. Lidský obličej: Vnímání tváře z pohledu kognitivních, behaviorálních a sociálních věd. Vyd. 1. Praha: Karolinum, 2009. ISBN 978-80-246-1556-1.**
4. **LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.**
5. **BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.**
6. **MARIEB, Elaine Nicpon a Jon MALLATT. Anatomie lidského těla. Vyd. 1. Brno: CP Books, 2005, xvi, 863 s. ISBN 8025100669.**

Vedoucí diplomové práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá biometrickými charakteristikami lidského těla a biometrickými systémy. Práce seznamuje s charakteristikami lidského těla používanými v biometrických systémech zaměřených na krevní řečiště. Součástí práce je popis nejznámějších, ale i méně známých metod snímání a měření charakteristik lidského těla pro biometrické systémy. Praktická část se zaměřuje na terminál pro snímání krevního řečiště a otisků prstů MorphoAccess VP – Bio. Předmětem je popis terminálu, měření spolehlivosti terminálu a ověření shody krevního řečiště (otisků prstů) u rodinných příslušníků.

Klíčová slova: biometrie, biometrické systémy, identifikace, verifikace, krevní řečiště prstu

ABSTRACT

The thesis deals with biometric characteristics of human body and with biometric systems. The thesis presents the characteristics of human body used in biometric systems based on bloodstream. Part of this work describes the most common but also less common methods of removing and measuring of characteristics of human body for biometric systems. The practical part of this work is aimed on a terminal MorphoAccess VP - Bio used for removing bloodstream and fingerprints. The main object is to describe functionality of this terminal, to measure accuracy of the terminal and to prove a match of bloodstream (fingerprints) of family members.

Keywords: biometrics, biometrics systems, identification, verification, bloodstream finger

Touhle cestou bych chtěl poděkovat svému vedoucímu doc. Mgr. Milanu Adámkovi, PhD za odborné vedení, připomínky a cenné rady, které mi poskytoval během zpracovávání mé diplomové práce. Dále bych chtěl poděkovat Ing. Doře Lapkové a Ing. Michalu Pluháčkovi za konzultace, cenné rady, připomínky a trpělivost, které mi poskytovali během zpracovávání mé diplomové práce.

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

OBSAH

ÚVOD

Každý člověk je svým způsobem jedinečný a má charakteristiky, které jsou nezaměnitelné mezi jednotlivými jedinci. Příkladem mohou být např. otisky prstů. Tyto otisky u daného jedince vždy byly a budou jeho jedinečným identifikátorem.

Pro identifikaci jednotlivců se používají anatomicko-fyziologické a behaviorální charakteristiky člověka, které daly vzniknout jedinečným přístupovým biometrickým systémům založených na biometrii člověka. Jsou to jedny z nejspolehlivějších bezpečnostních systémů pro ochranu majetku a přístupů do objektů.

Diplomová práce je rozdělena na dvě části. Teoretická část se v prvních dvou kapitolách zaměřuje na historii biometrie a na používanou terminologii v biometrických systémech. V další části se práce věnuje lidskému tělu, kde jsou popsány charakteristiky lidského těla a cévní systém lidského těla se zaměřením na krevní řečiště. V poslední kapitole se práce věnuje stěžejnímu bodu teoretické části, kterou je vypracování literární rešerše zaměřenou na biometrickou identifikaci osob a využití krevního řečiště pro identifikaci osob. V rešerši jsou popsány nejznámější biometrické identifikační metody, kritéria pro biometrické systémy, jejich spolehlivost a využití v bezpečnostních aplikacích. V poslední části této kapitoly jsou popsány systémy pro měření krevního řečiště, kde jsou popsány možnosti využití systémů krevního řečiště, princip snímání krevního řečiště a typy biometrických systémů pro snímání krevního řečiště.

V první kapitole praktické části je detailně popsaný terminál pro snímání krevního řečiště MorphoAccess VP – Bio. Jsou zde popsány biometrické metody používané u terminálu MorphoAccess (krevní řečiště a otisk prstu) a jednotlivá použitá rozhraní. Dále jsou zde popsány možnosti propojení terminálu s PC, tabulky se základními technickými vlastnostmi terminálu a propojení terminálu s programem Easy2Enroll, popis vlastností a možnosti programu a první otestování terminálu. Druhá kapitola je zaměřená na praktické měření, kde je zjišťována spolehlivost a chybovost terminálu, měření shody otisků prstů (původně krevního řečiště) mezi 16 účastníky. Měření probíhalo vzájemně mezi všemi, mezi muži, ženami a rodinnými příslušníky. Tato část měření probíhala na terminálu MorphoSmart VP a programu MorphoEnroll. Zpracování a porovnání probíhalo přes program eFinger. Dále jsou zde popsány důvody přechodu z měření krevního řečiště na otisky prstů. Poslední část se věnuje vytvořením laboratorní úlohy pro budoucí využití ve školních laboratořích.

I. TEORETICKÁ ČÁST

1 HISTORIE BIOMETRIE

Biometrie jako systém pro rozpoznávání osob je znám již od pradávna. Už od dob, kdy se lidé začali vzájemně potkávat a poznávat se podle hlasu, obličeje nebo podle způsobu chůze atd. Jmenované způsoby jsou jen výčtem lidských charakteristik, kterými je člověk obdarován částečně již od svého narození. Všechny tyto charakteristiky jsou informace, kterými oplývá každý jedinec a které mohou být zaznamenány a následně strojově zpracovány. Jedná se tedy o signály, které nesou informace o našich biometrických charakteristikách. [1]

V dnešní moderní době je biometrie spojována převážně s počítačovou bezpečností, ale její počátky sahají mnohem dál do minulosti. Úplně za první a nejstarší biometrickou metodu můžeme považovat rozeznávání podle otisků prstů. Už v počátcích užívání této metody existovala spousta civilizací, které již měly nějakou znalost o papilárních liniích, které jsou obsaženy na lidské kůži. Příkladem může být třeba nález kamenů ve Spojených státech amerických na území dnešního státu Indiana, které obsahovaly rytinu znázorňující lidskou ruku s papilárními liniemi. Tyto kameny, nazývané též jako „petroglyfy“, byly stvořeny indiánskými kmeny, jejž obývaly toto území před několika tisíci lety před naším letopočtem. [9]

Podobně jako v Indianě, byly podobné pozůstatky otisků nalezeny také u Asyřanů. Tyto pozůstatky byly objeveny ve zříceninách starověkého asyrského města Ninive v místní části Aššurbanipalovy knihovny založené již v 9. století před naším letopočtem. Jednalo se o úlomky hliněných tabulek, které obsahovaly rozličné texty, ale také otisky prstů. Původně se archeologové domnívali, že otisky obsažené na tabulkách vznikly během jejich výroby, ale později byla tato domněnka vyvrácena, protože se otisky nacházely vždy na každé tabulce hned vedle vytesaného jména. Tím vznikla domněnka, že autor pravděpodobně svůj otisk umístil na tabulku schválně, aby zamezil falzifikaci tabulky. Podobné využití otisků prstů se prokázalo i u jiných archeologických vykopávek, které byly provedeny na různých místech v Egyptě, v Řecku a na místech tehdejšího území římského impéria. [9]

První dochované písemné zmínky o praktickém použití biometrie v historii byly např. v Egyptě nebo v Číně. V Egyptě se např. za pomocí biometrie řešilo neoprávněné nebo dvojí vyplácení měsíčních mezd. Jednalo se o identifikaci různých farmářů a dělníků na základě jejich jedinečného vzhledu (barva očí, barva pleti, výška, různé jizvy nebo

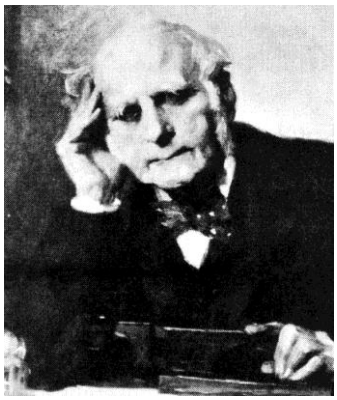
zranění, apod.), jenž se zaznamenával, a podle těchto informací se jednotliví pracovníci jednoznačné identifikovali. Ve 14. století v Číně bylo biometrie využito trochu jiným způsobem a to tak, že čínský kupec za pomocí inkoustu obarvoval dětem ruce, chodidla a vytvářel tak jejich otisky na papír. Důvodem bylo dokázání shody či odlišnosti jednotlivých dětí. [9][10][11]

První průkazné materiály o použití moderní biometrie se datují někde kolem poloviny 19. století našeho letopočtu. V tomto období se začaly otisky prstů využívat v kriminalistice. Mezi prvními, kdo využil biometrii v tomto století, byl **William James Herschel** (1833 - 1917), (Obr. 1) v roce 1858. Ten použil otisky u zaměstnanců dráhy pro potvrzení jejich identity. Použití otisků bylo jediným možným způsobem, jak prokázat identitu jednotlivých dělníků, protože většina z nich neuměla vůbec číst ani psát a tudíž od nich nemohl očekávat podpis. Tento otisk potvrzoval jejich identitu při přebírání platu. Podobný princip použil i v Indii, kde žil. Zde měl za úkol vyplácení „důchodů" indickým vojákům, kteří ale neměli žádné osobní doklady a nemohl tak některé z nich rozeznat od Evropanů. Herschel měl podezření, že se výplata vydává i osobám, které již zemřely, a zavedl proto nový výplatní systém, který měl těmto podvodům s vydáváním výplat zamezit. Proto musela každá výplata, která byla vyplacena, být potvrzena otiskem prstu na výplatní listinu. Později Herschel nabídl tuto metodu i pro využití ve věznici, kde měla zamezit záměnám mezi jednotlivými zločinci, jenž byli ohodnoceni na těžké a lehké případy. Tato metoda však nebyla nikdy použita. [1][9]

Obr. 1 William James Herschel [1]

V roce 1865 přišel se studií o dědičnosti fyzických vlastností **Francis Galton** (1822 - 1911), (Obr. 2), která pojednávala o tom, že narozené děti přebírají a dědí některé vlastnosti po svých rodičích. Mezi těmito vlastnostmi mohou být jak fyzické

charakteristiky, tak i některé vlastnosti jako je chování nebo jednání. V roce 1869 se Galton stává spoluzakladatelem vědy zvané *eugenika*, což je věda o dědičných chorobách a vadách u plodu. O rok později se Galton stává zakladatelem výzkumu dvojčat. V roce 1880 přichází s vědním oborem nazvaným antropometrie, což je obor zabývající se měřením lidských tělesných rozměrů. V roce 1892 publikoval Galton svoji práci s názvem „Fingerprints“, z nějž vychází zavedení daktyloskopie do praxe v roce 1900. V tomtéž roce Galton prosazuje použití daktyloskopie pro identifikační a verifikační účely. Prokázal neměnnost a jedinečnost papilárních linií na prstech. Poté byla daktyloskopie zavedena do policejní praxe. [1]



Obr. 2 Francis Galton [1]

Za počátky moderní biometrie můžeme považovat rok 1882. V tomto roce jistý **Alphonse Bertillon** (1853 – 1914), (Obr. 3), antropolog a šéf oddělení identifikace pachatelů u pařížské policie hledal nějaký způsob, kterým by mohl usvědčovat už jednou zatčené pachatele. Tito recidivisté totiž při každém zatčení používali falešná jména a údaje. Úřady jim ale nebyly schopné jejich opakované přečiny prokázat. Tomuto se pokusil zabránit Bertillon svojí metodou, kterou nazýval „bertillonáž“. Tato metoda spočívala v měření fyzických vlastností, které se u člověka v průběhu života už nemění. Pro zjišťování identity Bertillon používal některé charakteristické tělesné rysy jako např. velikost lebky, velikost nohy nebo délka prstu. Všechny tyto informace se zaznamenávaly a zanášely do antropometrických karet, jenž se seřazovaly podle velikosti hlavy do tří tříd, později doplněny i o otisky prstů a fotografii. Metoda se rychle rozšířila a začala se používat u policie a vyšetřovatelů po celém světě. Jenže jako každá prvotní metoda měla i tato metoda menší či větší chyby. Třeba se přišlo na to, že někteří jedinci mohou mít stejnou velikost hlavy, čímž docházelo k nechtěným záměnám v identifikaci pachatelů, kdy mohly být dva jedinci se stejnou velikostí hlavy považování za téhož člověka. Kvůli těmto nedostatkům byla jeho metoda odsouzena k zániku, a jak rychle byla zavedena, tak rychle

se přestala i používat. Některé Bertillonovy metody, inovace a hlavně standardizované fotografování pachatelů a systematické zpracování fotografií místa zločinu se však používají dodnes. [1][9]

Obr. 3 Alphonse Bertillon [1]

Mezi další průkopníky biometrie (Obr. 4) se řadí **Henry Faulds** (1843 – 1930), který se zabýval problematikou otisků prstů. Dále také **Juan Vucetich** (1838 – 1925) nebo český přírodovědec **Jan Evangelista Purkyně** (1787 – 1869). Purkyně byl první, kdo popsal jednotlivé typy charakteristických kreseb papilárních linií na koncích prstů, které rozdělil do 9 různých vzorů. [9]

Obr. 4 Zleva: Henry Faulds, Juan Vucetich, Jan Evangelista Purkyně [2]

2 ZÁKLADNÍ POJMY (TERMINOLOGIE)

V biometrii existuje několik pojmů, které se používají v bezpečnostních systémech. Tyto pojmy jsou odvozeny z anglického nebo latinského jazyka. Patří sem biometrie, identita, identifikace, autentizace, autorizace, verifikace, rekognoskace.

2.1 Biometrie

Pojem *biometrie* (biometric) je složenina ze dvou slov, a to ze slov *bio – život* a *metric – měření*. Pod pojmem *bio* si můžeme představit vědní obor, který se zabývá studiem a zkoumáním všech živých organismů, v našem případě hlavně člověka a jeho vlastností. Druhé ze slov *metric* se zaměřuje na měření biologických charakteristik člověka a jeho chováním. Celkově lze tedy na pojem biometrie nahlížet jako na vědu, jenž se zabývá měřením a zkoumáním „živých“ charakteristik člověka. [9][11]

2.2 Identita

Pojem *identita*, anglicky *identity*, latinsky *identitas*, odvozené od slova *idem – stejný*. Můžeme také použít termín *totožnost*. Tento pojem se používá tehdy, když porovnáváme nějaký pojem, objekt, situaci apod. a můžeme říci, že jsou si vzájemně záměnné. Z toho vyplývá, že jsou si rovny. Jedná se tedy o identitu, neboli totožnost něčeho s něčím nebo se sebou samým. Identitu můžeme rozdělit na 2 typy. Na identitu elektronickou a na identitu fyzickou. Elektronických můžeme mít hned několik např. nějakou svoji identitu na webové stránce, kde jsme registrovaní. Naopak fyzickou identitu máme každý jenom jednu, která je jedinečná. Neexistují dva lidi, kteří by ji měli shodnou. Fyzická je tvořena fyziologickými, anatomickými a behaviorálními rysy. [2][12]

2.3 Identifikace

Pojem *identifikace*, anglicky *identification*, latinsky *idem facere*. Jedná se o proces zjišťování totožnosti osob. Osoba se musí nejdříve zaregistrovat tak, že předá svoje biometrické vlastnosti do systému, které se potom uloží do databáze. Systém má za úkol zjistit identitu neznámé osoby. To se provede na základě srovnání uložených informací v databázi (šablona) a aktuálně sejmutých informací (vzorek). Tento proces porovnání se děje tak dlouho, dokud nedojde ke shodě údajů v databázi. Výstupem je buď nalezení identity a povolení ke vstupu nebo zamítnutí vstupu, protože nedošlo ke shodě. Jestliže dojde k identifikaci uživatele, dojde k povolení ke vstupu. Režim identifikace je náročnější

na výkon systému, než verifikace, protože se vzorek porovnává se všemi šablonami uloženými v databázi. [12][13][14] Identifikaci můžeme rozdělit na:

2.3.1 Policejně-soudní identifikace

Policejně-soudní identifikace sice patří mezi nejnáročnější metody, za to je ale nejspolehlivější ze všech. Metody používané v tomto typu identifikace nám zaručují jednoznačnou totožnost osoby mezi miliony dalších jedinců. Pro práci v policejně-soudní identifikaci se využívají různá laboratorní pracoviště a jejich počítačová a ostatní výbava. Tyto metody jsou nejčastěji používány bezpečnostními složkami, popř. dalšími orgány činných v trestním řízení. [2][14] Mezi nejčastější metody patří:

- daktyloskopie,
- analýza DNA,
- fonetická analýza lidského hlasu,
- pach lidského těla,
- tvar vnějšího ucha, apod.

2.3.2 Bezpečnostně-komerční identifikace

Tyto typy metod jsou běžně používány v kriminalistice a jiných bezpečnostních oborech. Potom byly upraveny pro použití v bezpečnostní a komerční sféře. Některé metody zde používané musely být pro použití v bezpečnostně-komerční identifikaci zjednodušeny, aby s nimi byla práce ulehčena, a naopak některé byly rozpracovány a rozvinuty hlouběji. Důvodem takového zjednodušování nebo většího prohloubení bylo průmyslové a komerční nasazení přímo v praxi. Díky tomu v komerční sféře vzniklo velké množství aplikací, jež mohou být použity zpětně i v policejně-soudní identifikaci.

Tam, kde je u policejně-soudní identifikace potřeba lidského faktoru, tam je bezpečnostně-komerční identifikace zcela automatizována. U tohoto typu identifikace se v současné době pro identifikaci používají metody založené na poznatcích z daktyloskopie, anatomických, fyziologických a behaviorálních vlastností apod. I když jsou tyto technologie používané v bezpečnostně-komerční identifikaci vcelku drahé, stále vycházejí v plošném použití levněji, než použití technologií v policejně-soudní identifikaci. [2][14]

2.3.3 Ezoterická identifikace

Do ezoterické identifikace můžeme zařadit metody, které nejsou zatím ve velkém povědomí, tzn., že nejsou moc známé, rozšířené nebo nejsou ještě dostatečně prověřené, aby mohly být rozsáhleji použity v praxi. I když nejsou tyto metody natolik rozšířené, jsou mezi nimi metody, kterým je věnovaná velká pozornost, protože se z nich mohou stát metody, které v budoucnu budou rovnocennými partnery v policejně-soudní nebo bezpečnostně-komerční identifikaci. [2][14] Mezi ezoterické identifikační metody můžeme zařadit:

- bipedální lokomoci,
- termovizní obrazy lidského těla,
- otisky rtů,
- otisky pórů,
- pach lidského těla,
- obsah solí v lidském těle,
- struktura vroubkování nehtu, apod.

2.4 Verifikace

Pojem *verifikace*, anglicky *verification*, latinsky *verum facere – činit pravdivým*. Verifikace následuje po identifikace, jedná se tedy o ověření pravdivosti výroku. Bezpečnostní systém už zná identitu uživatele a úkolem verifikace je potvrdit identitu tohoto uživatele. Pokud je záznam nalezen, dojde k porovnání dat mezi vzorkem a šablonou. Jakmile se dosáhne vzájemné shody mezi vzorkem a šablonou, je proces verifikace ukončen a identita je potvrzena nebo v opačném případě vyvrácena. Verifikace je ve většině případů rychlejší a méně náročná na operační výkon než identifikace, protože systém srovnává jen jeden vzorek s jednou šablonou v databázi. Tento proces je též někdy nazýván jako One-to-One. [12][13]

2.5 Autentizace

Pojem *autentizace*, anglicky *authentication*. Jedná se proces ověření proklamované identity subjektu. Po dokončení autentizace obvykle následuje autorizace. Autentizace je podobná rekognoskaci. Na rozdíl od rekognoskace, ale na konci autentizace získává uživatel nějaký status, např. oprávněný/neoprávněný, apod. [11][12]

2.6 Autorizace

Pojem *autorizace*, anglicky *authorization.* Je proces získávání souhlasu s provedením nějaké operace, povolení přístupu někam nebo k něčemu.

2.7 Rekognoskace

Pojem *rekognoskace*, anglicky *recognition*. Pojem v oblasti biometrie znamená rozpoznávání člověka při zkoumání vhodné biometrické vlastnosti. Tento termín nemusí nutně znamenat identifikaci nebo verifikaci. [11][12]

3 LIDSKÉ TĚLO

3.1 Charakteristiky lidského těla

Charakteristiky lidského těla nebo také biometrické charakteristiky, jsou vlastnosti, se kterými se člověk už rodí nebo je získává v průběhu života učením. Některé jsou neměnné od narození (např. DNA), a některé se vyvíjí až v průběhu života (např. oční duhovka). Mezi biometrické charakterisitky můžeme zařadit anatomické, fyziologické a behaviorální charakteristiky. Lidské tělo se skládá ze třech základních částí. Tyto části se dále dělí na jednotlivé podčásti. Mezi tyto tři základní části patří hlava, trup a končetiny. Končetiny můžeme dále rozdělit na horní končetiny (ruce) a dolní končetiny (nohy).

Charakteristiky lidského těla lze snímat pro potřeby policejně-soudní (kriminalistika, jiné policejní vyšetřování, apod.) nebo pro bezpečnostně-komerční potřeby (identifikační přístupové systémy, identifikační průkazy, apod.). **Hlava (caput)** jako samostatná oblast obsahuje velké množství měřitelných části lidského těla pro potřebu biometrického snímání. Do policejně-soudních potřeb můžeme zařadit otisky ucha, otisky rtů, otisky zubů, póry, aj. a bezpečnostně-komerčních potřeb, můžeme zase zařadit snímání obličeje, snímání duhovky a sítnice, snímání hlasu a řeči. Oblast **trupu (truncus)** nemá v bezpečnostní sféře velké využití, protože neexistuje téměř žádný biometrický přístupový systém, který by pracoval na základě nějaké části lidského trupu. Tato oblast má využití spíše v oblasti policejně-soudní identifikace. Další oblastí jsou lidské končetiny, které můžeme rozdělit na **horní končetiny (membrum superius)** a **dolní končetiny (membrum inferius).** V biometrické identifikaci mají končetiny největší využití.

Končetiny lze pro policejně-soudní potřeby využít převážně v oblasti snímání otisků prstů a dlaní na místě činu, otisků chodidel (trasologie[1]), otisky jiných částí končetin, apod. Pro potřeby bezpečnostně-komerční mají končetiny mnohem větší uplatnění např. snímání otisků prstů a dlaní, snímání krevního řečiště prstů, dlaní a hřbetů ruky, snímání chůze (bipedální lokomoce), snímání písma a rukopisu, snímání dynamiky stisku počítačových kláves, apod. Poslední oblastí jsou vlastnosti, které jsou společné pro celé tělo. Příkladem

[1] Trasologie - kriminalistický obor, který se zabývá zkoumáním stop (např. obuvi, nohou, pneumatik apod.).

může být DNA[2] (krev, sliny, atd.), které má využití převážně v kriminalistice nebo snímání pachu. [17]

3.1.1 Anatomické charakteristiky

Anatomie zkoumá stavbu lidského těla (z širšího přírodovědného hlediska živočišného těla vůbec). Popisuje tvar, vnitřní složení a polohu jednotlivých částí, a tím umožňuje pochopit i jejich funkci. Pojem anatomie je sice hojně používán, ale kvůli rychlému vývoji disciplín studujících mikroskopickou stavbu orgánů a tkání, tento pojem z pohledu vědních oborů vyhovovat. Proto se zavedl pojem *morfologie*[3]. Anatomie je v tomto pojetí součástí morfologických věd. [6][17]

V celém lidském těle nejsou tkáně izolované, ale sdružují se ve větší celky, tzv. orgány. Tyto orgány, nazývané též jako ústroje, jsou celky, které jsou určeny k určité funkci. Orgány, které svojí činností navazují na činnost jiných orgánů a spolupracují spolu, vytvářejí větší funkční celek, který nazýváme soustava orgánů. Jejich vzájemnou součinností, souhrou a závislostí jsou zajišťovány základní životní funkce organismu. Soustavy orgánů můžeme rozdělit na 11 typů soustav (soustava kosterní, svalová, oběhová, dýchací, trávící, kožní, vylučovací, pohlavní, nervová, smyslová, soustava žláz s vnitřním vyměšováním). [6][18]

3.1.2 Fyziologické charakteristiky

Fyziologie se zabývá funkčními projevy organismu jako celku, zkoumá činnost jednotlivých tělesných soustav, jejich souhru a vztahy organismu k prostředí. Základní stavební jednotkou je buňka, která tvoří tkáně (svalovou, nervovou, aj.). Funkčně i stavebně definované celky tvoří orgány sestavené z různých tkání. [6]

- *Genotypické charakteristiky* – jedná se o vlastnosti jedince, které jsou geneticky zděděné po rodičích rodičů, rodičích atd. Tyto vlastnosti jsou časově neměnné a neovlivnitelné a tedy vhodné pro použití v biometrických systémech,

---

[2] DNA (deoxyribonucleic acid) - Deoxyribonukleová kyselina. Molekula kódující geny odpovědné za strukturu a funkci živého organismu a umožňující přenos genetické informace z generace na generaci.

[3] Morfologie – věda integrující obory zabývající se zkoumáním tvaru, stavby a vývoje těla.

- *Fenotypické charakteristiky* – jedná se o vlastnosti jedince, které se nedědí a vznikají náhodně ve stádiu embrya. V tomto stádiu se vlastnosti vytvářejí pro každého člověka jedinečně. Příkladem mohou být otisky prstů, barva duhovky, a mnohé další. [19]

3.1.3 Behaviorální charakteristiky

Behaviorální charakteristiky, někdy též nazývané jako dynamické, jsou vlastnosti, se kterými se člověk nerodí, ale učí se je během svého života. Dobrým příkladem behaviorální charakteristiky člověka může být lidská chůze. Ta se začíná projevovat v cca 9 měsících, kdy je dítě schopné vertikalizace nejprve jen s podporou a poté i bez podpory. Poté se lidská chůze, ale i jiné behaviorální vlastnosti vyvíjejí stále dál, až se z nich stanou jedinečné vlastnosti pro každého jedince, které lze potom využít pro biometrické systémy. Výhodou behaviorálních charakteristik oproti jiným biometrickým charakteristikám je, jejich snadnější užívání a není nutné speciálního hardwaru, se kterým by musela osoba pracovat. [19][21] Nejběžnější biometrické behaviorální systémy jsou založené na:

- bipedální lokomoci,
- dynamice podpisu,
- dynamice stisku počítačových kláves,
- hlasu a řeči, apod. [20]

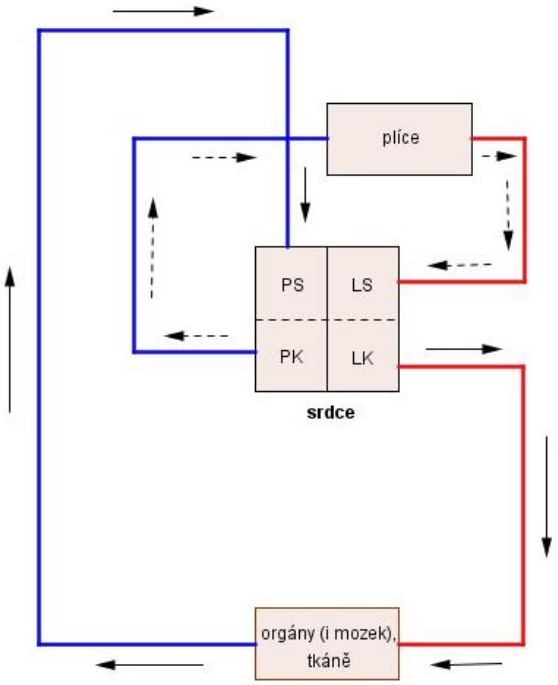
3.2 Krevní řečiště lidského těla

Krevním řečištěm v této kapitole myšlen krevní oběh, jehož médiem je krev. Každý člověk má ve svém těle jedinečné rozložení jednotlivých cév. Této jedinečnosti lze využít pro rozeznání jednotlivých lidí pomocí biometrických systémů. Systémy pro měření krevního řečiště se využívají převážně pro měření na prstech, dlaních, hřbetech ruky a na zápěstích.

3.2.1 Cévní systém

Cévní systém (Obr. 5), nazývaný též jako oběhová soustava nebo kardiovaskulární systém, je jedna z mnoha orgánových soustav živočichů (mezi další patří např. pohybová soustava, mízní soustava, dýchací soustava, trávící soustava apod.), jenž slouží např. pro přenos

živin, plynů a odpadních látek z tkání nebo do tkání. Pro přenos těchto médií slouží krev nebo hemolymfa (krvomíza). [7][8][15]



Obr. 5 Cévní systém [8]

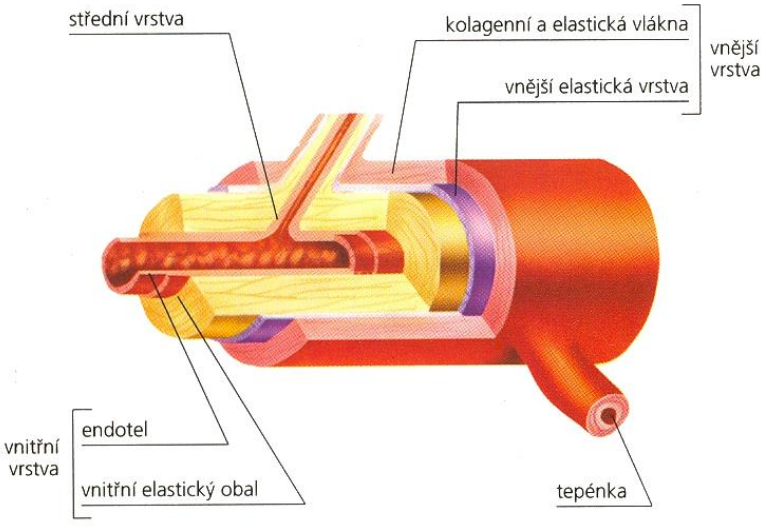
3.2.2 Skladba cévního systému

Cévní systém se skládá ze srdce, soustavy krevních a mízních cév, kostní dřeně, sleziny, mízních uzlin a nervového řízení. Jednotný cévní systém můžeme rozdělit na soustavu krevních cév (systema vasculare), srdce (cor) a mízní soustavu (systema lymphaticum). S cévním systémem úzce souvisí i lymfatická soustava. Tato soustava se skládá ze sítě lymfatických cév, jenž odvádějí tkáňovou tekutinu tzv. lymfu zpět do krevního oběhu. [7]

- *srdce* – hlavním a nejdůležitějším orgánem krevního oběhu je srdce. Jedná se svalovou pumpu, jenž se skládá z levé a pravé síně a levé a pravé komory. Levá síň a levá komora jsou odděleny přepážkou od pravé síně a pravé komory,
- *soustava mízních cév (lymfatická soustava)* – lymfatická soustava nemá na rozdíl od soustavy krevních cév žádný „hnací motor“ jako je srdce. Struktura je velmi podobná té, jako je u krevní soustavy. Lymfatický systém je složen z lymfatických kapilár, cév, lymfatických uzlin, kmenů (mízovody) a orgánů (brzlík, mandle, slezina, kostní dřeň a slepé střevo). V lymfatickém systému koluje lymfa (míza),

- *soustava krevních cév (krevní soustava)* – oběhová soustava člověka patří mezi uzavřené oběhové soustavy obratlovců. V uzavřené oběhové soustavě obratlovců se krev transportuje a rozvádí pomocí soustavy krevních cév (systema vasculare), které lze rozdělit na 3 základní typy (tepny, žíly a vlásečnice). Tepny a žíly jsou potom mezi sebou navzájem široce propojeny pomocí krevních vlásečnic (kapilár),
- *kostní dřeň, slezina, mízní uzliny, nervové řízení.* [7][8]

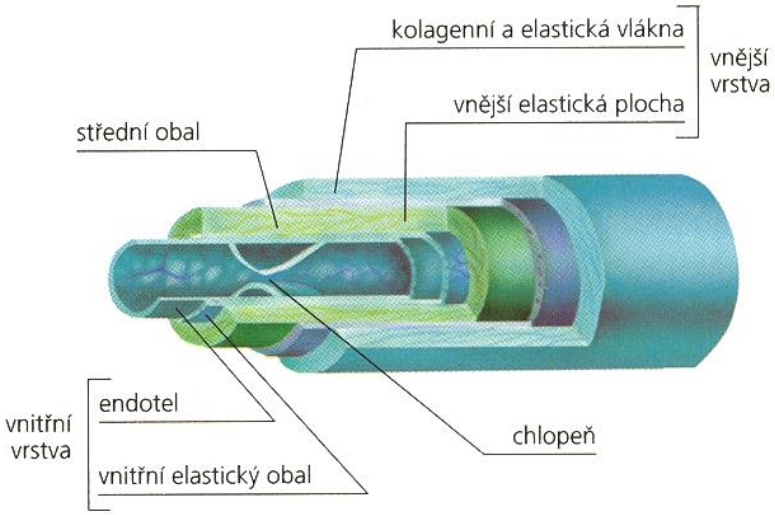
Tepny (arterie) – tepny (Obr. 6) se rozdělují podle světlosti. Podle světlosti můžeme rozlišovat tepny velké (ø 8 mm), větší, včetně aorty (ø 26 mm), dále na malé a střední (až ø 3 mm) a nakonec tepénky, nazývány též jako arterioly (ø cca 10^2 μm). Směrem od aorty tlak i rychlost toku krve klesá, neboť postupným větvením se zvětšuje výsledná světlost, daná součtem jednotlivých průměrů těchto cév. Celkový průměr (cca 0,4 m^2) kapilár je mnohonásobně větší než světlost aorty. Průměr hrudní aorty s věkem vzrůstá, kdežto průměr kyčelní a stehenní tepny se s věkem prakticky nemění, narůstá ovšem tloušťka její stěny. [7][15]



Obr. 6 Řez tepnou [16]

Žíly (vény) – žíly (Obr. 7) přivádějí krev do srdce a odvádějí krev z vlásečnic. Žíly můžeme rozdělit na velké, střední, malé (ø cca od 1 mm do 9 mm) a žilky, nazývány též jako venuly (ø cca od 0,02 mm do 1 mm). Přetlak v žilách klesá směrem k srdci, a to asi ze 2 kPa v kapilárách na asi 0,8 kPa ve velkých mimohrudních žilách. Nejnižší je v pravé síni. Největší žilní návrat je při vdechu, kdy se nitrohrudní podtlak mění z cca 0,35 kPa na 0,8 kPa a klesá rovněž tlak v pravé síni. Současné snížení bránice

zvyšuje nitrobřišní tlak a tím i tlakový spád v hrudníku, což dále podporuje návrat žilní krve do pravé síně a tím i množství krve vypuzované pravou komorou. [7][15]



Obr. 7 Řez žilou [16]

Vlásečnice (kapiláry) – jedná se o nejmenší a nejtenčí cévy v lidském těle, které dosahují délky cca 0,5 mm, průměru cca 20 μm a zabírají plochu cca 6300 m^2. Vlásečnice tvoří husté sítě v jednotlivých orgánech, které bývají různě upravené. Mezi stěnami vlásečnic dochází k veškeré látkové výměně mezi krví a tkáněmi. Vlásečnice se samy aktivně neuzavírají, to obstarávají prekapiláry se svěrači, jejichž otevírání a zavírání rozhoduje o velikosti kapilárního povrchu, který bude v kontaktu s krví. [7][15]

4 BIOMETRICKÉ SYSTÉMY

4.1 biometrické identifikační metody

Pro potřeby biometrické identifikace lze lidské tělo rozdělit na několik základních oblastí. Biometrické oblasti lze rozdělit podle lidského těla na oblast hlavy, oblast rukou, oblast nohou a ostatní.

Tab. 1 Srovnání biometrických metod [1][2][5]

Metoda	Oblast využití		Rozhraní s uživatelem	Charakteristika		Přesnost
	P-S	B-K		A-F	B	
Snímání obličeje	+	-	obličej je sejmut snímačem na vzdálenost cca 2 m	+	-	●●
Duhovka	-	+	pohled do kamery ve vzdálenosti od cca 30 cm	+	-	●●●
Sítnice	-	+	oko se zaměří na bod optického snímače, na vzdálenost cca 2 cm	+	-	●●●
Vnější ucho	+	+	uživatel nastaví ucho ke snímači	+	-	●●
Hlas a řeč	+	+	uživatel vysloví frázi nebo slovo do mikrofonu	-	+	●
Otisky prstů	+	+	prst se pokládá na plochu snímače	+	-	●●●
Otisk dlaně	+	+	dlaň se pokládá na plochu snímače	+	-	●●●
Vroubkování nehtu	-	+	prst je vložen do speciálního snímače	+	-	●●●
Žíly hřbetu ruky	-	+	ruka je vložena do snímače	+	-	●●
Žíly dlaně ruky	-	+	dlaň je vložena nebo položena do zařízení se snímačem	+	-	●●
Žíly prstu ruky	-	+	prst je položen nebo vložen do zařízení se snímačem	+	-	●●
Dynamika podpisu	+	+	podpis je uskutečněn speciálním perem na speciální podložku	-	+	●
Dynamika stisku PC kláves	-	+	uživatel píše vzorový text na klávesnici	-	+	●●

Bipedální lokomoce	+	+	snímání pohybu nohou je snímáno na dálku	-	+	●●
DNA	+	-	mnoho způsobů získání (krev, sliny, sperma atd.)	+	-	●●●
Snímání pachu	+	-	většinou kus látky s pachem je vložena do speciální láhve nebo sáčku	+	-	●
Ortodoncie	+	-	otisky zubů jsou sejmuty z daného předmětu	+	-	●
Snímání pohybu rtů	+	+	snímání pohybu rtů probíhá na dálku	+	-	●
Otisky pórů	+	-	otisky póru jsou sejmuty z daného předmětu	+	-	●
Geometrie ruky	+	+	ruka se pokládá na plochu snímače	+	-	●

● Nízká ●● Střední ●●● Vysoká

P-S…….policejně-soudní identifikace

B-K……bezpečnostně-komerční identifikace

A-F……anatomicko-fyziologická charakteristika

B……behaviorální charakteristika

4.1.1 Snímání obličeje

Obličej můžeme považovat za jeden z nejznámějších biometrických rysů u člověka. Rozpoznávání podle obličeje používáme každodenně v zaměstnání, ve škole nebo běžně na ulici. Poznáváme převážně podle vzhledu obličeje. Každý má obličej jiný a jedinečný, jinou velikost hlavy, očí, uší, rtů, nosu, brady nebo vzdálenost mezi nimi (např. oči). Díky této lidské variabilitě existují milióny jedinečných obličejů po celém světě. I dvojčata, která jsou na první pohled úplně stejná, se od sebe odlišují v jednotlivých nepatrných nuancích. [1][3]

Při vzniku biometrických systémů zaměřených na snímání obličeje se běžně používaly 2D systémy. Ty ale po čase přestaly vyhovovat a pro zvýšení spolehlivosti a nepodvrhnutelnosti systému se začaly používat systémy pro 3D snímání, které zároveň

zvyšují také biometrickou entropii. Nynější nejnovější 3D systémy jsou i lépe chráněny před podvrhy a podvody např. použitím busty lidské hlavy. Tyto systémy používají pro snímání termosnímače, které dokážou odhalit, zda se jedná o bustu nebo živou lidskou tvář. [1][3]

Pro rozpoznávání lidského obličeje můžeme tedy použít několik metod. Snímání 2D, snímání 3D, termosnímky nebo jejich kombinace. Výhodou u 2D systému je, že je registrace možná i přes fotografii a použití běžných kamery. 3D systémy jsou zase velmi přesnou a spolehlivou metodou s jednoduchou obsluhou. Nevýhodou 2D systému je jeho nízká přesnost a bezpečnost (lehce oklamatelný), změna vzhledu může mít negativní vliv na identifikaci, získání identifikačního prvku uživatele a jeho zneužití je velmi snadné. Nevýhodou 3D systému je citlivost na světlo, vysoká cena, omezení dosahu kamery. Stejně jako u 2D systémů je problém i zde se změnou vzhledu, i když ne tak velký. [4]

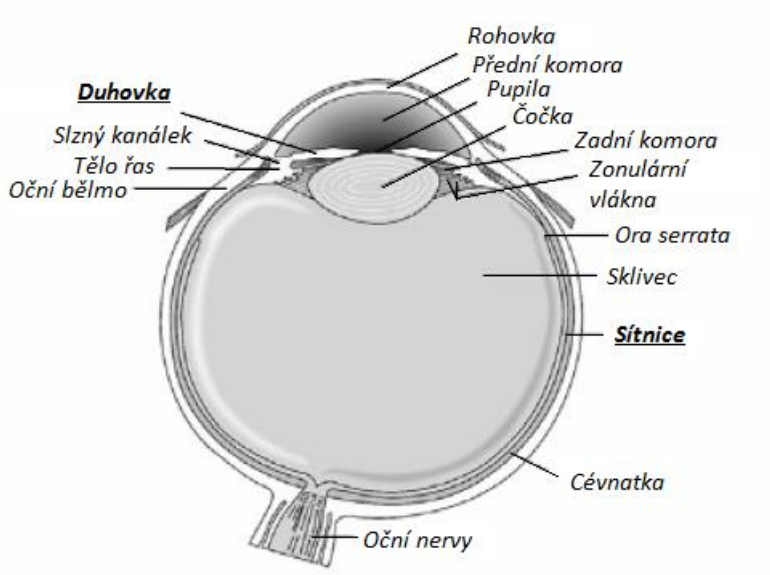
Jak už bylo řečeno, každý obličej je jiný, čili jedinečný. To je způsobeno variabilitou, která je zapříčiněna mnoha vlivy:

- **mimikou obličeje** – mimikou může být poměrně dramaticky změněn snímaný obrázek. Nejvíce kolem úst, očí, obočí a čela,
- **porostem (vlasy, vousy)** – i delší vlasy nebo vousy můžou poměrně dost změnit vizáž jedince,
- **osvětlení** – také hůře osvětlená nebo naopak přesvětlená místnost může mít za následek špatnou identifikaci jedince. Venku mohou nastat problémy s proměnlivostí a intenzitou světla,
- **doplňky (brýle, čepice, apod.)** – nošení různých módních doplňků může ovlivnit snímaný obrázek a následně jejich identifikaci,
- **stárnutí** – posledním vlivem je vliv stárnutí. Není příliš jasné, jak velký vliv má stárnutí na snímání. Systém má v databázi snímky, podle kterých se posuzuje identita člověka. Jenomže časové období mezi snímky je příliš krátké na to, aby se takové dlouhotrvající změny projevily. [1]

4.1.2 Oční duhovka a sítnice

Podobně jako některé jiné části lidského těla jsou unikátní, tak i lidské oko (Obr. 8) je jedinečné a lze jej použít v biometrických systémech. V lidském oku se nachází hned dvě části, které vykazují vysokou biometrickou entropii. První částí je oční duhovka,

někdy nazývaná též jako panenka a druhou je oční sítnice, které je umístěna uvnitř oka, je tedy pouhým pohledem nepozorovatelná. Vzorkování na duhovce a vzor žil na sítnici je u každého člověka zcela unikátní, kde tohle platí i u jednovaječných dvojčat. [1]



Obr. 8 Skladba lidského oka [1]

V biometrických systémech je snímání oka (ať už oční duhovky nebo oční sítnice) velmi mladé odvětví, které se rozvíjí až v posledních letech. Mezi první patenty na automatizované rozpoznávání podle oční duhovky je známé z roku 1994. U oční duhovky i oční sítnice je velkou výhodou, že obsahují velké množství informací, a že lze tuto metodu použít u větší skupiny uživatelů. Další výhodou je, že biometrické systémy založené na tomto lidském orgánu (oku), lze velmi obtížně nepovoleně obejít. Důvodem je obtížnost při získávání záznamů oční duhovky a především oční sítnice. [1][4] Skladbu lidského oka můžeme rozdělit na:

- **rohovka** – nachází se v přední části oka. Průhledná vazivová tkáň, která spolu s čočkou umožňuje lom světelných paprsků do oka,
- **přední komora** – komora, která je vyplněna nitrooční tekutinou. Tato tekutina se neustále obnovuje,
- **duhovka** – kruhovitě uspořádána svalovina, která zužuje a rozšiřuje zornici,
- **pupila (zornice)** – černý otvor uprostřed duhovky. Jejím úkolem je regulace množství světla přicházejícího do oka,
- **čočka** – čočka má schopnost se vyklenovat, a tím měnit index lomu,

- **oční bělmo** – bílá vrstva, pokrývající celou oční bulvu, která v přední části přechází v rohovku,
- **sítnice** – vnitřní část, která obsahuje světlocitlivé buňky. Je na ní zobrazen viděný obraz,
- **sklivec** – čirá hmota, která vyplňuje vnitřní část oka,
- **oční nerv** – nerv nesoucí velký počet nervových vláken ústící do centrálního nervového systému. [1]

Oční duhovka

Při pohledu do lidského oka je duhovka barevná část oka, která se může projevovat několika barvami. Téměř každý jedinec má při porodu neutrální barvu očí, která se začne v průběhu jeho života přebarvovat a měnit. Duhovka je silně pigmentována a její barva se pohybuje nejběžněji ve stupnici odstínů modré, hnědé, zelené, šedé nebo jejich kombinacích. Občas se může stát, že kvůli nedostatku pigmentu (melaninu) se u člověka projeví vzácná genetická porucha tzv. albinismus. [1]

I u duhovky, jako u většiny ostatních problémů rozpoznávání vzoru je hlavním problémem variabilita uvnitř jedné třídy a mezi jednotlivými třídami. Každého jedince můžeme spolehlivě rozpoznat jedině tak, že rozdíl mezi jednotlivými vlastnostmi jedné ze tříd je menší než rozdíl mezi jednotlivými třídami. Při dodržení daného principu, že variabilita mezi třídami by měla být větší, než variabilita uvnitř jedné třídy, nabízí vzory oční duhovky významný přístup ke spolehlivé identifikaci osob. Výhodou je, že je oční duhovka stabilní během života, systém je uživatelsky příjemný. Dále je duhovka dobře chráněna vůči vnějším vlivům a poskytuje velkou míru biometrické entropie informace. Nevýhodou je, že k podvedení systému může být použita kontaktní čočka nebo fotografie a také strach budoucích uživatelů, že systém může poškodit oko. [1][2]

Mezi další problémy nebo omezení, které mohou být spojovány s biometrickými systémy na bázi oční duhovky, je např. spolupráce uživatele. Tento uživatel musí stát na přesně definovaném místě, v definované vzdálenosti a musí se dívat přímo do snímače. Problémem je také, že tyto systémy jsou velmi nákladné na vysoký operační výkon.

Dalším běžným problémem je zdravotní stav uživatelů. Důvodem můžou být různé nemoci (nystagmus[4], aniridia[5]) nebo operace šedého zákalu. [1]

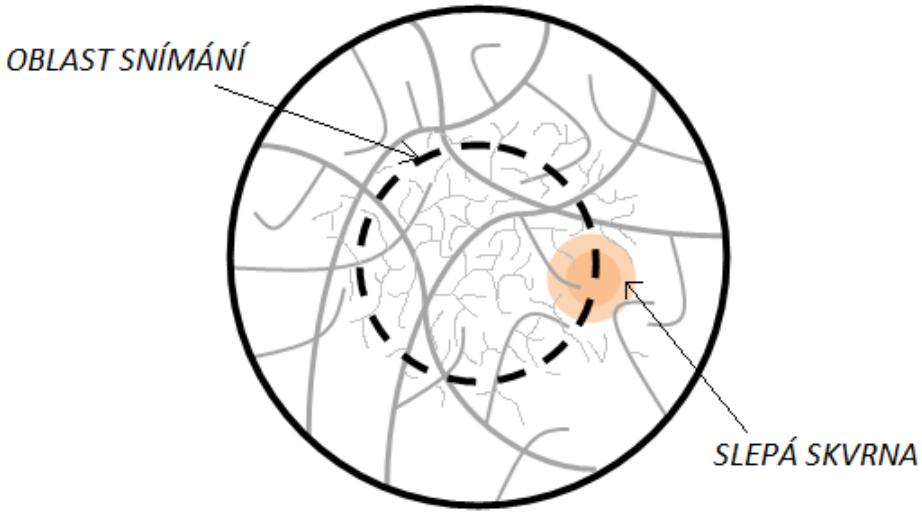
Oční sítnice

Další biometrickou metodu pro rozpoznávání, kterou nám oko nabízí, je oční sítnice (*retinal identification*). Snímání sítnice na rozdíl od snímání duhovky je mnohem složitější, protože potřebujeme získat dostatečně kvalitní snímek očního pozadí. Tato metoda funguje na principu snímání a srovnávání obrazu vzoru (choroid) získanou ze sítnice oka a na základě toho provádí identifikaci osob. Systémy pro snímání sítnice jsou založeny na speciálních optických kamerách. [1] Jak bylo už napsáno v předchozím odstavci, získat kvalitní snímek oční sítnice je mnohem složitější, než získat snímek duhovky. Je to z toho důvodu, že duhovka je na přední straně oční bulvy, kdežto sítnice se nachází na zadní straně oční bulvy. Světlo, které prochází do oka, je detekováno sítnicí a tato informace je dále vedena do mozku. Obraz, který dopadá na sítnici, je zaostřen čočkou a oční duhovka upravuje množství světla dopadající na sítnici. Za sítnicí se nachází choroidální vaskulatura, což je řada cév. Tím, že se oční sítnice nachází uvnitř oka, je chráněná vůči vnějším vlivům, a díky tomu je vzor cév za sítnicí téměř neměnný. Z technického hlediska se pro potřebu biometrických systémů založených na snímání oční sítnice používají speciální optické kamery, které pro osvětlení sítnice využívají infračervené světlo. Pro světlo této vlnové délky je sítnice průhledná a není tedy možné získat snímek sítnice. Po prvotním průchodu světla do oka a jeho následném odrazu od sítě cév, který leží za sítnicí, se nám vytvoří snímek sítnice, který můžeme využít pro identifikaci. Výhodou identifikace pomocí oční sítnice je vysoká přesnost, rychlost, vysoká bezpečnost a nemožnost obelstění systému. Obtížnost vytvořit kopii oka, která by funkčně napodobovala odrazivost sítnice, zaostřování čočky, apod. Nevýhodou je malá uživatelská příjemnost. I když snímání není vyloženě nepříjemné, pro správnou identifikaci je nutné vydržet bez pohybu cca 10 až 15 sekund, což činí snímání méně příjemným. Dále je tu nemožnost použití této technologie ve vnějším prostředí. Systémy mají jednak malou velikost čočky a jednak je venku příliš mnoho světla, které ovlivňuje získaný snímek. Dále

[4] Nystagmus – oční vada, která způsobuje nekontrolované, rychlé a trhavé pohyby očí.

[5] Aniridia – jedná se o oční vadu, při které částečně nebo úplně chybí duhovka.

je tu nemožnost použití brýlí, kdy s tímhle mají problém hlavně lidé se silným astigmatismem[6] a nakonec je to vysoká cena snímačů. [1][2]



Obr. 9 Snímaná část cév v choroidu [2]

Na obrázku sítnice oka (Obr. 9) jsou šedé křivky vzor cév v choroidu, světlý bod označuje slepou skvrnu. Tento bod je optický nerv, který vede do sítnice. Přerušovaný kruh označuje oblast, která má být snímána.

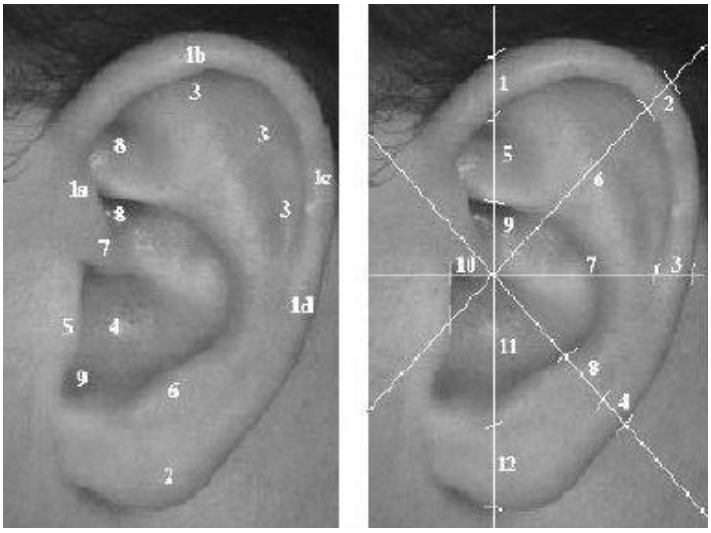
4.1.3 Tvar vnějšího ucha

Jedná se o jednu z nejmladších identifikačních metod, která se začala používat teprve před několika lety. Otisky uší se začaly objevovat na několika místech trestných činů v Evropě a Spojených státech amerických. Tyto otisky zaujaly jak policii, tak i vyšetřující orgány, které se začaly těmito otisky zabývat, a tím začaly být významnou identifikační metodou v bezpečnostních sborech. [2]

Kromě toho, že otisk ucha lze využít pro policejní vyšetřování, lze jeho vlastnosti použít i pro přístupové a identifikační systémy. Porovnání se provádí na základě komplexní struktury ucha. Růst ucha probíhá v prvních 4 měsících, potom se jen zvětšují proporce, což značí invarianci tvaru ucha během života a možnost jeho využití jako biometrické vlastnosti. Tento způsob je i uživatelsky příjemný, protože je možné získat snímek ucha na dálku a jsou zde tedy dobré předpoklady k akceptovatelnosti uživateli. [1]

[6] Astigmatismus – refrakční vada, která způsobuje nepřesné zaostření světla na sítnici.

V biometrických systémech pro rozpoznávání lidského ucha lze použít několik metod. Termogram ucha, grafový model ucha založený na diagramu Voronoi, PCA metoda, 3D tvar ucha, Iannarellisův systém.



Obr. 10 Iannarellisův systém snímání tvaru vnějšího ucha [1]

Iannarellisův systém

Iannarellisův systém o nejběžněji používaný antropometrický systém (Obr. 10), který se používá pro snímání ucha. Tento systém používá pro svoji práci 12 rozměrů ucha. Aby tento systém spolehlivě fungoval, je potřeba, aby došlo k zarovnání a normalizaci obou dvou uší. Tyto rozměry ucha jsou ještě dále doplněny o podpůrné rozlišovací znaky, jako je informace o pohlaví a rase. Výhodou identifikace pomocí tvaru vnějšího ucha nutnost fyzického kontaktu uživatele, naopak nevýhodou je nízká rozlišovací schopnost. [1]

4.1.4 Hlas a řeč

Další relativně mladou metodou je rozpoznávání jedinců podle hlasu a řeči. Technologie rozpoznávání hlasu je založena na odlišnostech vokálního traktu osob. Tvar a rezonance ústní dutiny, hlasivek, jazyka a zubů dokážou jednoznačně zformovat náš biometrický otisk hlasu. Tato mladá disciplína dříve nazývaná *fonoskopie* a nyní jako *audioexpertíza* se v současné době celkem rychle rozvíjí. Předmětem zkoumání je zde lidská řeč a hlas, jejichž cílem je rozpoznat hlas „anonymního“ řečníka od řečníka, jehož totožnost (záznam hlasu) známe. Občas se audioexpertíza používá pro policejní případy, kdy je podle telefonátu nebo jiné nahrávky potřeba určit identitu člověka, jehož hlas je zde zaznamenán. V dnešní době je možné používat řeč a hlas pro potřeby kriminalistického a soudního

rozpoznávání díky rozvoji fonetických věd. V tomto případě jde o *forenzní fonetiku*. Dále je zde využito i znalostí a instrumentálních prostředků jiných disciplín (akustika, audiotechnika, apod.). [2][5]

Pro účely biometrických systémů je nejprve nutná registrace, kdy uživatel vytvoří svoji šablonu, tedy svoji hlasovou stopu, která je následně uložena do databáze. Pro zvýšení bezpečnosti je lepší používat delší věty než krátká slova. Při identifikaci je uživatel vyzván k vyslovení svojí věty. Pro ještě větší zvýšení bezpečnosti je dobré, když uživatel má v systému uložených hned několik delších nebo kratších vět a systém si následně z těchto vět vybere jednu pro identifikaci.

V biometrických systémech založených na hlasu a řeči se využívá rozpoznávání a ověřování hlasu, což jsou dva úplně jiné přístupy. Při rozpoznávání hlasu je nejprve vysloveno slovo, které je následně vyhledáno v databázi a potom se rozhodne, které slovo odpovídá dané výslovnosti. Kdežto u ověřování hlasu je uživatelem vyslovená fráze porovnávána s již předem uloženou registrační šablonou v databázi a systém určí míru shody vzorku a šablony. Výhodou těchto systémů je uživatelská přívětivost pro uživatele a možnost snímání hlasu na dálku. Nevýhodou, že v místech s vysokou hlučnosti jsou tyto systémy nepoužitelné. Dále může při identifikaci vzniknout problém s momentálním fyzickým a psychickým stavem uživatelů. [5]

4.1.5 Otisky prstů

Otisky prstů jsou asi nejznámější a nejrozšířenější biometrickou technologií ze všech. Otisků prstů se hojně využívá jak policejně-soudní sféře, tak i v bezpečnostně-komerční. V policejně-soudní sféře se otisky využívají především pro identifikaci pachatele nějakého zločinu, který neúmyslně takový otisk zanechal na místě činu, tzv. daktyloskopie. V bezpečnostně-komerční sféře se otisky také využívají pro identifikaci a verifikaci, ale zde např. pro povolené vpuštění do střeženého objektu.

Otisky má každý jedinec na povrchu svých rukou (i nohou). Pro otisky prstů můžeme použít také pojem papilární linie. Ty jsou pro každého člověka jedinečné a lze na jejich základě rozeznávat jedince mezi sebou navzájem. Papilární linie jsou skladba struktur na povrchu prstu, které jednoznačně určují identitu člověka. Tyto linie se u člověka začínají tvořit už v embryonální fázi. Po jejich vzniku na povrchu kůže už zůstávají stejné a jsou neměnné s časem. Papilární linie se nachází jen na některých částech povrchu

lidského těla. Můžeme je najít na vnitřní straně prstů a dlaní obou rukou a na prstech a dlaních na obou nohách, nikde jinde se nevyskytují. [4]

Tab. 2 Markanty otisků prstů [23]

RIDGE ENDING UKONČENÍ	BRIDGE MOST
BIFURCATION VIDLICE	DOUBLE BIFURCAT. DVOJITÁ VIDLICE
DOT BOD	TRIFURCATION TROJVIDLICE
ISLAND OSTROV	OPPOSED BIFICURAT. PROTILEHLÁ VIDLICE
LAKE OKO	RIDGE CROSSING KŘÍŽENÉ UKONČENÍ
HOOK HÁK	OPPOSED BIFICURAT./ RIDGE ENDING

Papilární linie jsou vyvýšené části pokožky tzv. markanty (Tab. 2), které dosahují výšky cca 0,1 – 0,4 mm a šířky cca 0,2 – 0,7 mm. Všechny tyto vyvýšené části pokožky (jejich umístěním, množstvím, vzájemnou kombinací) společně vytvářejí daktyloskopické obrazce, které dávají unikátnost každému otisku a tím slouží pro daktyloskopickou identifikaci. Výhodou této technologie je uživatelská přívětivost pro uživatele, velká nabídka snímačů, malé rozměry, energetická nenáročnost apod. Nevýhodou je, že jestli se u identifikace neprovádí kontrola živosti, jsou tyto systémy lehce oklamatelné, je snadné získat otisky uživatele bez jeho vědomí a pro lidi s kožními problémy je identifikace velmi obtížná nebo někdy úplně nemožná. [1][2][4]

Obr. 11 Hlavní vzory seskupení papilárních linií [24]

Otisky prstů lze rozdělit do třech základních vzorů (Obr. 11) oblouk, smyčka a vír. Je známo, že 60-70 % všech nalezených otisků obsahuje smyčku, 25-35 % otisků obsahuje vír a oblouk obsahuje cca 5 % otisků prstů.

4.1.6 Vroubkování nehtu

Velmi vzácně používaná biometrická metoda, která je založena na snímání povrchu nehtu. Povrch nehtu je pokryt vroubkováním, u kterého má každý jedinec odlišný tvar. Tvar vroubkování na povrchu nehtu je dán tvarem lůžka, které nehet kopíruje. Snímání tvaru nehtu připomíná čárový kód. Snímání je umožněno díky keratinu (přírodní polymer), který je obsažen mezi nehtem a lůžkem pod ním. Tento polymer dokáže měnit orientaci polarizovaného světla, kdy při osvícení a správným úhlem, lze analyzovat fázové změny paprsku po odrazu. [5]

Nehet lze rozdělit do 6 základních částí. Na kořen nehtu (hlavní místo růstu nehtu), lůžko nehtu, nehtová ploténka, eponychium[7], nehtový val, sterilní matrix. Existují dvě technologie, které využívají pro svoji práci nehet. Jedná se o snímání struktury nehtového lůžka a zápis/čtení z nebo na nehet. Výhodou u této technologie je uživatelská přívětivost pro uživatele a vhodnost jako doplněk pro systémy na snímání otisků prstů. Nevýhodou je náchylnost na poškození nehtu a téměř nulové využití na rozdíl od jiných metod. [1]

4.1.7 Snímání krevního řečiště ruky

O problematice snímání krevního řečiště ruky je dále pojednáno v kapitole 4.5.

4.1.8 Geometrie ruky

Technologie pro rozpoznávání geometrie ruky existují ve dvou verzích a to ve verzi 2D a 3D. Technologie na rozpoznávání geometrie ruky patří mezi středně rozšířené bezpečnostní systémy. Oblíbenost 2D metody zaznamenala zvýšený zájem o tuto technologii a to převážně do provozů, kde nelze z nějakého důvodu použít jiné biometrické systémy. Kdežto 3D metoda je stále spíš ve vývoji a ještě bude chvíli trvat, než bude možné tuhle technologii použít v praxi. Při zavedení 3D technologie se zvětší i celková bezpečnost těchto metod. To je dáno tím, že na 3D snímku lze zachytit mnohem větší

[7] Eponychium – ztenčený okraj kůže zasahující přes nehet.

množství biometrické entropie geometrie ruky. Geometrie ruky se používá pro přístupové biometrické systémy z důvodu tvrzení, že lidská ruka je jedinečná, kdy tato jedinečnost má být zajištěna několika charakteristikami ruky. Jedná se o délku prstu, šířku prstu, výšku prstu, zakřivení a lokální anomálie. [1][2]

Systémy (2D) pro snímání geometrie ruky pro svoji práci používají běžné kamery, na které nejsou kladeny žádné specifické požadavky. Nejsou užívané ani barevné kamery, protože barevný snímek nám nepodá žádné nové informace, a proto si systém vystačí jen s černobílou kamerou. Tyto kamery jsou ve většině případů doplněny o zdroj světla, aby byl výsledný snímek co nejvěrohodnější a nebyl pokažen špatným světelnými podmínkami. Využívá se běžného viditelného spektra nebo infračerveného spektra. Existují ale i systémy, které žádné umělé osvětlení neobsahují a spoléhají se jen na světlo z okolního prostředí. Většina dnešních systémů používá pro rozpoznávání pouze siluety ruky shora a zespodu, ale některé z nich umožňují vytvářet i „třetí rozměr“ za pomocí zrcadla.

Výhodou je komfort uživatele, odolnost proti nečistotám, možnost použití metody i při vzniku škrábanců nebo jizev, malá náročnost na paměťovou kapacitu a operační výkon. Naopak nevýhodou je, že při vzniku např. zlomeniny prstu a následného špatného srůstu, může být prst trochu zkřivený, což tyto biometrické systémy netolerují. Dále se tyto systémy pro nízkou přesnost hodí spíš pro verifikaci, nikoliv už identifikaci. Dále je nutné u těchto systému sundávat různé šperky (např. prsteny) a lidé s artritidou nebo Parkinsonovou chorobou můžou mít problém korektně vložit ruku mezi distanční kolíčky. [1][5]

Metody rozpoznávání podle geometrie ruky:

- metoda založená na přímých měřeních,
- metoda založená na zarovnání rukou,
- metoda založená na analýze šířky prstů,
- metoda založená na 3D geometrii ruky. [5]

4.1.9 Podpis a písmo

Behaviorální biometrická metoda, která slouží k rozpoznání neprávoplatného uživatele, pokoušejícího se falzifikovat podpis. Tato metoda se používá převážně při rozpoznávání podpisu při verifikaci osob. Identifikace je též možná, ale v současnosti se této možnosti

moc nevyužívá a nemá velké uplatnění. Rozpoznávání podle písma a podpisu může být považováno za částečně statickou a částečně dynamickou biometrickou metodu. Statická metoda zaznamenává a uchovává pouze konečný výsledek podpisu, kdežto dynamická metoda zaznamenává i průběh celého psaní. Pro využití této metody je potřeba tablet a speciální aktivní pero k podpisu, které ukládá veškeré potřebné parametry průběhu psaní. Výhodou je rychlost získávání vzorku (u fráze je to 5 sekund, u náčrtu jsou to 2 sekundy), kdy vzorek u fráze obsahuje vysoký stupeň individuálních vlastností, které jsou stabilní a snadno reprodukovatelné a vzorek u náčrtu je zase anonymní na rozdíl u podpisu. Nevýhodou je, že fráze je závislá na stylu písma a celkovém fyzickém a psychickém stavu a u náčrtu musí při verifikaci obrázek kreslen co nejpřesněji stejnými tahy jako u vzoru. Podpis a písmo je velmi známá a stará metoda identifikace osob. V dnešní době můžeme obě metody (statická, dynamická) dále rozdělit na:

- *rozpoznávání písma* – jedná se o rozdělení písmen do jednotlivých tříd, vytváření vět z obrazového podkladu a rozpoznávání smyslu psaného textu,
- *rozpoznávání podpisu* – každý podpis má své jedinečné charakteristické vlastnosti, na kterých tato metoda rozpoznávání spočívá, a to bez ohledu, jestli se jedná o statické nebo dynamické vlastnosti.

Tyto systémy pro svoji funkci (verifikaci) vyžadují zadání určitého ručně napsaného vzoru, který následně slouží pro zjištění individuálních charakteristik uživatele. Ruční zadání do systému lze rozdělit:

- *verifikace pomocí fráze* – metoda vyžaduje zadání určitého úryvku textu, který je následně vyhodnocen,
- *verifikace pomocí náčrtu* – metoda vyžaduje nakreslení určitého jednoduchého obrázku.

4.1.10 Dynamika stisku počítačových kláves

Dynamika stisku počítačových kláves je biometrická metoda pro verifikaci uživatele. Tato metoda patří do behaviorálních charakteristik člověka. Nejčastěji ji spojujeme s počítačovou technikou a hlavně s počítačovými klávesnicemi, kde pomocí klávesnice a speciálního SW dochází k automatické verifikaci uživatele. Jak bylo už napsáno, jedná se o behaviorální charakteristiku, která může být do jisté míry ovlivněna fyzickým a psychickým stavem uživatele, což v případě tohoto systémů nemusí být až zas takový

problém jako u jiných biometrických systémů založených na behaviorálních charakteristikách, jako je např. snímání hlasu. [2][5]

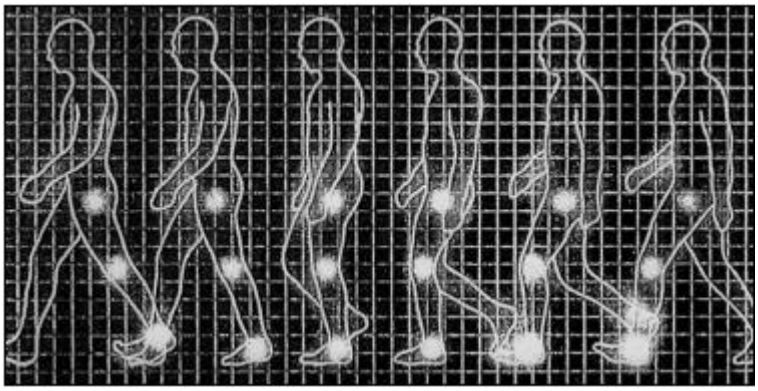
Pro potřeby systému je potřeba znát hned několik jedinečných vlastností a informací, které jsou zde použity pro vytvoření charakteristického profilu uživatele. Informace od uživatele se získávají při psaní na klávesnici na úrovni operačního systému (dále jen OS), protože právě OS umožňuje zachytit stisk klávesy a opět její uvolnění. Právě stisk a uvolnění kláves jsou hlavní charakteristikou, která poskytuje dvě hodnoty, ze kterých lze vypočítat dobu trvání stisku dané klávesnice. [2] Kromě této charakteristiky, lze používat i jiné přístupy:

- *rychlost psaní* – každý jedinec má určitou frekvenci psaní, takže je možné snímat počet stisků kláves za určitý časový interval,
- *frekvence chyb* – při psaní dostatečně dlouhého textu každý jedinec udělá v textu chybu, která je potom nucen smazat klávesnicí *Backspace*. Právě počet zmáčknutí klávesy *Backspace* se zaznamenává a sleduje se tento jev pro výpočet celkové frekvence chyb,
- *styl psaní velkých písmen* – založeno na principu, zda uživatel při psaní velkých písmen nejprve uvolňuje *Shift* anebo klávesu se znakem,
- *síla použitá při stisku kláves* – pro tento způsob je potřeba speciální klávesnice, která měří sílu stlačení. U této metody záleží, kde se jaká klávesnice nachází a jaký prst danou klávesnici zmáčkne. Všechno tohle ovlivňuje následné zmáčknutí a vyhodnocení tlaku na klávesnici. [2]

4.1.11 Bipedální lokomoce

Bipedální lokomoce neboli schopnost pohybu na dvou nohách, jednoduše chůze. Je druh mechanického pohybu, jenž pro svoji funkci využívá dolních končetin, které umožňují přesun mezi místy. Bipedální lokomoce (Obr. 12) je vlastní všem dvounohým živočichům včetně člověka, kteří pro pohyb z místa na místo používají dolní končetiny, které se rytmicky střídají mezi sebou, čímž vznikají jednotlivé kroky a tím dochází k pohybu. Pro chůzi po dvou nohách je charakteristické, že každý jednotlivý krok má svůj okamžik. Situace, kdy jsou obě nohy v klidu a spočívají na zemi, se nazývá oboustranná opora, kdežto když váha těla spočívá na jedné noze a druhá noha je v pohybu, tuto situaci označujeme jako jednostranná opora. [22]

Cílem technologie založené na snímání pohybu člověka je rozpoznat osobu na základě vlastností její chůze, pokud možno v co nejširším spektru prováděných a přirozených situacích. Osoby pomocí této technologie lze snímat i na větší vzdálenost a to za pomocí běžných kamer. Problémem této technologie jsou horší rozlišovací schopnosti mezi jednotlivými uživateli. Problém s rozlišením uživatelů se řešil tak, že se používaly speciální značky na oblečení, které měly pomoci k lepší identifikaci. Průběh samotného rozpoznání jedince je závislý na několika faktorech. Příkladem může být použití rozličného oblečení, bot nebo také zdravotní stav (nemoc, zranění, úrazy, apod.) nebo i psychický stav uživatele.



Obr. 12 Zobrazení lidské chůze [22]

Dále může být limitující i vliv okolního prostředí (množství okolo proudících lidí, osvětlení místnosti nebo venkovního okolí, apod.). Všechny tyto faktory můžou ovlivnit rozlišovací schopnosti biometrického systému a tento uživatel nemusí být identifikován a následně např. vpuštěn do objektu. Výhodou u bipedální lokomoce je možnost snímat pohyb na dálku, čímž je takový systém pro uživatele příjemný a lze použít běžně dostupné a levnější kamery. Nevýhodou je nízké rozpoznání jednotlivých uživatelů. [22]

4.1.12 DNA

Pro potřeby identifikace se DNA začalo v biometrice prosazovat na základě toho, že DNA obsahuje jednotlivé úseky, které jsou pro každého jedince originální a jedinečné. **DNA - Deoxyribonucleic Acid** (deoxyribonukleová kyselina) je nosičem genetické informace. DNA patří do skupiny tzv. nukleových kyselin, kam patří ještě **RNA – Ribonucleic Acid** (ribonukleová kyselina). V molekulách těchto kyselin se nachází všechny informace o stavbě a mechanismu fungování těla. U obou nukleových kyselin jsou základním stavebním kamenem nukleotidy. Tyto nukleotidy se dělí na pět typů. Jedná se o **adenin, guanin, cytosin** (zkráceně **A, G, C**), které jsou společné pro obě nukleové

kyseliny DNA i RNA. Potom je zde **thymin (T)**, který (kromě A, G, C) je navíc u DNA a **uracil (U)**, který (kromě A, G, C) je navíc u RNA. [1][5]

Pro použití v jednotlivých typech identifikací je DNA v praxi použitelná jen u policejně-soudní identifikace. DNA je spolu s otisky prstů nejpoužívanější metodou identifikace v kriminalistice. Naopak v bezpečnostně-komerční identifikaci pro přístupové systémy není praktické využití této technologie. Největším problémem biometrických zařízení založené na DNA je uživatelská přívětivost, protože neexistuje způsob odběru DNA bez toho, aniž by se musel uživatel dotýkat nebo dokonce, aby musela být nějak narušena lidská pokožka nějakým vpichem. Dalším problémem v použití těchto systémů by byla časová náročnost. I když časová náročnost v dnešní době klesla z dříve uváděných několika hodin na dnešní průměr cca desítek minut, stále se jedná o časovou náročnost, která je v biometrických přístupových systémech nepřípustná. Výhodami u identifikace přes DNA jsou jedinečnost pro každého jedince, možnost získání DNA z každé buňky v těle, využití ve forenzní medicíně a jeho neměnnost během života. Nevýhody mohou zahrnovat nedostatečnou kompletní automatizaci procesů, pomalost vyhodnocení vzorku a cenová náročnost DNA obsahuje cenné informace o nositeli (rasa, zdravotní stav, atd.), které při získání cizí osobou mohou být zneužity. [1][17]

4.1.13 Snímání pachu

Metoda snímání pachu není příliš známá biometrická technika, protože je tato metoda stále ve vývoji a neexistují žádné komerční prostředky, které by tuto lidskou vlastnost pro identifikaci využívaly. Naopak v policejně-soudní identifikaci má tato metoda svoje místo a využití. V dnešní době se v kriminalistické praxi hojně využívají čichové smysly psů. K tomuhle se nedají využít žádné senzory, protože neexistují dostatečně přesné senzory, které by umožňovaly porovnávat a správně vyhodnocovat víc než jednu pachovou stopu zároveň, protože se lidský pach skládá z cca 30 chemických sloučenin. Intenzita nebo absence těchto sloučenin spolu dohromady vytvářejí jedinečnou pachovou stopu člověka, kdy může být tato pachová stopa ještě ovlivněna různými faktory, jako je emocionální nebo hormonální stav člověka. První vývojové verze systémů založených na funkci snímání pachu se snaží o co nejrealističtější napodobení lidského čichu. Při tvorbě těchto systémů je nutné, aby byly co nejpřesnější, protože nelze vymezit přesné prostory sledování pro zjišťování pachů. [1]

4.1.14 Další identifikační metody

Zde jsou uvedeny jedny z nejméně známých nebo experimentálních metod používaných k identifikaci, kdy některé z nich nemusejí být běžně dostupné nebo komerčně využívané. Některé z těchto metod se používají převážně v policejně-soudních aplikacích, jiné zase v bezpečnostně-komerčních aplikacích. Byla zde zařazena odontologie, snímání pohybu rtů, dynamika pohybu myši, absorpční spektrum lidské kůže, obsah solí v lidském těle a póry.

Odontologie

Soudní odontologie je vědní obor, který se zabývá zkoumáním a vyhodnocováním soudních dentálních důkazů. Tyto důkazy můžou sloužit pro identifikaci člověka na základě jeho chrupu. Tato metoda se používá převážně, když je lidské tělo v pokročilé fázi rozkladu nebo došlo k jeho znetvoření (po silném nárazu, po spáleninách, apod.), že nelze tělo běžně identifikovat. Dále je možné využít lidský chrup pro analýzu otisků zubů po kousnutí. [1]

Pohyb rtů

Jedná se o biometrický systém založený na rozpoznávání pohybů rtů u člověka. Porovnání pohybu rtů se provádí během pohovoru nebo při vyřčení předdefinovaného textu. Často se používá v kombinaci se systémy na snímání hlasu a řeči. Tento typ systému využívá pro svoji funkci dvě možnosti osvětlení a snímání. Obě možnosti jsou založeny na osvětlení rtů. Jedná se metodu FIR (Far-InfraRed) a NIR (Near-InfraRed). První z nich je velmi bezpečná, ale i velmi nákladná na zakoupení a provoz, druhá je levnější, ale za to je méně bezpečná. [1]

Dynamika pohybu počítačové myši

Dynamika pohybu počítačové myši je biometrická metoda, která využívá pro svoji funkci všechny provedené pohyby myší. Všechny tyto pohyby jsou zaznamenány a převedeny na data, ze kterých je následně zpracována unikátní charakteristika uživatele. Pro použití

této metody lze použít běžnou myš nebo touchpad[8], takže není potřeba žádný speciální hardware. [26] Akce s myší, lze rozdělit do 4 kategorií:

- *pohyb myší* – myší je pohybováno po stole nebo podložce,
- *drag and drop* – u myši je nejprve stlačeno tlačítko a poté následuje pohyb a nakonec dojde opět na uvolnění tlačítka myši,
- *point and click* – myší je pohybováno a následně poté následuje klik nebo dvojklik myší,
- *klid* – nedochází k manipulaci s myší. [27]

Absorpční spektrum lidské kůže

Podobně jako se povrch lidské kůže liší na pohled, liší se i vnitřní struktura pod povrchem kůže. Lidská kůže má několik vrstev, které se liší svojí tloušťkou. Uvnitř jednotlivých vrstev je i rozdílný tvar buněk a jejich hustota. Při použití čtecího zařízení se kůže ozařuje různými vlnovými délkami a jejich následný odraz je následně analyzován. [5]

Otisky pórů (Poroskopie)

Kromě známější metody snímání otisků prstů za účelem identifikace lze použít snímání otisků pórů. Tato metoda identifikace odborně nazývána poroskopie slouží pro identifikaci osoby a její totožnosti na základě otisků prstů, které se vyskytují v otiscích prstů. V této metodě se na otisku posuzuje tvar póru, velikost, plocha vůči ose souměrnosti papilárních linií, vzdálenost mezi papilárními liniemi a jiné rozdílnosti. [25]

4.2 Kritéria pro biometrické systémy

Biometrické identifikační systémy potřebují pro svoji funkčnost anatomicko-fyziologické nebo behaviorální charakteristiky člověka. Problémem ale je, že lidské tělo podléhá změnám a ne všechny lidské charakteristiky zůstávají v průběhu času stálé a neměnné. Jedná se tedy o kritéria biologických charakteristik člověka. Dalšími parametry pro samotnou funkčnost biometrických identifikačních a verifikačních systémů i pro jejich efektivnost a celkovou úspěšnost jsou operační, technická, finanční a výrobní kritéria.

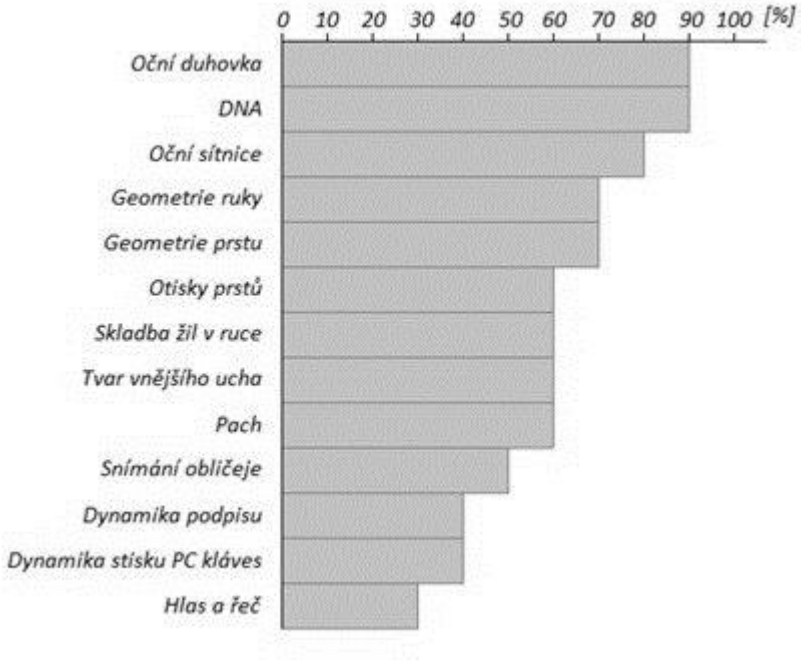
[8] Touchpad - vstupní zařízení běžně používané u notebooků. Jeho účelem je pohybovat kurzorem po obrazovce podle pohybů uživatelova prstu. Jde o náhradu za počítačovou myš.

4.2.1 Kritéria biometrických charakteristik uživatelů

Kritéria biologických charakteristik člověka jsou důležitou součástí pro použití a celkovou funkčnost biometrických systémů. Některé lidské biologické charakteristiky se během života mění více (např. hlas), některé méně (oční duhovka). S tímto se musí u biometrických systémů počítat, protože se tyto charakteristiky zaznamenávají v nějakém stádiu a uloží se do databáze, proto je nutné tyto informace v databázi udržovat co nejvíce aktuální. Biometrické vlastnosti nemusejí a nebývají ovlivněné jenom procesem stárnutí těla, ale může se jednat i o celkové opotřebení tkáně, změna biometrických vlastností způsobené úrazem (např. pořezané prsty, kdy už nejdou rozeznat otisky prstů), může jednat i o špínu a nečistoty nebo nemožnost určitého typů lidí používat určitý systém. Při výběru biometrického systému je tedy nutné počítat s těmito změnami a lidské tělo uživatele musí splňovat následující kritéria:

- *jedinečnost* – jedná se o podmínku, bez které by nemohly systémy vůbec fungovat. Jde o jedinečné vlastnosti, které má každý člověk jiné a nikdy se nevyskytují u dvou nebo více lidí stejné hodnoty a právě na těchto hodnotách jsou biometrické systémy založeny,
- *neměnnost* – pro potřeby biometrických systémů se používají lidské vlastnosti, které jsou co nejméně neměnné v čase a které budou měřitelné i po čase,
- *univerzálnost* – jedná se o vlastnosti, které musí být přítomny u velkého počtu lidí, aby bylo možné ve větší míře použít tyto vlastnosti v biometrických systémech,
- *měřitelnost* – musí se jednat o vlastnosti, které jsou měřitelné za použití stejných technických prostředků,
- *uživatelská přijatelnost* – biometrické systémy musí být při použití uživatelsky příjemné a nesmí uživatele odrazovat od jejich použití. Třeba u biometrického systému pro snímání oční sítnice se někteří uživatelé bojí tyto čtečky používat, protože se obávají poranění oka, naopak např. systémy pro snímání obličeje jsou pro uživatele velmi příjemné, neboť ke snímání dochází na dálku a není potřeba žádného styku s přístrojem. Osoba při použití nesmí pociťovat diskriminaci v souvislosti s barvou pleti, věkem, profesí, fyzickým, anatomicko-fyziologickým nebo psychickým stavem uživatele, apod. [2][13]

U lidského těla dochází k mnoha změnám, kdy jsou některé vlastnosti závislé na stálosti v čase méně a některé více. Nejvíce času odolávají vlastnosti oční duhovky a DNA, kdy nedochází téměř k žádným změnám, a když nějaká změna nastane, tak to nemá vliv pro použití v biometrických systémech. Naopak charakteristika lidského hlasu se hodně mění v průběhu života, hlavně tedy v období puberty. Nejméně ovlivnitelné biometrické vlastnosti jsou zobrazeny na obrázku (Obr. 13). Čím vyšší hodnota, tím větší odolnost a trvanlivost vůči času. [2][13]



Obr. 13 Stálost biometrických vlastností v čase [29]

4.2.2 Kritéria biometrických systémů

Stejně jako lidské tělo musí splňovat určité podmínky pro použití v biometrických systémech, musí i samotné biometrické systémy splňovat určité podmínky, aby byly v praxi co nejefektivnější.

Operační kritéria

Každý biometrický systém musí splňovat několik operačních kritérii, jako je uchovatelnost, spolehlivost, exkluzivita a praktičnost.

- *Uchovatelnost* – všechny získané a naměřené identifikační charakteristiky a údaje se musí zálohovat a musí být k dispozici po několik let. Uschovávání identifikačních materiálů musí být finančně nenáročné, ale při tom musí být zabráněno poškození nebo zhoršení jejich kvality,

- *spolehlivost* – proces měření, zpracování, ukládání, vyhodnocování a jiná manipulace s biometrickými charakteristikami musí být dostatečně spolehlivý a kdykoliv zopakovatelný se stejnými výsledky,
- *exkluzivita* – použitý identifikační biometrický systém musí být dostatečný pro identifikaci, aby nemusel být doplněný o jiný podpůrný biometrický systém,
- *praktičnost* – použitá metoda musí být praktická a jednoduchá na použití. Uživatel by měl být co nejméně v kontaktu se zařízením. Průběh snímání by měl být co nejrychlejší a uživatel by měl provádět co nejméně úkonů, které by se nemusel dopředu nijak učit nebo je trénovat. [2]

Technická kritéria

Každý systém by měl splňovat nějaká technická kritéria. Mezi ně patří minimální časové zpracování a vyhodnocení, přijatelná chybovost (která neovlivní bezpečnost systému), flexibilita, odolnost (vůči vnitřním a vnějším vlivům, ale v menší míře i proti vandalismu), efektivnost, výkonnost (nesmí se projevovat nedostatek operačního výkonu a systém musí např. stihnout obsloužit určité množství lidí za určitý čas), standardizace (kompatibilita), skladovatelnost identifikačních charakteristik, kapacita úložného prostoru, přesnost, jednoduchost, rychlost (v rámci sekund). [2]

Finanční kritéria

Dalším velmi důležitým kritériem je kritérium finanční, které má mnohdy rozhodující roli při výběru systému. Při pořizování biometrického systému se musí zájemce dívat i na cenu takového zařízení. Většina biometrických systémů ale není levnou záležitostí. Jejich cena se pohybuje od několika tisíc až po několik stovek tisíc korun. Kvůli finanční nákladnosti se biometrické technologie běžně nepoužívají u rodinných domů (ale mohou, když si zákazník zaplatí), ale většinou jde o velké soukromé objekty, jako jsou různé haly, hangáry, velké firmy, které potřebují chránit svoje know-how a majetek a jiné objekty, ve kterých bývá uchováván drahý majetek nebo mají chránit životy a kontrolovat lidi (muzea, banky, letiště, atd.). Finance se posuzují z krátkodobého i dlouhodobého pohledu. [2] Zohledňuje se:

- pořizovací cena, cena instalace, cena školení, tréninků,
- cena upgradů, nových modifikací,
- cena návazných systémů (fyzická ostraha, aj.).

Výrobní kritéria

Jedná se o kvalitativní zpracování systému, kvalitu dodavatele, výrobce, schopnost efektivní a cenově přijatelné podpory při provozu zařízení ze strany výrobce nebo dodavatele, dále kompatibilita s jinými zařízeními, reference atd. [2]

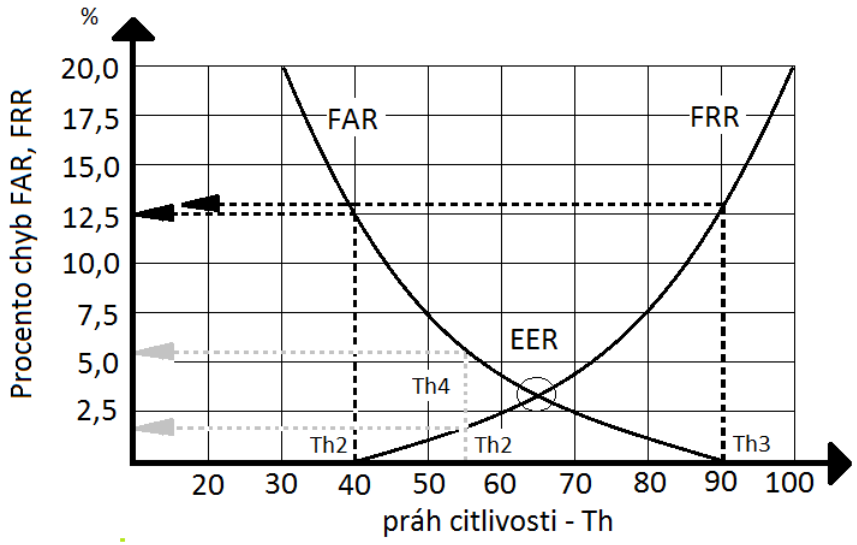
4.3 Spolehlivost biometrických systémů

Rok co rok na trh přibývají nová biometrická zařízení, spadající pod různá odvětví biometriky, takže je v dnešní době z čeho vybírat. Každý potenciální i skutečný uživatel, který se rozhodne ke koupi takového systému, si ale nejprve pokládá otázku, zda je takový typ systému spolehlivý a jaká je spolehlivost metody, se kterou tento systému pracuje. Takový systém by měl být vhodný do praxe, ale stejně tak dobře by měl skvěle fungovat v laboratorních podmínkách, v terénu a v každodenní praxi. Při pořizování kteréhokoliv bezpečnostního systémů existuje několik podmínek, kterými bychom se měli řídit. Za prvé je to výběr systému, který je založený na nějaké vhodné biometrické metodě (otisky prstů, snímání duhovky, snímání obličeje, atd.), který chceme každý den používat, kdy tento systém by nám měl vyhovovat a měli bychom k němu mít správné dispozice. Dále je nutné zvážit spoustu faktorů, které nám pomůžou vybrat ten správný systém, který nám nejvíce vyhovuje. Tyto faktory můžeme rozdělit na hlavní a vedlejší. Mezi hlavní kritéria můžeme zařadit spolehlivou identifikaci, verifikaci a mezi vedlejší lze zařadit cenu zařízení, uživatelskou přívětivost, odolnost vůči vnitřním a vnějším vlivům, rychlost zpracování údajů, vysokou kapacitu databáze apod. [2][11]

Mezi nejdůležitější kritérium patří schopnost systémů jednoznačně a bezchybně rozpoznat identitu právoplatného uživatele, který je oficiálně uložený v databázi systému a neznámé osoby. U takto aplikovaného systému může nastat občasná chyba ve spolehlivosti a systém nedokáže rozpoznat osobou s oprávněním, kterou následně odmítne vpustit do střeženého objektu, a naopak osobu, která není v systému, vpustí dovnitř. Hledání identity osoby uložené v databázi se děje na základě porovnání jednotlivých jedinečných charakteristik snímané osoby, jenž toto porovnání vyžaduje nebo se jej dobrovolně či povinně účastní. Porovnávají se aktuálně pořízené snímky s biometrickou charakteristikou ze systému a referenční údaje uložené v systému, které byly pořízeny již předem a které slouží jako vzor pro porovnání. Aby nedocházelo k problémům s rozpoznáváním jednotlivých osob při použití systému, používá se dvou základních metod:

- **FRR – False Rejection Rate** – (pravděpodobnost chybného odmítnutí) – někdy používaný také pojem **Type I Error Rate** (chyba I. typu),
- **FAR – False Acceptance Rate** (pravděpodobnost chybného přijetí) – někdy používaný také pojem **Type II Error Rate** (chyba II. typu). [2][11]

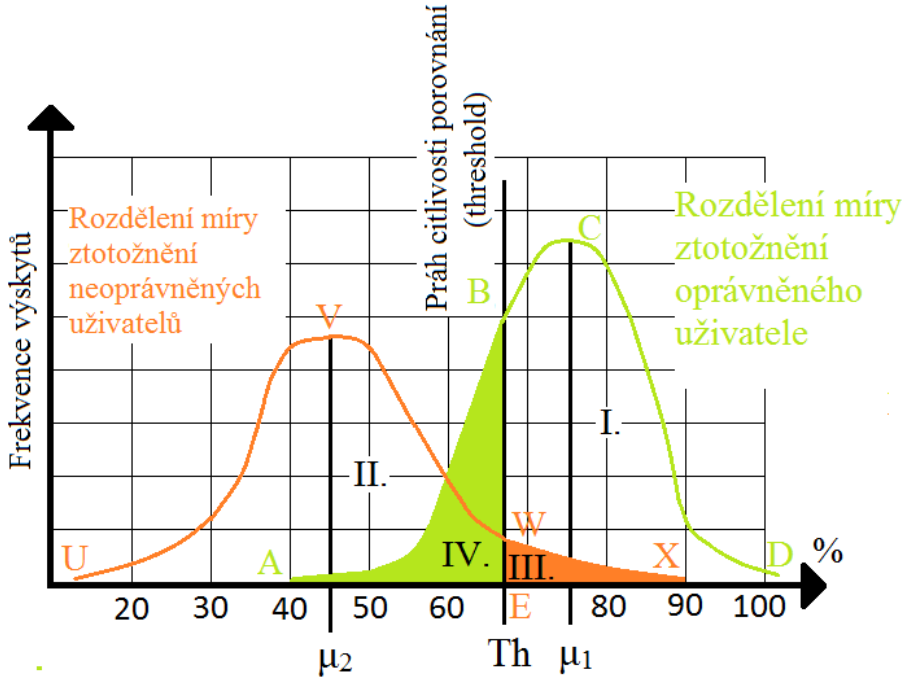
Míra chybného přijetí (FAR) a míra chybného odmítnutí (FRR) vyjadřují pravděpodobnost výskytu dané chyby v procentech. Z těchto chyb vyplývá, že čím vyšší je FRR, tím nižší je FAR a naopak. FRR i FAR jsou obě závislé (obr. 14) na prahové hodnotě (threshold), kterou si nastavíme. Nastavení prahové hodnoty závisí na způsobu použití systému v praxi, tzn., jestli větší problém je někoho chybně přijmout nebo chybně odmítnout. Když se hodnoty FRR a FAR rovnají, označuje se tahle rovnost jako **EER – Equal Error Rate** (míra rovné chyby). EER nám umožňuje určit přibližnou hodnotu bezpečnosti systému. Hodnoty FRR a FAR mají ale mají pořád vyšší odpovídající hodnotu. [5]



Obr. 14 Závislost FAR a FRR na Th [5]

Biometrické metody (identifikace, verifikace) jsou založeny na vyhodnocování podobnosti biometrického vzoru a šablony. Po každém snímání osoby jsou zaznamenané hodnoty a markanty zcela jiné. Z toho vyplývá, že míra ztotožnění je pokaždé jiná a závisí na každé biometrické aplikaci a jejím technickém řešení. Pro každé zařízení je potom možné graficky vyjádřit závislost četnosti míry ztotožnění osob, které se podrobují jednotlivým

metodám (identifikaci, verifikaci). Všechny tyto informace, lze následně zobrazit v histogramu (Obr. 15) pro dvě skupiny osob. [2]



Obr. 15 Histogram – rozdělení ztotožnění oprávněných a neoprávněných uživatelů [2]

Na histogramu je označena první křivka body A, B, C, D, které značí četnost výsledků porovnání jednoho a toho samého oprávněného uživatele, který se již mnohonásobně podrobil identifikačnímu a verifikačnímu procesu. Další křivka, která je označena body U, V, W, X značí pokusy, které mají na svědomí neoprávnění uživatelé, jejichž cílem bylo proniknout přes dané biometrické zařízení. Dále je na grafu vidět přímka EB, která je kolmá na osu x. Tahle přímka, kterou má každá pracovní aplikace, se nazývá práh citlivosti (Th - threshold) a společně s oběma křivkami (A, B, C, D a U, V, W, X) rozděluje plochu do čtyř oblastí, označené od I. do IV. Jestliže je výsledek porovnání vyšší než práh citlivosti, je potom následně oprávněný uživatel akceptován a vpuštěn, v opačném případě je odmítnut. Stejně tak to platí i u neoprávněné osoby. Pokud je výsledek porovnání vyšší, jsou tyto osoby akceptovány a pokud je nižší, jsou okamžitě zamítnuty. Rozhodnutí o tom, kdo je a kdo není oprávněný uživatel, rozhoduje míra ztotožnění biometrických vzorků. [2]

- **oblast I.** neboli **plocha** $\mathbf{P_{E,\ B,\ C,\ D,\ E}}$ označuje *korektní akceptaci oprávněného uživatele*, tzn., že uživatel je s aplikací spokojen a byl akceptován,

- **oblast II.** neboli **plocha $P_{U, V, W, E, U}$** označuje *korektní odmítnutí neoprávněného uživatele*, tzn., že neoprávněná osoba je nespokojená, protože se jí nepovedlo projít přes aplikaci,
- **oblast III.** neboli **plocha $P_{W, X, E, W}$** označuje *nekorektní akceptaci neoprávněného uživatele*, tzn., že neoprávněná osoba je spokojená, protože se jí podařilo projít přes aplikaci neoprávněně. Naopak nespokojený je správce aplikace, neboť došlo k proniknutí do střeženého objektu a vzniku bezpečnostního incidentu,
- **oblast IV.** neboli **plocha $P_{A, B, E, A}$** označuje *nekorektní odmítnutí oprávněného uživatele*, tzn., že uživatel není spokojen, protože i když je oprávněný uživatel, tak jej aplikace nerozpoznala a nevpustila dovnitř. [2]

Definice míry ztotožnění referenční šablony P‘ a načteného biometrického vzorku P:

$$s = Sim(P', P) \quad (1)$$

Práh citlivosti Th

Kvalita identifikace a verifikace je dána prahem citlivosti každé aplikace/zařízení. O vlastnostech identifikace/verifikace rozhoduje tedy použitá biometrická metoda a její technická realizace a všechny aspekty s nimi spojené. [2]

- jestliže je míra ztotožnění $s \leq Th$, pak se P = P‘. Osoba označená jako P je osoba s oprávněním pro vstup. Tomuto výroku je přiřazen stav H_0,
- stav H_1 je charakteristický pro nerovnost $s < Th$. Z toho vyplývá $P \neq P'$ a osoba je označena jako neoprávněná.

4.3.1 FRR (False Rejection Rate)

V překladu *pravděpodobnost chybného odmítnutí*, což je jedno z hlavních kritérií, jenž poukazuje na bezpečnost a uživatelskou spolehlivost. FRR nám udává, s jak velkou pravděpodobností bude zařízení chybovat a jestli nerozpozná oprávněného uživatele, jenž má v systému uloženou svoji šablonu. Na základě toho je uživatel odmítnut nebo vůbec nenalezen a je nucen se pokusit o prokázání svojí identity opětovně. [2]

Definice FRR: [2]

$$FRR = \frac{N_{FR}}{N_{EIA}} \text{ nebo } FRR = \frac{N_{FR}}{N_{EVA}} \quad (2)$$

N_{FR}……Number of False Rejection (počet chybných odmítnutí)

N_{EIA}……Number of Enrolle Identification Attemps (počet pokusů oprávněných osob o identifikaci)

N_{EVA}…… Number of Enrolle Verification Attemps (počet pokusů oprávněných osob o verifikaci)

Pomocí histogramu můžeme FRR definovat jako poměr dvou ploch:

$$FRR = \frac{P_{A,B,E,A}}{P_{A,B,C,D,A}} \quad (3)$$

FRR není z hlediska bezpečnosti nějak kriticky negativní jev. Chybné odmítnutí není v praxi vůbec vítaným jevem. Tento jev může být v malé míře tolerován, ale velmi časté výskyty tohoto typu problému u oprávněných uživatelů musí být včasně a rychle vyřešeny, neboť se jedná o jev, který je uživatelsky velmi nepříjemný a to potom následně snižuje „víru“ ve funkčnost takovéhoto systému a je přehnaně „tvrdý“ k uživatelům, kteří jsou regulérně v systému registrovaní. Naopak u policejně-soudních aplikací, může taková chyba zapříčinit propuštění pachatele z důvodu selhání techniky. Zde se jedná o velmi závažný nedostatek. [2]

4.3.2 FAR (False Acceptance Rate)

V překladu *pravděpodobnost chybného přijetí*, je druhé ještě možná důležitější kritérium v bezpečnosti biometrických systémů. FAR nám udává, s jak velkou pravděpodobností bude zařízení chybovat a jestli rozpozná neoprávněného uživatele, jenž není v systému vůbec zaveden a nemá svoji šablonu. Na základě toho může být neznámá osoba přijata a vpuštěna do střeženého objektu, kde nemá povolení se pohybovat. Tohle se nesmí stávat a takoví útočníci musí být nekompromisně biometrickými systémy odmítnuti. Existuje totiž spousta takových útoků na tato zařízení. Útočník se snaží získat cizí identitu a proniknout do objektu. [2]

Definice FAR:

$$FAR = \frac{N_{FA}}{N_{IIA}} \text{ nebo } FAR = \frac{N_{FA}}{N_{IVA}} \quad (4)$$

N_{FA}……Number of False Acceptance (počet chybných přijetí)

N_{IIA}……Number of Impostor Identification Attemps (počet pokusů neoprávněných osob o identifikaci)

N_{IVA}…… Number of Impostor Verification Attemps (počet pokusů neoprávněných osob o verifikaci)

Pomocí histogramu můžeme FAR definovat jako poměr dvou ploch:

$$FAR = \frac{P_{W,X,E,W}}{P_{U,V,X,U}} \quad (5)$$

V policejně-soudních aplikacích je falešné přijetí také velkým problémem. Příkladem může být osoba, která je neprávoplatně obviněna ze zločinu, kterou nespáchala. To se může stát, když má u takovéto osoby dojít k potvrzení identity a je chybně ztotožněna s úplně jinou osobou, tzn., že identita jedné osoby byla zaměněna za identitu jiné osoby, která už je např. trestně stíhána. Vyšetřování takového zločinu je potom vedeno špatným směrem. [2]

4.3.3 Přesnější výpočty chybovosti (FTE, FTA, FMR, FNMR)

Tyto přesnější výpočty slouží pro jemnější a detailnější přehled a rozdělení chybovosti biometrických zařízení. Výpočty chybovosti FAR a FRR vycházejí z předpokladu, že počty chyb i pokusů jednotlivých osob jsou vyrovnané. V případě, že to tak není, nejsou takto získané výsledky zcela nezaujaté. Jestliže tohle nastane, musíme postupovat tak, že spočítáme chybovost pro každou osobu zvlášť. [1]

FTE (Failure to Enroll)

Existuje spousta lidí, kteří se nemohou z nějakého důvodu (postižení) do zařízení registrovat nebo jen velmi obtížně. Příkladem můžou být nevidomí lidé, kteří mohou mít

problém s kontrolou otevřením očí nebo jedinci s chybějícím článkem prstu. Nemožnost zaregistrovat se do systému se nazývá Failure to Enroll. [1][2]

FTA (Failure to Acquire)

I když se podaří uživateli zaregistrovat do systému, může se stát, že získaná data nejsou v příliš vysoké kvalitě pro další použití a zpracování. V takovém případě je nutné data získat znovu a v lepší kvalitě než v předchozím pokusu, to nazýváme Failure to Acquire. [1][2]

FMR (False Match Rate) a FNMR (False Non-Match Rate)

Po získání dat v lepší kvalitě můžeme začít porovnávat vstupní data s již předem vytvořenou šablonou. Pokud dojde při srovnání k nesprávnému ztotožnění, nazýváme tuto situaci False Match Rate a pokud dojde k nesprávnému neztotožnění, nazýváme tuto situaci False Non-Match Rate. [1][2] V situaci, kdy povolíme pouze jediné získání biometrických dat, můžeme FAR a FRR vyjádřit:

$$FRR = FTE + FTA + FNMR \tag{6}$$

$$FAR = (1 - FTE) \cdot (1 - FTA) \cdot FMR \tag{7}$$

4.4 Využití biometrie v bezpečnostních aplikacích

Využití biometrických charakteristik člověka a bezpečnostních biometrických systémů je v praxi velmi široké. Tento obor a systémy vznikly převážně pro ochranu, kontrolu, usvědčování pachatelů, bezpečnostní aplikace atd. V bezpečnostně-komerčních aplikacích se může jednat o zabezpečení vstupů do objektů jako je banka, nemocnice, vojenských objektů a jiných budov, které vyžadují velmi vysokou úroveň bezpečnosti, dále k zjišťování identity při výběru u banky, na letišti nebo přístup k počítačové technice. Ještě než se začaly používat pro ochranu různých objektů, používaly se už dříve pro policejně-soudní aplikace.

4.4.1 Biometrie v policejně-soudních aplikacích

Biometrie se v policejně-soudních aplikacích začala používat už někdy v 19. století. Slouží hlavně pro usvědčování pachatelů v kriminalistice. Může se jednat o snímání otisků

z důkazních materiálů, sběr DNA na místě činu nebo zkoumání těla po úderu nějakým neznámým předmětem. Na rozdíl od biometrických systémů v bezpečnostně-komerčních aplikacích je nutný pro sběr a vyhodnocování biometrických informací přítomnost lidského faktoru. Pro kriminalistické účely lze z pohledu biometrických charakteristik člověka použít několik metod. [28] Patří sem:

- *daktyloskopická identifikace* – nejčastější využití biometrie člověka je u daktyloskopické identifikace, tedy hledání otisků prstů na místě činu, provádění identifikace osob, neznámých mrtvol a vzájemné porovnávání daktyloskopických otisků z dosud neobjasněných trestných činů,
- *trasologická identifikace* – tato metoda zkoumá stopy nohou (bosých i s obuví), stopy pneumatik, rukavic, stopy po přemístění předmětu a části lidského těla, které neobsahují papilární linie. Zkoumá se šířka, délka, hloubka, opotřebení, tvar stopy apod. S takto seřazenými stopami je možné vytvořit tzv. pěšinku chůze, ze které se dají zjistit informace o různých vadách a odchylkách při chůzi,
- *odorologie* – metoda, která slouží pro identifikaci pachatele a různých věcí podle jejich pachu. Pro identifikaci lidí se nejčastěji využívá lidský pot, který zanechává pachovou stopu,
- *grafologie* – biometrická metoda pro zkoumání ručního písma. Tato metoda je založena na faktu, že každá osoba má jedinečný podpis a neexistují na světě dva totožné podpisy (pravděpodobnost výskytu dvou stejných podpisů je cca 1 : 68 trilionům),
- *fonoskopie* – metoda zkoumající zvukové záznamy, převážně lidský hlas a řeč. Každý jedinec má svůj tzv. „otisk hlasu“, kterým lze každého jednoznačně identifikovat, i když je záznam hlasu různě rozrušený, upravený nebo pozměněný,
- *biologické zkoumání* – metoda se zabývá zkoumáním biologických stop, které se nacházejí na místě činu. Zkoumají se stopy krve, slin, kůže, sperma, potu, vlasů, chlupů atd., ale žádná z těchto stop nám neurčí jasného pachatele, to umí jen DNA, které je v těchto stopách většinou obsažena. Podle těchto stop se poté určuje, do jaké identifikační skupiny pachatel patří, jakého je pohlaví, jakou má krevní skupinu nebo z jaké části těla stopa pochází.

Dále sem můžeme zahrnout i *antropologické zkoumání* (zkoumání kostí a pozůstatků), *fyziodetekční vyšetřování* (detektor lži), *rekognice* (člověk již jednou viděnou osobu pozná a ztotožní) a *vyšetřovací experiment* (má za úkol zjistit, zda mohl člověk vidět nebo slyšet z nějakého místa nějaký jev, např. záblesk nebo výstřel ze zbraně). [28]

4.4.2 Biometrie v bezpečnostně-komerčních aplikacích

Na rozdíl od policejně-soudních aplikací, kde je nutná přítomnost lidského faktoru, zde je lidská činnost nahrazena elektrickými zařízeními. Systémy na bázi biometrických vlastností člověka slouží převážně pro kontrolu vstupu do nebo k nějakému objektu.

Biometrické systémy řízení a kontroly vstupů

Biometrické systémy řízení a kontroly vstupů (ACS – Access Control Systems) jsou přístupové systémy používané v bezpečnostních aplikacích, které pro kontrolu vstupů do chráněných prostor využívají biometrické údaje uživatelů. Přístup do chráněných prostor mají pouze lidi, kteří jsou zaregistrovaní do databáze systému řízení a kontroly vstupu a kteří se mohou prokázat nějakou metodou autentizace. U systémů kontroly vstupu je nutné nějak omezit počet možných pokusů o přihlášení do systému, než bude osoba označena a odmítnuta jako nepovolená osoba, která nemá povolený přístup do střeženého objektu nebo prostor. Zvolit správný poměr počtu přihlášení je velmi důležité. Čím menší počet pokusů pro přihlášení do systému povolíme, tím bude zajištěna větší bezpečnost vstupu a nepovolená osoba nebude mít tolik času na získání dostatečného množství informací o systému, které by mohla využít při dalším pokusu o překonání bezpečnostního systému. Při použití menšího množství pokusů o autentizaci do systému může ale vzniknout problém s přihlášením oprávněného uživatele, který omylem vyvolá falešný poplach při špatné identifikaci do systému.

Použití biometrických systému řízení a kontroly vstupu je velmi široké. Teoreticky lze tyto systémy použít i pro rodinné domy, ale většinou se tak neděje z finančních důvodů. Mnohem většího využití těchto systémů je u např. větších firem pro zabezpečení vchodů do firmy, výrobních hal, skladů, velínů, rozvodných a inženýrských sítí, kanceláří, provozů, utajovaných provozů apod. Další využití je u staveb potřebných pro funkci států nebo staveb, jejichž nefunkčnost by ohrozila bezpečnost státu, např. přehrady, elektrárny, důležité státní budovy, komunikační sítě, elektrické a rozvodné sítě, letiště, vojenské objekty a další objekty. Časté využití je i u veřejně přístupných staveb jako jsou různá

muzea, banky a jiné stavby, ve kterých se manipuluje s drahými nebo vzácnými předměty. Využití je i u menších objektů jako jsou bankomaty. [29]

4.4.3 Biometrie v počítačové bezpečnosti

Další možností, kde lze použít bezpečnostní systémy založené na biometrických charakteristikách člověka, je zabezpečení počítačové techniky. Většinou se jedná o zabezpečení přístupu k pracovní počítačové stanici. K počítači (dále jen PC) je připojen jeden z biometrických systémů, který nahrazuje např. zadávání hesla do systému nebo používání verifikačního předmětu (karty, tokeny[9]), čímž se zvyšuje bezpečnost chráněného počítače. Takto chráněný počítač je za prvé - bezpečnější z pohledu nutnosti použít jednu z jedinečných fyziologických vlastností člověka a za druhé - uživatel si nemusí pamatovat žádná hesla, která nemusí být vždycky v bezpečí a nehrozí jejich ztráta nebo prozrazení. [2]

Existuje nespočet kombinací, kterých lze dosáhnout. Základem je počítač. Může se jednat o běžný stolní počítač (desktop) nebo notebook, kdy už teď některé notebooky obsahují integrovanou čtečku otisků prstů. Kromě „běžných“ PC se může použít např. PDA, mobilní telefon nebo tablet, ale spousta těchto zařízení se také už prodává s integrovanou čtečkou otisků prstů. Na tento počítač nebo podobné zařízení se nainstaluje speciální software, který slouží ke komunikaci s biometrickým zařízením, ukládání biometrických šablon do databáze, porovnávání šablon s právě získaným vzorkem apod. Na takto vybavené PC se potom napojí některý z biometrických systémů. Nejčastěji se používá snímač otisků prstů, snímač oční duhovky, snímač obličeje a verifikace podle hlasu.

Přihlašování na pracovní stanici pomocí biometrického systému:

- uživatel prostřednictvím klávesnice PC zadá svoje uživatelské jméno do příslušné kolonky a následně je PC vyzván k předložení svojí biometrické charakteristiky (otisk prstu, vyslovení fráze apod.),
- PC odešle příkaz biometrickému systému, aby sejmul biometrický vzorek, a daný snímač následně sejme vzorek,
- získaný vzorek je biometrickým systémem odeslán do PC,

[9] Token – je fyzické zařízení (např. USB klíčenka), které usnadňuje uživatelům zabezpečený přístup.

- PC ve své databázi vyhledá již předem uloženou šablonu, se kterou získaný vzorek srovná,
- jestli se šablona a vzorek shodují, je uživateli umožněn přístup k PC, v opačném případě je přístup zamítnut. [2]

Kromě hardwaru (PC, biometrický přístupový systém) a softwaru je potřeba zajistit bezpečnost i komunikačním, přenosovým kanálům, samotným zařízením apod. Komunikace mezi PC a bezpečnostním systémem by měla být šifrována a měla by být odolná vůči odposlechům a modifikacím. Před použitím biometrického systému (např. u otisků prstů) musí být proveden test živosti. Dále musí být zajištěna detekce odpojení bezpečnostního systému od PC, kdy PC může být nahrazeno útočníkovým zařízením (notebookem). Také by měla být zajištěna preventivní fyzická ochrana, která by zabránila manipulaci se systémem a jeho ovlivňování. Všechna kabeláž celého systému by neměla být přístupna zvenčí a ani nijak viditelná.

4.5 Systémy pro měření krevního řečiště

Na trhu se začaly první systémy krevního řečiště objevovat již kolem roku 2000. V posledních letech došlo k rozmachu těchto technologií i k potřebě kvalitnějších a bezpečnějších systémů. Mezi první praktické příklady aplikace biometrického systému na bázi krevního řečiště je systém, který byl použit v Singapuru v roce 2004. Tento systém byl použit v mezinárodním finančním institutu, kde nahradil starší systém čipových karet. Dalším příkladem může být použití v systému pro kontrolu přístupu zaměstnanců do banky FirstBank v Puerto Ricu. [1]

4.5.1 Využití systémů pro měření krevního řečiště

Systémy pro krevní řečiště se pro ochranu biometrickými systémy začínají využívat stále více a jejich obliba stoupá. Krevní řečiště neboli soustava krevních cév je rozvedená do celého těla a celé ho prokrvuje. Krev je ze srdce pumpována okysličená a pomocí tepen a vlásečnic dodávána do celého těla. Zpět do srdce se vrací krev neokysličená.

Pro bezpečnostně-komerční aplikace se krevní řečiště snímá jenom v oblasti rukou. Ostatní oblasti lidského těla jsou pro snímání vždy z nějakého důvodu nevhodné. V ostatních oblastech lidského těla je např. kůže příliš tlustá, aby jí prošel zdroj světla, který je potřeba pro tuto technologii. Hypoteticky by něco podobného šlo použít u lidských nohou, zde je problém s uživatelskou přívětivostí. Uživatel by byl nucen si sundávat boty a ponožky

a vkládat nebo pokládat nohu na snímač. Proto se zdá být ruka jako nejlepší volba. Krevní řečiště na ruce lze snímat na čtyřech místech, a to na třetím článku prstu, na dlani, na hřbetu a na zápěstí. Stejně jako mnoho jiných biometrických systémů, mají i systémy snímání krevního řečiště ruky využití převážně v bezpečnostně-komerčních aplikacích u řízení a kontroly vstupu. Jejich využití v bezpečnostních systémech je vysoké, a to především z důvodu jejich vysoké bezpečnosti, která je dána hlavně tím, že získat skladbu žil je velmi obtížné. Důvodem je její skrytí uvnitř těla, takže je běžným pohledem neviditelná. Krevní řečiště je z pohledu stálosti v čase po celý život téměř neměnné, takže se hodí pro použití v biometrických systémech. Snímání skladby krevního řečiště (cév) je umožněno pomocí vyzařování infračerveného světla (paprsků) s vlnovou délkou (cca 760 nm) odpovídající hodnotou NIR (Near-InfraRed) 700 nm – 1400 nm. Odkysličený hemoglobin[10] v cévách tohle světlo absorbuje s odlišnou délkou než kůže, čímž se sníží odrazivost. Následně jsou zobrazené cévy černě viditelné na snímku a je možné je porovnávat. [1][30]

4.5.2 Snímání žil ruky

Jako u mnoha jiných jedinečných biometrických charakteristik člověka má i krevní řečiště ruky vysokou rozlišovací schopnost u každého z nás a je během celého života uživatele stabilní. Velkou výhodou krevního řečiště je to, že je ukryté pod kůží a je téměř nemožné získat vzor rozložení žil pro případné oklamání systému. Pro systémy měření krevního řečiště ruky existují dvě nejznámější metody. Obě metody pro svoji funkci vyžadují NIR osvětlení a CCD[11] kameru. V této kombinaci dokážou systémy nasnímat žíly ruky. První metoda je založena na odrazu světla, tzv. reflexivní metoda, kde jsou kamera a zdroj světla umístěny na stejné straně prstu. Druhá metoda je založena na tom, že dojde nejprve k prosvícení prstu a poté k následnému útlumu paprsku uvnitř ruky, tzv. transmisivní metoda. U této metody se ruka vkládá mezi kameru a světelný zdroj. [1]

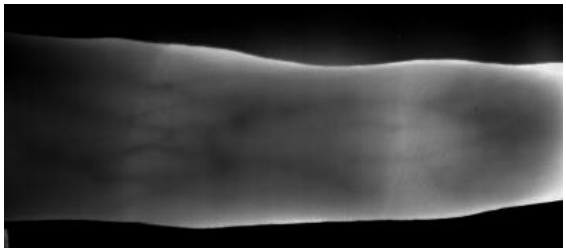
---

[10] Hemoglobin – červený transportní metaloprotein červených krvinek obratlovců. Hlavní funkce hemoglobinu spočívá v transportu kyslíku z plic do tkání a opačným směrem odstraňování oxidu uhličitého z tkání do plic.

[11] CCD (Charge-coupled device) – elektronická součástka používaná pro snímání obrazové informace.

Reflexivní metoda (odraz světla)

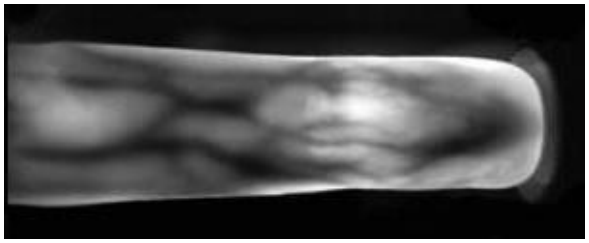
Metoda používající odražené světlo je založena na tom, že obraz vzoru je reprezentován malými rozdíly intenzity odraženého světla. Výsledný snímek je světlejší, než samotné žíly, které jsou tmavší než jejich okolí, což je způsobeno tím, že žíly světlo absorbují a okolní tkáň ne. Výhodou je malá velikost celého zařízení a je příjemnější pro uživatele, kteří nemusejí ruku vkládat dovnitř zařízení. Nevýhodou je složitá extrakce žil. [1]



Obr. 16 Snímek prstu při použití odrazu světla [1]

Transmisivní metoda (prostup světla)

V případě prostupu světla je výsledný obraz velmi kontrastní, jelikož obraz prostupuje z druhé strany ruky a zde není efekt odrazivosti kůže. Nevýhodou je velikost zařízení založeného na této metodě, na rozdíl od metody využívající odrazu světla. Uživatel je nucen vkládat ruku do zařízení mezi světelný zdroj a snímač. [1]



Obr. 17 Snímek prstu při použití prostupu světla [1]

Zpracování obrazu

Pro získání a zpracování obrazu řečiště je nutné splnit několik kroků, mezi které patří:

- *normalizace obrazu* – tedy úprava obrazu do takové podoby až bude střední hodnota a rozptyl intenzity v určité normě. Jedná se o důležitý krok pro další potřebné zpracování obrazu,
- *extrakce žil* – ze získaného normalizovaného obrazu se extrahuje krevní řečiště,
- *porovnání* – poslední fáze, kde dochází k porovnání extrahovaných příznaků a předem do databáze nahrané šablony. [1]

Obecné vlastnosti technologie žil ruky

- nasnímání trvá cca 0,5 sekundy, vytvoření množiny rysů z obrazu trvá cca 1 sekundu, verifikace je velmi rychlá, šablona v databázi zabírá cca 250 bytů, spolehlivost se pohybuje kolem: FAR = 10^{-4} % a FRR = 10^{-1} %,
- po celý život je struktura žil neměnná, rozlišovací schopnost je vyšší jak např. u geometrie ruky a lze tedy technologii žil ruky použít pro více uživatelů (cca 18 tisíc), kdy záleží na použité metodě,
- problémy s kůží, různá kožní onemocnění, prsteny nebo revma nemají žádný vliv při provedení identifikace/verifikace.

Jak už bylo uvedeno výše, pro snímání krevního řečiště na ruce lze použít 4 oblasti. Oblast dlaně ruky, oblast článku prstu, oblast hřbetu ruky a oblast zápěstí.

- *Dlaň ruky* – dlaň se pokládá nebo vkládá do snímače. Snímá se od zápěstí až po konečky prstů. Systémy založené na snímání dlaně jsou ze všech (prst, hřbet, zápěstí) nejbezpečnější, protože poskytují největší snímanou plochu a tím poskytují největší entropii,
- *článek prstu* – na rozdíl od snímačů dlaně neposkytují systémy pro snímání krevního řečiště prstu tolik prostoru, čímž je entropie z daných možností nejmenší. Tohle je navíc umocněno tím, že se řečiště snímá jen v třetím článku prstu, kde je více místa a žíly jsou zde více prokrveny. Snímání se provádí převážně na třech prostředních prstech. Relativní výhodou této metody je malá velikost konečného zařízení při použití reflexivní metody. Relativní je, protože už i ostatní metody dokážou poskytnout kompaktní zařízení,
- *hřbet ruky* – snímání se provádí na vrchní části ruky, tedy na hřbetu, tj. od zápěstí po začátky prstů. Entropie je zde menší. Hřbet ruky se předkládá před snímač, který je většinou upevněn na zdi,
- *zápěstí* – snímání probíhá přiložením nebo vložením zápěstí do zařízení, které následně vyhodnotí získané informace.

4.5.3 Příklady biometrických systémů krevního řečiště

Na trhu neexistuje mnoho biometrických bezpečnostních systémů na bázi snímání krevního řečiště. Nejvíce se této problematice věnují firmy Safran Morpho, Hitachi a Fujistu. Existují, ale i jiné firmy, jako je Sony, Evena (lékařské systémy) apod.

FV-Station 4G (Safran Morpho)

FV-Station 4G (Obr. 16) je biometrický snímač vzoru krevního řečiště prstů na ruce od firmy Safran Morpho. Tento systém přináší uživatelům vysoký výkon, jednoduché použití a progresivní design. Systém FV-Station 4G byl vyvinut pro realizaci přístupových a docházkových systémů jakéhokoliv rozsahu. Systém zvládá rychlé vyhodnocování a průchody osob. Lze jej doplňovat o různá přídavná zařízení podle požadavků na různé instalace. [35]

Systém je k dostání ve 4 základních verzích. Základní FV-Station 4G (Base), FV-Station 4G (Prox) – vestavěná čtečka HID Prox, FV-Station 4G (iCLASS) – vestavěná bezkontaktní čtečka karet iCLASS, FV-Station 4G (MIFARE/DESFire) – vestavěná bezkontaktní čtečka karet MIFARE/DESFire. [35]

Obr. 18 FV-Station 4G [35]

PalmSecure (Fujitsu)

PalmSecure (Obr. 17) je technologie pro snímání obrazu vzoru krevního řečiště ve dlani od firmy Fujitsu. Firma vyrábí bezdotykové zařízení, které je pro uživatele hygienické a snadno ovladatelné přístupové zařízení. Technologie od firmy Fujitsu pracuje na principu zachycení obrazu dlaňových cév pomocí infračervených paprsků (reflexivní metoda).

Výhodou technologie PalmSecure je, že snímač při vytváření obrazu cév dokáže rozeznat vzorec žil jen tehdy, když cévami aktivně proudí odkysličený hemoglobin. [30]

Obr. 19 PalmSecure – snímání vzoru krevního řečiště dlaně [30]

Firma Fujitsu se zabývá vývojem systémů snímání vzoru krevního řečiště dlaně hlavně pro přístupy k elektronickým zařízením (PC, ultrabooky, mobilní telefony apod.). U PC se jedná o snímače (např. OEM Sensor STD), které jsou položeny vedle klávesnice nebo se integrují přímo do počítačové myši pro zabezpečení přihlášení, správu přístupu a ochranu dat pro podniková prostředí. U ultrabooků jsou tyto snímače integrovány přímo do těla přístroje. Fujitsu předvedla ultrabook s označením Lifebook U904. Tento model se již prodává s čtečkou otisků prstů (cena cca 40 000kč v základním provedení), ale měla by se objevit verze se snímačem krevního řečiště (Palm Vein Unit). Do budoucna chce firma tuto technologii dostat i do mobilních telefonů a tabletů, které firma sama vyrábí nebo se spojí s některým mobilním hráčem na trhu. [31] Systém PalmSecure má následující využití:

- řízení fyzického přístupu pro zaměstnance a návštěvníky, zlepšení zabezpečení budov,
- docházkové systémy určené ke snížení podvodů zaměstnanců, automatizované vydávání mzdy,
- přístup k IT systémům v podniku,
- zákazník přichází do styku s bezpečnostním systémem, který mu zaručuje automatizaci plateb, bankovní transakce, převody, registrace apod.

Firma se zabývá i jiným využitím této technologie. Příkladem může být použití vzoru krevního řečiště jako náhrada za palubní letenky na letištích nebo jako náhrada za platební karty do různých obchodů. [32]

Eyes-On (Evena)

Eyes-On jsou brýle (Obr. 18) pro AR[12], tedy rozšířenou realitu určené pro zdravotnický segment, které neslouží pro bezpečnostní účely. Brýle umožňují díky infračervenému vysílači a dvěma kamerami snímat krevní řečiště. Funkce je stejná jako u bezpečnostních systémů založených na krevním řečišti. Tedy snímání krevního řečiště, které díky hemoglobinu v žilách absorbují světlo s jinou vlnovou délkou než kůže. Integrovaný infračervený vysílač pracuje se čtyřmi různými frekvencemi pro detailnější, lepší a ostřejší obraz. Za pomoci těchto brýlí mohou lékaři např. najít u pacienta vhodnou cévu pro zasunutí injekce nebo kanyly a díky brýlím mohou pořizovat fotodokumentaci s celým průběhem zákroku. Velkou výhodou je, že lékaři mohou mít po celou dobu zákroku volné ruce pro jinou činnost. Firma Evena nabízí i vojenskou verzi těchto brýlí pro vojenské lékaře, které se liší hlavně v použitých materiálech a jsou odolnější vůči extrémní zátěži. Tahle verze brýlí nese označení Evena Eagle. [33][34]

Obr. 20 Eyes-On od firmy Evena [33]

[12] AR (Augmented Reality) – česky rozšířená realita – je označení používané pro reálný obraz světa doplněný počítačem vytvořenými objekty, neboli zobrazení reality a následné doplněné o digitální prvky.

II. PRAKTICKÁ ČÁST

5 MORPHOACCESS VP SERIES

Pro praktické měření bylo využito zařízení od firmy Safran Morpho, které nese označení MorphoAccess VP Series. Jedná se o první multimodální zařízení na trhu, které ke svojí funkci využívá 2 typy biometrických charakteristik člověka, a to snímání krevního řečiště a snímání otisku prstu. Série VP se vyrábí ve 2 typech (Obr. 19). MorphoAccess VP – Bio, který umožňuje jen identifikaci a MorphoAccess VP – Dual, který umožňuje identifikaci i verifikaci, pro kterou je potřeba bezkontaktní karta MIFARE® 4k nebo DESFire® 2k, 4k, 8k. Pro praktické měření byla k dispozici verze Bio, která umožňuje pouze identifikaci.

Obr. 21 Zleva: MorphoAccess VP – Bio, MorphoAccess VP – Dual [38]

Jak již bylo napsáno, jedná se o multimodální zařízení, tzn., že zařízení se skládá ze dvou částí – klasického optoelektronického snímače pro čtení informace otisků prstů a infračerveného senzoru pro nasvícení části krevního řečiště třetího článku prstu (blíž ke dlani) a přečtení jeho dat. Kombinace těchto dvou biometrických metod dělají z tohoto zařízení jedno z nejlepších a nejbezpečnějších biometrických zařízení na trhu. Bezpečnost je v kombinaci s nízkými hodnotami FAR a FRR ještě umocněna a je až 10x nižší, než u nejlepších biometrických zařízení na trhu, které disponují jen jednou biometrickou metodou.

Systém MorphoAccess VP (Bio i Dual) používá indikaci pomocí LED panelu, který je umístěn na horní straně zařízení. Zařízení disponuje 6 barvami LED světla, kde každá barva má svůj význam. Použitá je zde zelená (Green), červená (Red), modrá (Blue), žlutá (Yellow), azurová (Cyan) a fialová (Magenta). Následující tabulka (Tab. 3) popisuje základní stavy LED diod, které se liší i tím, že pouze svítí, blikají nebo rychle blikají.

Tab. 3 Základní významy indikace LED diod [36]

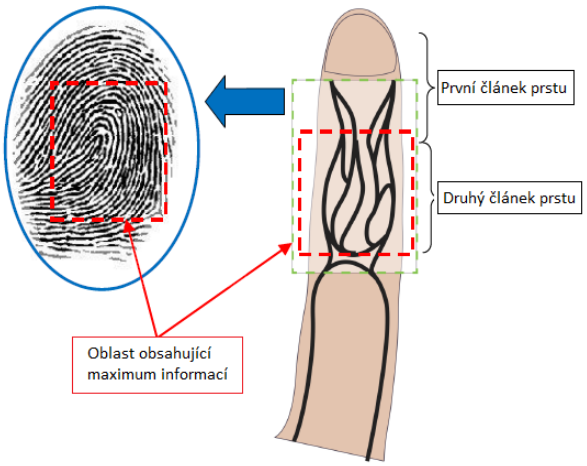
Stav LED	Událost
Zelená (Green) 	Vstup povolen (LED panel svítí)
	Získávání dat kompletní u aktuálně vloženého prstu při registraci do systému (LED panel na 0,5 sekundy zasvítí)
	Registrace kompletní při registraci do systému (LED panel na 1 sekundu zasvítí)
Červená (Red) 	Vstup zamítnut (LED panel svítí)
	Chyba senzoru (LED panel bliká)
Modrá (Blue) 	Systém čeká na prst nebo kartu – stav klidu (LED panel svítí)
Žlutá (Yellow) 	Špatná pozice prstu na snímači (LED panel bliká)
	Prst odebrán příliš brzo (LED panel svítí)
	Prázdná databáze nebo absence databáze (LED panel bliká)
	Špatná pozice prstu na snímači při registraci do systému (LED panel rychle bliká)
Azurová (Cyan) 	Systém oznamuje, že USB klíč může být odebrán (LED panel rychle bliká)
Fialová (Magenta) 	Probíhá konfigurace terminálu (LED panel bliká)
	Update firmware biometrického systému (LED panel bliká)
	Systém čeká na prst při registraci do systému (LED panel rychle bliká)
	Průběh získávání dat při registraci do systému (LED panel rychle bliká)
	Aktuální pozice – získávání dat kompletní při registraci do systému (LED panel rychle bliká)
	Získání dat kompletní – odebrat prst a vložit další při registraci do systému (LED panel bliká po dobu 1s následované rychlým blikáním)
	Registrace kompletní - průběh zaznamenávání biometrických dat (LED panel rychle bliká)

5.1 Popis terminálu

Pro praktickou část je v tomto bodu popsán použitý terminál. V první části jsou popsány obě používané biometrické metody, se kterými terminál pracuje, správné a špatné pozice prstu při snímání, které jsou důležité pro správné užívání a detailní popis terminálu a všech jeho konektorů a svorkovnic.

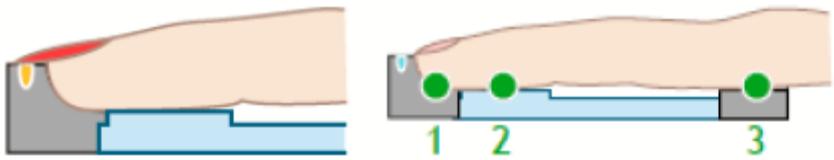
5.1.1 Použité biometrické metody u MorphoAccess VP

K identifikaci a verifikaci je u terminálu MorphoAccess VP použita kombinace krevního řečiště a otisků prstů (Obr. 20). U otisku prstu se pro snímání používá oblast prvního článku prstu. Pro krevní řečiště je oblast snímání někde mezi prvním a třetím článkem prstu ruky.



Obr. 22 Nejpoužívanější oblasti prstu pro biometrická data [36]

Správná pozice

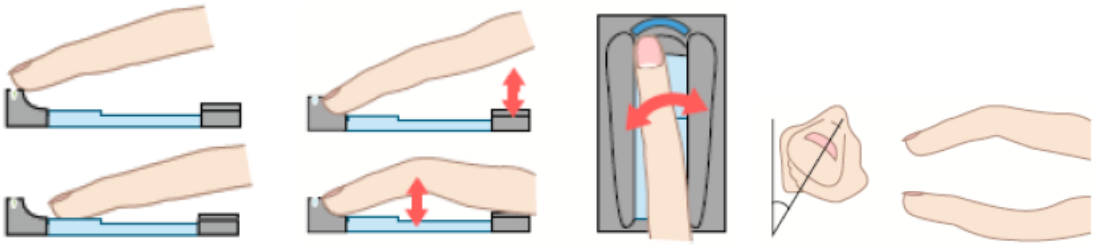


Obr. 23 Správné polohy prstu na snímači [36]

- Umístěte špičku prstu do kontaktu s kulatým okrajem konce (1),
- v případě dlouhého nehtu umístěte nehet na horní vrch kulatého okraje konce, kdy konec prstu bude v kontaktu kulatým okrajem konce (1) a ne špičkou nehtu,
- držte prst v kontaktu s kulatým okrajem konce (1),

- ujistěte se, že první článek prstu s otiskem je ve správném kontaktu s průhlednou plochou optického snímače (2),
- umístěte základnu prstu na snímač ve správné poloze na druhé straně (3),
- nechte volně položenou dlaň ruky na plášti terminálu. [36]

Špatná pozice



Obr. 24 Špatné polohy prstu na snímači [36]

- Nepokládejte prst na vrch kulatého okraje konce,
- nepokládejte prst na povrch senzoru: prst musí být v kontaktu s kulatým okrajem konce,
- prst se nesmí nechávat ve vzduchu a nesmí se ohýbat,
- nenaklánějte prst: prst musí být rovnoběžně se stěnami senzoru,
- při vložení prstu se s ním nesmí otáčet,
- neohýbejte prst nahoru ani dolů. [36]

Stav prstu

Při použití snímače je nutné, aby prst byl ve správném stavu pro správnou identifikaci:

- otřete si před použitím prst, jestli je příliš vlhký,
- před použitím si zahřejte prst, jestli je příliš studený nebo suchý,
- je-li prst příliš suchý, tak je jemně navlhčete,
- v případě, že je prst znečištěný, tak prst očistěte,
- netlačte příliš silně na snímač, aby se zabránilo zúžení krevních cév. [36]

5.1.2 Uživatelské rozhraní

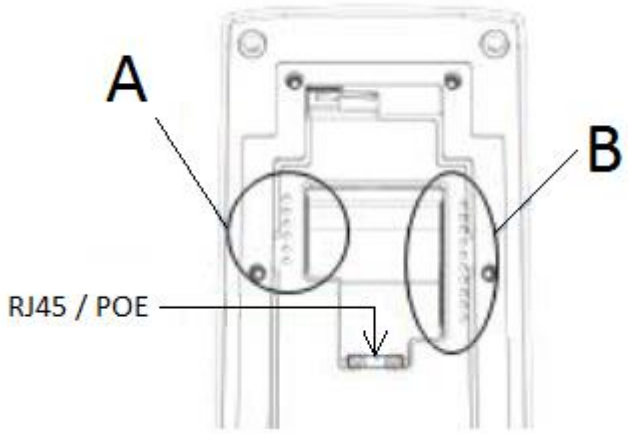
Terminál MorphoAccess VP (Obr. 23) je jednoduché a ergonomické přístupové biometrické zařízení, které je určeno převážně pro montáž na zeď. Terminál MorphoAccess VP se skládá ze 4 základních částí:

1. vysoce kvalitní optický skener pořizující biometrická data z prstu,
2. LED diody (Multi-color),
3. více tónový bzučák,
4. čtečka bezkontaktních karet MIFARE®/DESFire®.

Obr. 25 Přední pohled MorphoAccess VP [36]

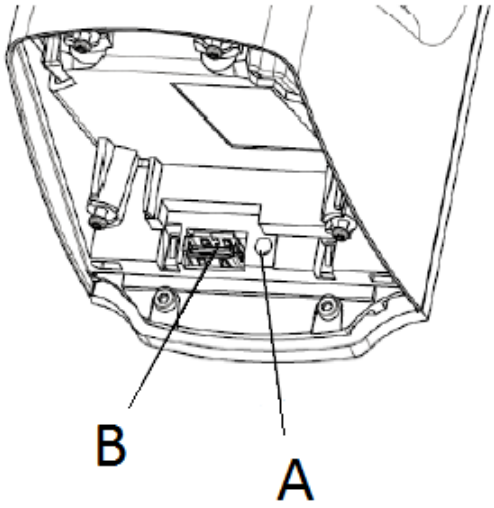
5.1.3 Napájecí rozhraní

Terminál MorphoAccess VP je možné napájet dvěma různými způsoby. Terminál je možné napájet přes +12V DC/GND zdroj nebo použít napájení přes POE (Power Over Ethernet), (Obr. 24), tedy napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem. [36]



Obr. 26 Pohled zezadu MorphoAccess VP [36]

Při napájení může dojít k zamrznutí terminálu, ať z důvodu hardwarové nebo softwarové chyby. Proto se na spodní straně po odkrytování terminálu, hned vedle USB portu (Obr. 25B), nachází tlačítko (Obr. 25A) pro „tvrdý reset“, kterým se zařízení „natvrdo“ vypne a uvede do původní podoby. [36]

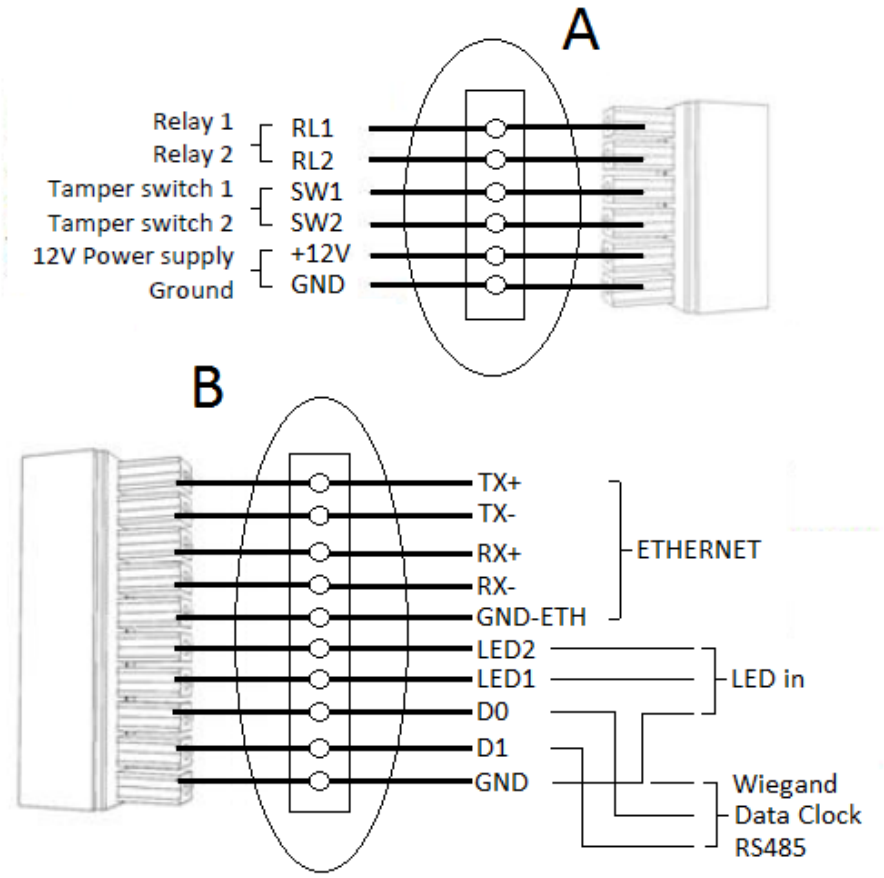


Obr. 27 Pohled zespodu MorphoAccess VP [36]

5.1.4 Řídící rozhraní

Terminál zezadu obsahuje svorkovnice. První část (Obr. 26A) ukazuje připojení napájení, zem, dvě svorky pro tamper switche a dvě svorky pro připojení relé. Na druhé části obrázku (Obr. 26B) najdeme popis svorkovnice pro připojení Ethernet konektorů (LAN 10/100 Mbps, pro použití TCP nebo SSL protokolu), dvě svorky pro LED diody, svorky pro připojení k přístupovému systému (Wiegand, Data Clock), svorku pro

sběrnicové zapojení (RS-485) a zem. Dále se na terminálu nachází konektor RJ45 pro síťové rozhraní Ethernet a USB port, který se nachází pod spodním krytem terminálu a může sloužit jako Wi-Fi USB adaptér. [36]



Obr. 28 Konektory (svorkovnice) [36]

5.2 Propojení terminálu s PC

Pro plné využití potenciálu zařízení je potřeba terminál propojit s PC. Propojení uživateli slouží ke konfiguraci terminálu a jeho různých nastavení, pro nahrávání vylepšení, upgradů a firmwaru, přidávání licencí (pro odemčení rozšířených vlastností), dále pro manipulaci a správu databází, upravování, přidávání, mazání atd. uživatelských účtů nebo konfiguraci Wi-Fi připojení. Terminál MorphoAccess VP s PC, lze propojit několika způsoby. Přes jeden Ethernet kabel, přes dva Ethernet kabely a switchem nebo přes LAN. Pro připojení je potřeba několik síťových parametrů (IP adresu terminálu, IP adresu brány a masku podsítě), (Tab. 4). [36]

Tab. 4 Síťové parametry

Přiřazená IP adresa	Parametr	Hodnota
Statická (defaultně)	IP adresa terminálu	134.1.32.214
	IP adresa brány	134.1.6.20
	Maska podsítě	255.255.240.0
Dynamická (DHCP)	Host Name	MA<Serial Number>

5.2.1 Propojení terminálu a PC přes Ethernet kabel

Propojení terminálu a PC je uskutečněno přes kabel Ethernet, který je zde použit pro vzájemnou komunikaci. V propojení terminálu a PC přes kabel Ethernet má několik limitů.

- V případě, že Ethernet port umístěný v PC nepodporuje funkci Auto MDI/MDIX[13], pak je potřeba použít křížený Ethernet kabel. Pokud není k dispozici žádný křížený Ethernet kabel, je nutné použít switch.
- Je-li PC, které má být propojeno s terminálem, připojeno k síti, musí být odpojeno od sítě LAN nebo vybavené dvěma síťovými rozhraními, kdy jedno bude použito pro spojení s terminálem. [36]

5.2.2 Propojení terminálu a PC pomocí switche

Další možností propojení terminálu a PC je pomocí síťového prvku switche (přepínače). Tuto metodu lze použít hlavně, když není k dispozici žádný křížený síťový kabel. Pro provedení této metody je zapotřebí jednoho Ethernet switche a dvou standardních přímých Ethernet kabelů. Jako náhradu nelze použít Ethernet HUB, který neumožňuje připojení mezi dvěma porty, proto je nutné použít Ethernet switch. [36]

5.2.3 Propojení terminálu a PC pomocí lokální sítě LAN

Poslední možností, jak propojit terminál s PC, je použití lokální sítě LAN. Terminál vyžaduje pro svoje připojení IP adresu nebo jméno hostitele (Host Name). Vybrat můžeme mezi statickou adresou a dynamickou adresou, která je přidělena automaticky DHCP serverem. Doporučuje se připojit terminál na dedikovanou síť pro snížení možných

[13] Auto MDI/MDIX – eliminace nutnosti použití nekřížených kabelů (možno použít přímé i křížené kabely).

podvodných přístupů k nastavení terminálu. Před připojením k síti LAN je nutné zadat parametry sítě LAN terminálu. Hodnoty těchto parametrů musí být poskytnuty a schváleny správcem sítě. [36]

5.2.4 Nastavení hodnot IP adresy pomocí USB klíče

Parametry připojení k síti můžou být inicializovány a měněny pomocí vysokokapacitního USB klíče. Není potřeba kabelového připojení s PC. USB klíč musí mít minimálně 8 GB paměti, rozhraní alespoň USB 2.0, naformátovaný na FAT16 nebo FAT32 s speciální PC aplikaci (USB Network Configuration Tool). Nastavení IP adresy pomocí USB klíče je vhodné pro terminály, které nejsou vybaveny klávesnicí a displejem. USB klíč ale může být použitý i u jiných terminálů, které klávesnicí a displejem disponují. Nastavení hodnot IP přes USB obsahuje 2 následující kroky:

První krok – vytvořit konfigurační soubor na USB klíči.

- Nejprve na PC spustíme aplikaci USB Network Configuration Tool. Vložíme USB klíč do USB portu a v programu nejprve zvolíme DHCP režim (IP adresa je přidělena automaticky) nebo statický režim (statická IP). Pokud si zvolíme režim DHCP, musíme uvést Host Name terminálu získaný od administrátora sítě. Pokud je vybrán statický režim, musíme zadat IP adresu terminálu poskytnutou správcem sítě. Po vyplnění všech polí klikneme na Write File. Vyberte kořenový adresář USB klíče. [36]

Druhý krok – použít změny na terminálu.

- Sejmeme spodní kryt terminálu pro přístup k USB portu terminálu (Obr. 25B). Zapneme terminál a vložíme USB klíč s vytvořeným konfiguračním souborem. Po vložení se spustí proces, který trvá několik vteřin. Proces je doprovázen zvukovými a světelnými signály. Těmito signály je proces i ukončen žádostí o odstranění USB klíče (LED panel rychlé bliká azurovou barvou). Po vyjmutí USB klíče se terminál restartuje a použije nové hodnoty IP adresy. Terminál je připraven pro připojení k síti. [36]

5.2.5 Nastavení Wi-Fi sítě

Terminál MorphoAccess VP je možné připojit na Wi-Fi. K dispozici jen při dodržení těchto podmínek:

- Morpho USB Wi-Fi adaptér musí být připojen k přednímu USB portu terminálu,

- terminál musí obsahovat Wi-Fi licenci,
- terminál nesmí být připojen k síti pomocí Ethernet kabelu. Připojení Wi-Fi a Ethernet kabelu se vzájemně vylučují,
- po získání Wi-Fi licence a vložení USB Wi-Fi adaptéru se terminál musí restartovat stisknutím tlačítka reset (Obr. 25A). [36]

5.3 Seznam základních technických parametrů a vlastností

Tab. 5 Technické specifikace terminálu [39]

Technologie	Multimodální – kombinace krevního řečiště a otisku prstu
	Zachycení a vyhodnocení dat ze dvou biometrických metod současně
Fyzické vlastnosti	Š x V x H – 90 x 160 x 125 mm (3.54” x 6.3” x 4.92”)
	Váha – 515 g
Senzor	Optický
	Senzor otisku prstu - 400 x 400 bodů, 500 dpi, 256 stupnice šedi, certifikace FBI PIV IQS
	Zevnější snímání prstu
Procesor	Dual Core procesor ARM9 – první jádro @200MHz, druhé jádro @400MHz
Karta	MIFARE®/DESFire® (pouze u modelu MorphoAccess VP - Dual)
Indikace zařízení	Zelené podsvícení snímače při vložení prstu
	Barevný LED indikátor (zelená, červená, modrá, žlutá, fialová, azurová)
	Více tónový bzučák

Tab. 6 Vlastnosti systému [39]

Biometrické vlastnosti	Identifikace 1:5000 (standardní verze), 1:10000 (verze s licencí)
	Verifikace s použitím bezkontaktní karty (pouze u modelu MorphoAccess VP - Dual)
Kapacita uživatelů	5000 – 10 000 uživatelů ve standardní verzi
	20 000 – 50 000 uživatelů ve verzi s licencí
Bezpečnostní vlastnosti	Nastavitelné FAR: 10^{-2} až 10^{-8}
	Stabilní bez ohledu na počet osob v databázi

Tab. 7 Výkonnost systému [39]

Rychlost vyhodnocení	Identifikace: 1 - 1,5s (1:500 – 1:5000)
	Verifikace: 1s (pouze u modelu MorphoAccess VP - Dual)
Použitelnost	FTE
Přesnost	FAR: 10^{-4}

Tab. 8 Rozhraní terminálu [39]

LAN	Ethernet 10/100
	Bezdrátová LAN (Wi-Fi), WEP a WPA šifrování
	TCP/IP (pro zadání otisků prstů)
Kontrola vstupu (output)	Wiegand (pro připojení k přístupovému systému)
	Dataclock ISO2 (pro připojení k přístupovému systému)
	RS-485 (pro sběrnicové zapojení)
Kontrola vstupu (input)	LED in
Bezpečnostní switche	Detekce odcizení
	Detekce narušení (Tamper)
USB port	Konfigurace terminálu přes USB klíč
Napájení	Externí 9V – 16V DC (1A min @12V)

Tab. 9 Pracovní prostředí terminálu [39]

IP odolnost	IP65
Teplota	Provozní: -10°C do 50°C (14°F do 122°F)
	Úložiště: -20°C do 70°C (-4°F do 158°F)
Vlhkost	Provozní: 10 % < RH < 80 %
	Úložiště: RH < 95 %

Tab. 10 Certifikace [39]

Obrazový senzor	FBI PIV IQS
Použitý algoritmus (otisk prstu)	FIPS 201, MINEX
EMC/bezpečnostní standardy	CE, CB, FCC, NF EN 60825-1 2008-01
Standardy	RoHS, REACh, WEEE

Tab. 11 Příslušenství a SW výbava [39]

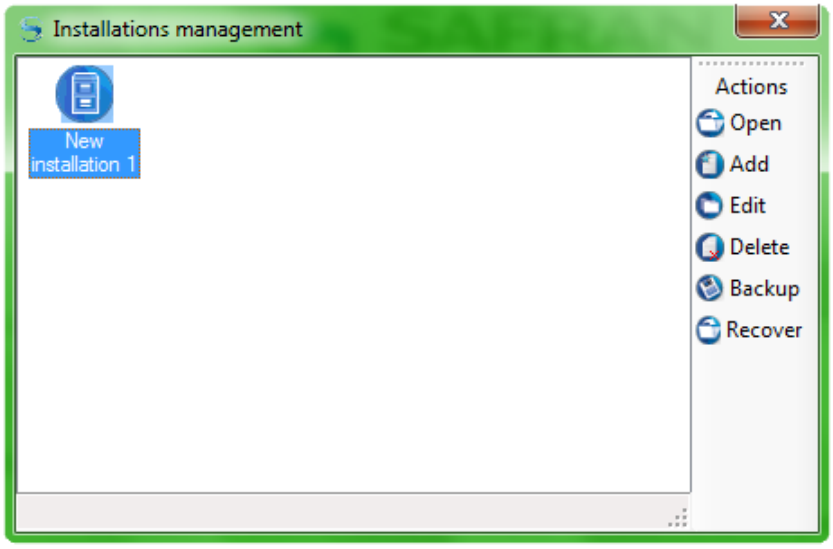
Příslušenství (součástí balení)	Montážní deska na zeď
Příslušenství (doplňkové)	Napájecí zdroj
	MIFARE®/DESFire® bezkontaktní karty
	MA WI-FI Pack
SW výbava	Morpho Enroll
	Morpho Integrator's Kit (MIK)

5.4 Easy2Enroll a testování funkčnosti s terminálem

V tomto bodu praktické části se diplomová část zabývá programovým rozhraním pro komunikaci s terminálem MorphoAccess VP. Pro komunikaci s pracovní stanicí byl použit program Easy2Enroll, který je vyvíjen přímo firmou Safran Morpho, nebo je možné použít i program Morpho Enroll. Práce se věnuje základním krokům pro zprovoznění terminálu s programem, který zahrnuje založení uživatelského účtu, první spuštění programu, propojení terminálu s programem, vytvoření nového uživatele, testování programu s terminálem a popis funkcí programu Easy2Enroll.

5.4.1 Založení účtu

Po úspěšné instalaci spustíme nainstalovaný program, u kterého jsme vyzváni k výběru jazyka (angličtina, francouzština a španělština). Následuje okno s vytvořením nového účtu. Napravo zvolíme **Add** a v novém okně zvolíme, jaký typ instalace chceme (pro svoje měření jsem zvolil **Access Database**), potom zvolíme název databáze (defaultně je New Installation 1) a umístění databáze, dále si zaškrtneme pracovní dny (pondělí až neděle) a potvrdíme **Confirm**. V okně (Obr. 27) **Installations management** se nám objeví nová položka **New installation 1**, kterou označíme a napravo klikneme na **Open**.



Obr. 29 Konečné okno po přidání účtu

Po kliknutí na **Open** vybereme položku **Administrator** a potvrdíme tlačítkem OK, vyskočí okno, kde si vytvoříme administrátorské heslo (které je vyžadováno při každém spuštění) a tím se dostaneme na hlavní stranu programu (Obr. 28). Tím byl nainstalován program Easy2Enroll.

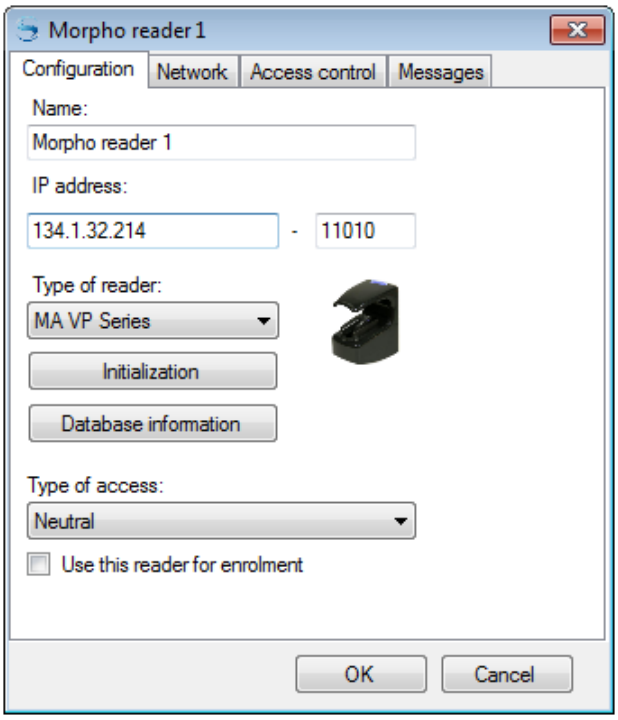
Obr. 30 Hlavní rozhraní programu Easy2Enroll

5.4.2 První spuštění programu

Pokud program spouštíme podruhé, jsme požádání o výběr jazyka a vložení administrátorského hesla, které jsme si vytvořili již při první instalaci a spuštění programu.

Jako první je nutné přidat čtečku. V našem případě se jedná o MorphoAccess VP. V levém sloupci klikneme na **Morpho readers** a klikneme na **Add a reader**. Objeví se okno (Obr. 29) se čtyřmi záložkami (Configuration, Network, Access control a Messages).

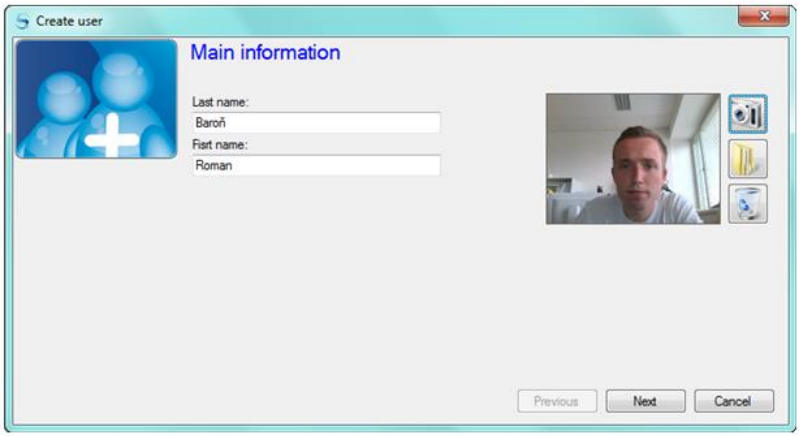
Zůstaneme na položce **Configuration**, zde si můžeme pojmenovat čtečku, zadáme IP adresu zařízení (IP address - 134.1.32.214), vybereme typ čtečky (Type of reader), v našem případě MA VP Series a typ přístupu (Type of access) necháme na **neutral**. Na položce **Network** vepíšeme masku sítě (Subnet mask - 255.255.255.0) a vše potvrdíme tlačítkem OK. Pro propojení je nutné si ve vlastnostech síťového adaptéru v počítači nastavit IP adresu (134.1.32.10) a masku podsítě (255.255.255.0). Že se nám podařilo propojení, zjistíme tak, že v hlavním rozhraní se místo nápisu **Check status of your network** objeví nápis **Active installation**. Čtečka by měla začít komunikovat se softwarem Easy2Enroll.



Obr. 31 Záložka Configuration v programu Easy2Enroll

5.4.3 Vytvoření nového uživatele v databázi

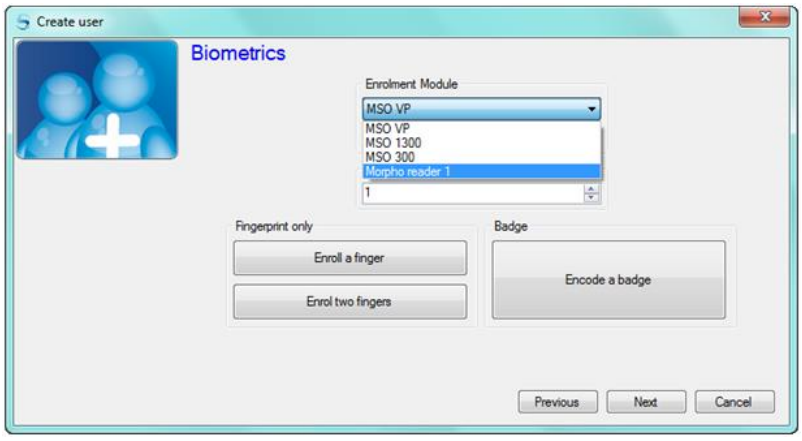
V panelu nástrojů vybereme položku **Users** a zvolíme **Create User**. Otevře se nám okno s hlavními informacemi (Obr. 30), kde vložíme jméno a příjmení uživatele, případně vytvoříme fotografii uživatele.



Obr. 32 Hlavní informace při vytváření uživatele

V další části vytvoříme přístupovou skupinu, kterou si libovolně pojmenujeme. V další části (Obr. 31) vybereme používaný terminál **Enrolment Module** (v mém případě pojmenovaný Morpho reader 1), číslo uživatele (ID) a necháme si přes čtečku načíst otisk prstu a krevní řečiště. Můžeme si vybrat, zda chceme jen jeden prst **Enroll a finger** pro

přihlašování nebo zda použijeme dva prsty **Enroll two fingers**. Použití dvou prstu je vhodnější, protože si můžeme jeden prst např. pořezat a potom bychom se nemohli úspěšně přihlásit. Funkce **Enroll a badge** slouží pouze pro verifikaci kartou. Tato možnost u tohoto terminálu nebyla k dispozici.



Obr. 33 Okno pro snímání biometrických údajů

Pro sejmutí snímku otisku prstu a krevního řečiště klikneme na tlačítko **Enroll a finger**. Poté vložíme prst do snímače. Správné sejmutí snímku poznáme tak, že terminál bliká fialově a ozve se zvukový signál. Po zvukovém signálu vložíme prst opětovně do terminálu ještě dvakrát. Po trojím úspěšném vložení prstu nám vyskočí okno (Obr. 32) s průměrným hodnocením kvality (Tab. 12) všech tří snímku jednoho prstu. Při použití dvou prstů (Enroll two fingers) se třikrát vloží jeden prst a po bliknutí zelené barvy na terminálu vložíme třikrát druhý prst. Výsledkem bude opět tabulka se dvěma skóre. Poté jen potvrdíme **Confirm** a přidáme uživatele.

Obr. 34 Okno s průměrnými hodnotami kvality (jeden a dva prsty)

Pro testování systému s jedním prstem byl použit ukazováček levé ruky s hodnotou skóre 103 a pro testování systému se dvěma prsty byl použit prsteníček a prostředníček pravé ruky s hodnotou skóre 95 a 82. Hodnota skóre závisí na tom, jak správně je prst na snímač položen a na stavu prstu.

Tab. 12 Číselná kvalita skóre biometrických údajů

Hodnota	do 40	40 - 60	60 - 90	90 - 120	Nad 120
Kvalita	Velmi špatná	Špatná	Dobrá	Velmi dobrá	Vynikající

5.4.4 Testování funkčnosti

Pro prvotní otestování systému byly do databáze vloženy šablony čtyř uživatelů (Obr. 33). Chce-li se uživatel přihlásit do systému, vloží do terminálu jeden ze svých referenčních prstů. Je-li oprávněný uživatel přijat, terminál zabliká zeleně v doprovodu zvukového signálu a naopak je-li odmítnut, terminál zabliká červeně v doprovodu zvukového signálu.

	Last name	First name	Status	ID
▶	Baroň1	Roman	Allowed	1
	Baroň2	Roman	Allowed	2
	Baroň3	Roman	Allowed	3
	Baroň4	Roman	Allowed	4

Obr. 35 Seznam uživatelů

Všichni čtyři uživatelé (Tab. 13) nesli příjmení, jméno, identifikační číslo, stav přístupu, použitou ruku, počet použitých prstů, prst a výslednou kvalitu skóre.

Tab. 13 Seznam uživatelů a jejich informace

Příjmení	**Jméno**	**ID**	**Přístup**	**Ruka**	**Počet prstů**	**Prst (y)**	**Kvalita skóre**
Baroň1	Roman	1	Povolen	Levá	1	Prsteníček	75
Baroň2	Roman	2	Povolen	Levá	2	Prostředníček, ukazováček	110, 97
Baroň3	Roman	3	Povolen	Pravá	1	Ukazováček	92
Baroň4	Roman	4	Povolen	Pravá	2	Prostředníček, prsteníček	100, 88

Že byl přístup povolen nebo zamítnut, je možno si kromě blikání terminálu a zvukového doprovodu ověřit i přímo v programu. V hlavním rozhraní programu se dole nachází seznam událostí (Obr. 34), který zobrazuje posledních 2000 událostí. Pokud není viditelný, můžeme si ho zapnout přes hlavní lištu v položce **View – Evenst list** (seznam událostí). V tomto seznamu se nachází poslední události, ze kterých lze vyčíst datum pokusu

o přístup, typ události – zda byl uživatel přijat (User accepted) nebo se jedná o neznámého uživatele (Unknown identifier), název čtečky (Readers) – pokud je do systému připojeno více čteček, tak podle tohoto seznamu poznáme, u které z nich došlo k přístupu nebo zamítnutí, identifikační číslo a jméno a příjmení uživatele.

	Date	Type	Reader	Identifier	Last name	First name
	10.4.2014 14:51:36	Unknown Identifier	Morpho reader 1			
	10.4.2014 14:49:21	User accepted	Morpho reader 1	1	Baroň1	Roman
▶	10.4.2014 14:47:06	Unknown Identifier	Morpho reader 1			
	10.4.2014 14:43:33	User accepted	Morpho reader 1	2	Baroň2	Roman
	10.4.2014 14:25:54	User accepted	Morpho reader 1	3	Baroň3	Roman
	10.4.2014 14:25:47	User accepted	Morpho reader 1	3	Baroň3	Roman
	10.4.2014 14:24:08	User accepted	Morpho reader 1	4	Baroň4	Roman

Obr. 36 Seznam událostí

5.4.5 Popis funkcí programu

Při spuštění programu je na hlavní liště položka **File** - umožňuje změnu hesla, odhlášení a vypnutí programu. **View** – umožňuje zapínat a vypínat panely nástrojů, panely statistik, panely událostí, zkratky, ikonu na hlavním panelu Windows. **Tools** – obsahuje nastavení událostí, tisk šablon karet a správce licencí. **Preferences** – umožňuje nastavení terminálu, emailu, RFID, synchronizace čteček, automatické uložení, nastavení biometrie a další informace pro uživatele. **Windows** – nastavení oken a ikon. **Help** – o programu a uživatelská příručka.

Obr. 37 Panel nástrojů

Pod hlavní lištou se nachází panel nástrojů (Obr. 35). Na tomhle panelu se nachází **Settings** – správa zapojených čteček, stav zapojených čteček (název čtečky, IP adresa, stav, sériové číslo, verze, počet databází). **Schedule and Access Rights** – správa skupin s přístupem, správa časových zón. **Users** – vytvoření nového uživatele, vyhledávání uživatelů, seznam uživatelů, obnovení uživatelů, import seznamů, čas a docházka. **Events** – seznam událostí, přihlášení a zprávy událostí. **Map** – úprava a otvírání nových map. **Administration** – správa uživatelských profilů.

6 PRAKTICKÉ MĚŘENÍ

Tahle kapitola je zaměřena na praktické použití měřící soustavy (Obr. 36). Měřící soustava se skládá z terminálu MorphoAccess VP – Bio, stolního terminálu MorphoSmart Finger VP, notebooku HP a programy Easy2Enroll a MorphoEnroll.

Obr. 38 Měřící soustava (MorphoAccess VP, MorphoSmart VP a notebook)

Cílem praktického měření je výpočet chybovosti systému a měření shody u otisků prstů rodinných příslušníků (nahrazeno původním plánem, že bude snímána shoda krevního řečiště u rodinných příslušníků, viz. kapitola 7).

6.1 Spolehlivost identifikace pomocí terminálu

Spolehlivost identifikace pomocí metody krevního řečiště je celkem vysoká. Výhodou této metody na rozdíl od ostatních je nemožnost jakkoliv zjistit vzor skladby žil, které jsou skryté pod kůží a tento vzor pak použít k obelstění terminálu. Vzorek např. otisku prstu nebo snímek obličeje lze hypoteticky získat velmi snadno, ale získat vzor žil bez IR diod s různými vlnovými délkami a nějaké kamery je velmi složité, aniž by si toho dotyčná osoba všimla. Ale i u ostatních metod je rozdíl mezi získáním těchto biometrických informací a jejich použití v reálných podmínkách. U mnoha biometrických systémů se používají různé testy, které znemožňují systém obelstít, jako např. test živosti, který lze jen velmi obtížně obejít. Velkou výhodou terminálu MorphoAccess VP je jeho multimodálnost, tzn., že používá pro identifikaci a verifikaci dvou biometrických vlastností člověka. Při vložení prstu do terminálu se do šablony uživatele zapíše vzor krevního

řečiště, který je doplněný o otisk prstu. Spolehlivost tohoto terminálu je proto vyšší, než u nejlepších systému založených jenom na jedné metodě.

6.1.1 Měření chybovosti terminálu

Pro měření chybovosti terminálu jsou důležité dvě hodnoty, a to pravděpodobnost chybného odmítnutí (FRR) a pravděpodobnost chybného přijetí (FAR), které pracují s hodnotou citlivosti, tzv. thresholdem (Th). Threshold je hodnota, u které když nastavíme Th např. na 55, tak je FAR = cca 5,5% a FRR = cca 1,5%, tzn., že je 5,5% pravděpodobnost přijetí nežádoucí osoby a 1,5% pravděpodobnost, že terminál odmítne oprávněného uživatele (viz. Obr. 14). Hypoteticky je tedy možné, že by se na šablonu nějakého oprávněného uživatele mohl přes terminál dostat někdo neoprávněný.

Měření bylo provedeno v reálném čase a zúčastnilo se ho 30 osob. Každé osobě byla vybrána levá nebo pravá ruka (levá i pravá ruka byly v měření zastoupeny ve stejném množství). Každá osoba podstoupila registraci sejmutím snímku ukazováčku (Uk) dané ruky funkcí Enroll a Finger a sejmutím snímku prostředníčku (Pr) a prsteníčku (Ps) v libovolném pořadí funkcí Enroll Two Fingers. V databázi byly tedy uloženy 2 šablony od každého účastníka (1. vzorek ukazováčku a 2. vzorek prostředníčku a prsteníčku) celkově tedy 60 šablon. Následně proběhly 3 testy identifikace osob. U každého účastníka se testovala 3x identifikace přes ukazováček a 3x identifikace přes prostředníček nebo prsteníček. Proběhlo tedy 180 pokusů o identifikaci. Použitý práh byl na defaultní hodnotě, protože kvůli chybě v programu nebylo možné hodnotu měnit.

Příloha P I Tabulka naměřených údajů pro výpočet spolehlivosti

Ze 180 identifikací bylo 7 nesprávných odmítnutí, z toho 5 u ukazováčku a 2 u prostředníčku/prsteníčku nebo 4 u levé ruky a 3 u pravé ruky. A 173 úspěšných přijetí. Úroveň kvality biometrických údajů se pohybuje od 0 – 40 jako velmi špatná kvalita až nad 120 jako vynikající kvalita. Vynikající kvality (tedy nad 120) dosáhlo 14 vzorků z 90. Velmi dobré kvality (rozmezí 90- 120) dosáhlo největšího počtu vzorků 66. Kvality dobrá (rozmezí 60 - 90) dosáhlo 9 vzorků. Kvality špatná (rozmezí 40 - 60) dosáhl jen jeden vzorek a kvalita velmi špatná (do 40) se vůbec neobjevila.

Vypočtené FAR vyšlo 0%, což značí, že je hypotetická 0% pravděpodobnost přijmutí neoprávněného uživatele, při použití libovolného prstu, libovolné ruky. 0% je dáno tím, že na žádnou z 60 šablon se nedokázal přihlásit žádný neoprávněný uživatel. Prvních 15

účastníku zanechalo 2x15=30 šablon a druhých 15 účastníků se snažilo na tyto šablony přihlásit a potom to bylo naopak. Nikdo se nedokázal přihlásit na cizí šablonu.

$$FAR = \frac{počet\ nesprávných\ přijetí}{počet\ všech\ pokusů\ o\ nesprávné\ přijetí} \cdot 100\% = \frac{0}{60} \cdot 100\% = 0\%$$

Celkové FRR vyšlo 3,88%, což značí, že je hypotetická 3,88% pravděpodobnost odmítnutí oprávněného uživatele při použití libovolného prstu libovolné ruky.

$$FRR.celkem = \frac{počet\ nespráv.odmít.libovol.prstu\ a\ ruky}{počet\ všech\ pokusů\ o\ ident.libovol.prstu\ a\ ruky} \cdot 100\%$$
$$= \frac{7}{180} \cdot 100\% = 3{,}88\%$$

Celkové FRR pro levou a pravou ruku vyšlo 4,44% a 3,33%, což značí, že je hypotetická 4,44% pravděpodobnost odmítnutí oprávněného uživatele při použití libovolného prstu levé ruky a hypotetická 3,33% pravděpodobnost odmítnutí oprávněného uživatele při použití libovolného prstu pravé ruky.

$$FRR.levá.celkem = \frac{počet\ nespráv.odmít.libovol.prstu\ levé\ ruky}{počet\ všech\ pokusů\ o\ ident.libovol.prstu\ levé\ ruky} \cdot 100\%$$
$$= \frac{4}{90} \cdot 100\% = 4{,}44\%$$

$$FRR.pravá.celkem = \frac{počet\ nespráv.odmít.libovol.prstu\ pravé\ ruky}{počet\ všech\ pokusů\ o\ ident.libovol.prstu\ pravé\ ruky} \cdot 100\%$$
$$= \frac{3}{90} \cdot 100\% = 3{,}33\%$$

Celkové FRR pro ukazováček a prostředníček/prsteníček vyšlo 5,55% a 2,22%, což značí, že je hypotetická 5,55% pravděpodobnost odmítnutí oprávněného uživatele při použití libovolného ukazováčku a hypotetická 2,22% pravděpodobnost odmítnutí oprávněného uživatele při použití libovolného prostředníčku/prsteníčku.

$$FRR.Uk = \frac{počet\ nespráv.odmít.Uk\ libovol.ruky}{počet\ všech\ pokusů\ o\ ident.Uk\ libovol.ruky} \cdot 100\% = \frac{5}{90} \cdot 100\%$$
$$= 5{,}55\%$$

$$FRR.Pr,Ps = \frac{počet\ nespráv.odmít.Pr,Ps\ libovol.ruky}{počet\ všech\ pokusů\ o\ ident.Pr,Ps\ libovol.ruky} \cdot 100\% = \frac{2}{90} \cdot 100\%$$
$$= 2{,}22\%$$

FRR pro levé ukazováčky a levé prostředníčky/prsteníčky vyšlo 6,66% a 2,22%, což značí, že je hypotetická 6,66% pravděpodobnost odmítnutí oprávněného uživatele při použití levého ukazováčku a hypotetická 2,22% pravděpodobnost odmítnutí oprávněného uživatele při použití levého prostředníčku/prsteníčku.

$$FRR.levý.Uk = \frac{počet\ nespráv.odmít.Uk\ levé\ ruky}{počet\ všech\ pokusů\ o\ ident.Uk\ levé\ ruky} \cdot 100\% = \frac{3}{45} \cdot 100\%$$
$$= 6{,}66\%$$

$$FRR.levý.Pr,Ps = \frac{počet\ nespráv.odmít.Pr,Ps\ levé\ ruky}{počet\ všech\ pokusů\ o\ ident.Pr,Ps\ levé\ ruky} \cdot 100\%$$
$$= \frac{1}{45} \cdot 100\% = 2{,}22\%$$

FRR pro pravé ukazováčky a pravé prostředníčky/prsteníčky vyšlo 4,44% a 2,22%, což značí, že je hypotetická 4,44% pravděpodobnost odmítnutí oprávněného uživatele při použití pravého ukazováčku a hypotetická 2,22% pravděpodobnost odmítnutí oprávněného uživatele při použití pravého prostředníčku/prsteníčku.

$$FRR.pravý.Uk = \frac{počet\ nespráv.odmít.Uk\ pravé\ ruky}{počet\ všech\ pokusů\ o\ ident.Uk\ pravé\ ruky} \cdot 100\% = \frac{2}{45} \cdot 100\%$$
$$= 4{,}44\%$$

$$FRR.pravý.Pr,Ps = \frac{počet\ nespráv.odmít.Pr,Ps\ pravé\ ruky}{počet\ všech\ pokusů\ o\ ident.Pr,Ps\ pravé\ ruky} \cdot 100\%$$
$$= \frac{1}{45} \cdot 100\% = 2{,}22\%$$

Z celkového počtu měření vychází, že nejvyšší hypotetickou pravděpodobnost odmítnutí oprávněného uživatele je, když k identifikaci použijeme ukazováček levé ruky, která se pohybuje kolem cca 6,66%. Nejnižší hypotetická pravděpodobnost odmítnutí oprávněného uživatele je, když k identifikaci použijeme libovolný prostředníček nebo prsteníček libovolné ruky. Zde se hypotetická pravděpodobnost vždy pohybuje okolo 2,22%.

Výsledek není moc prokazatelný, ale mnohem větší množství otestovaných přístupů přes terminál by přineslo mnohem přesnější hodnoty.

6.2 Měření shody otisků prstů

V původním plánu byla praktická část diplomové práce zaměřena na snímání krevního řečiště rodinných příslušníků, ale z důvodů popsaných v kapitole 7, bylo vybráno snímání otisků prstů (terminál je multimodální) zaměřené převážně na rodinné příslušníky. Pro tuhle změnu byl použit terminál MorphoSmart Finger VP od stejného výrobce, dodávaný spolu s terminálem MorphoAccess VP. Pro tento terminál, který se zapojuje přes USB, je použitý jiný program MorphoEnroll. Ten na rozdíl od programu Easy2Enroll s terminálem funguje.

Jednotlivé snímky byly získány programem MorphoEnroll. Pomocí tohoto programu a terminálu MorphoSmart Finger VP bylo pořízeno 12 snímku od každého jedince. Jednalo se o 6 snímků levé ruky a 6 snímků pravé ruky, z nichž byly 3 snímky palce a 3 snímky ukazováčku každé ruky. Snímky byly potom převedeny z formátu RAW[14] do formátu BMP. Celkově bylo od každé osoby získáno 24 obrázků v obou formátech. Tyto snímky byly následně upraveny a porovnány v programu eFinger. Program eFinger byl zvolen, protože program MorphoEnroll neumožňuje přímé srovnání dvou snímků pro zjištění shody dvou snímků.

[14] RAW – třída souborových formátů – slovíčko raw z anglického jazyka znamená v češtině nezpracovaný.

6.2.1 Vytvoření databáze otisků prstů

Pro získání snímků otisků prstů byl použit terminál MorphoSmart VP (Obr. 37) a program MorphoEnroll. Terminál se k počítači připojuje přes USB a pro svoji funkci vyžaduje instalaci ovladačů MorphoSmart USB Driver.

Obr. 39 MorphoSmart VP [37]

Pro měření bylo vybráno 16 lidí. Z toho 7 žen a 9 mužů. Rodinných příslušníků bylo 9 a 7 lidí bez rodinného vztahu. V 1. rodinné skupině byli 4 lidé (2 sourozenci, jejich matka a jejich bratranec). V 2. rodinné skupině byli 3 lidé (2 sourozenci a jejich 1 sestřenice). V 3. rodinné skupině byli 2 lidé (dva bratři). Všech 16 lidí nebylo záměrně uváděno pod vlastním jménem, ale všichni byli uváděni pod názvem subjekt1 až subjekt16 (V tabulkách jako S1 až S16).

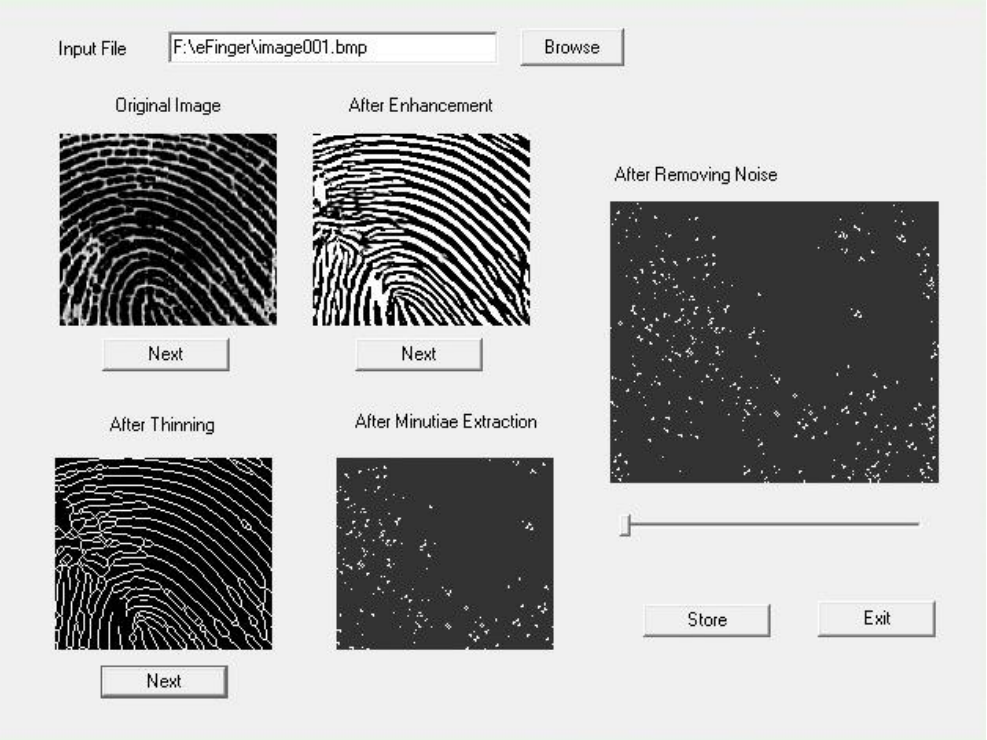
Každému jedinci byly udělány 3 snímky každého prstu. Mezi vybranými prsty byl levý ukazováček a palec a pravý ukazováček a palec. Celkově tedy 4 prsty každého jedince po 3 snímcích. Pro práci bylo tedy k dispozici 192 snímků, z toho 108 rodinných příslušníků.

Pro následovné srovnání v programu eFinger byly vybrány vždy jen 2 nejlepší a nejpodobnější vzorky, na kterých bylo zřetelně vidět celý prst, co nejvíce markantů papilárních linií a smyčky uprostřed prstu.

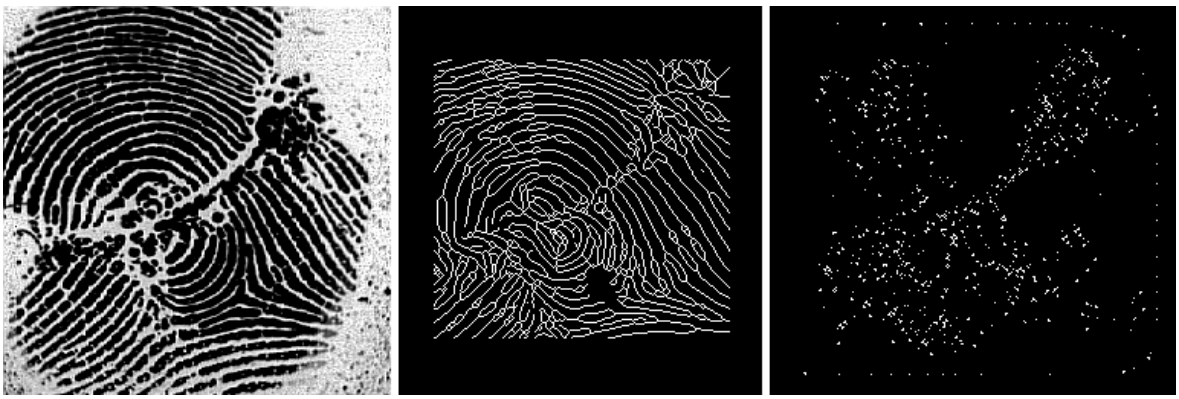
Snímky byly pořízeny ve dvou formátech (RAW a BMP). Celá databáze snímků otisků prstů bude v budoucnu přístupná pro možné využití a další měření. Ve škole má vzniknout laboratoř jen pro biometrické systémy a myslím, že tyto snímky mohou být v budoucnu použitelné. Hlavně z důvodu, že se jedná převážně o snímky rodinných příslušníků.

6.2.2 Porovnání shody otisků prstů v programu eFinger

Vzhledem k tomu, že nebyl ve škole nalezen fungující program pro porovnávání shody otisků prstů, bylo sáhnuto po volně přístupném programu eFinger z internetu. Nejprve byly snímky otisků prstů pořízeny přes terminál MorphoSmart VP. Tyto snímky byly následně uloženy na disk, ze kterého byly nahrány do programu eFinger. Na hlavní liště byla vybrána položka **Database – Add New Image** pro uložení snímků do databáze. V novém okně byl vybrán vždy jeden otisk po druhém, u kterého byly extrahovány body a otisk byl uložen do databáze (Obr. 38).

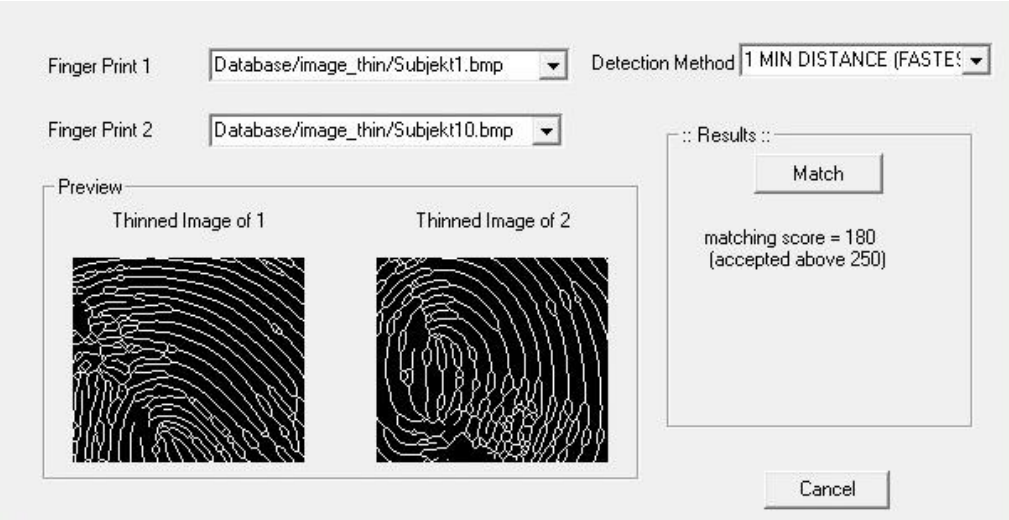


Obr. 40 Extrakce bodů z otisku prstu



Obr. 41 Ukázka průběh extrakce otisků prstů

Když byly převedeny všechny otisky, byla vybrána položka **Match – Already in DB** na hlavní liště (Obr. 40). Poté byly v kolonkách **Finger Print 1** a **Finger Print 2** vybrány otisky, které měly být vzájemně porovnány. A v pravé kolonce **Detection Method** byla vybrána metoda, v případě této práce **MIN DISTANCE**, protože se jednalo o nejrychlejší a nejprůkaznější metodu a data ostatních dvou metod nedávaly velký smysl.



Obr. 42 Vzájemné porovnání dvou otisků prstů

Otisky mezi sebou byly porovnávány následovně. Od každého subjektu (v tabulkách jako S1 až S16) byly srovnávány vždy 2 snímky stejného prstu (snímek 1 a snímek 2). Porovnávání otisků probíhalo mezi dvěma různými lidmi (např. S3 a S12) a mezi sebou samotným (např. S5 a S5). V tabulce 1 to bylo v pořadí (snímek 1 – snímek 1, snímek 1 – snímek 2), v tabulce 2 (2-2, 2-1), v tabulce 3 (2-1, 1-1) a v tabulce 4 (2-1, 2-2). V dalších tabulkách je rozdělení na muže, ženy a rodinné příslušníky.

V tabulkách jsou některé kolonky barevně zvýrazněné. Jedná se o jednotlivé skupiny rodinných příslušníků. Žlutá barva označuje 1. rodinnou skupinu (2 sourozenci, jejich matka a jejich bratranec), modrá označuje 2. rodinnou skupinu (2 sourozenci a jejich sestřenice) a zelená označuje 3. rodinou skupinu (dva bratři).

Ženy jsou vedeny pod označením S1, S3, S4, S5, S6, S8, S15 a muži jsou vedeny pod označením S2, S7, S9, S10, S11, S12, S13, S14 a S16.

6.2.3 Výsledky porovnání shody otisků prstů

V tabulce 1 (Tab. 14) byly porovnávány snímky 1 a snímky 2 (mezi sebou samotným) a snímky 1 a snímky 1 (pro dva různé subjekty). V tabulce 2 (Tab. 15) to byly 2-1 a 2-2.

Tab. 14 Tabulka 1 v pořadí 1-2 a 1-1

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
S1	456	222	236	234	205	226	213	184	242	180	193	186	187	225	203	169
S2	212	463	234	207	187	238	195	182	243	162	191	186	192	205	174	180
S3	236	249	451	206	195	212	191	189	223	164	187	189	171	206	154	184
S4	228	240	237	452	212	216	239	201	254	202	178	193	187	241	190	168
S5	259	239	241	238	453	247	235	227	248	205	165	165	195	188	166	165
S6	219	232	208	187	208	451	206	186	230	174	185	192	158	202	141	176
S7	240	222	211	241	213	246	436	230	258	232	172	177	191	211	144	161
S8	225	224	235	238	242	231	214	455	240	217	165	175	183	189	172	179
S9	216	243	222	215	197	235	222	196	744	191	177	173	197	235	189	160
S10	226	202	199	254	230	213	319	229	249	478	156	183	233	206	201	150
S11	148	146	142	141	138	145	137	142	136	136	449	149	132	129	121	235
S12	158	158	163	168	149	165	155	161	147	171	192	450	168	151	157	218
S13	225	227	204	232	228	185	223	203	235	246	146	177	463	217	240	142
S14	200	184	184	192	153	186	172	152	210	169	161	186	184	560	210	145
S15	234	228	201	245	205	187	201	200	224	200	141	171	234	217	487	139
S16	148	159	161	153	153	156	147	169	141	142	185	184	137	124	129	444

Tab. 15 Tabulka 2 v pořadí 2-1 a 2-2

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
S1	460	235	217	217	195	190	231	228	211	232	200	202	145	195	181	199
S2	207	450	239	228	186	177	230	240	213	208	187	206	185	219	194	203
S3	246	259	455	233	201	193	241	247	222	213	186	195	165	200	214	195
S4	218	255	207	456	194	184	241	222	241	217	179	199	164	202	189	189
S5	243	231	240	243	461	242	242	230	234	237	163	176	169	152	230	186
S6	229	219	235	225	245	462	240	216	224	233	163	166	170	126	208	180
S7	214	237	200	215	193	191	459	219	214	216	193	204	163	190	171	211
S8	226	260	231	218	191	183	228	456	254	225	178	209	174	216	190	194
S9	211	169	253	239	191	182	229	238	779	221	180	199	206	238	210	201
S10	236	243	235	224	217	201	240	233	230	454	191	199	159	177	195	190
S11	152	143	149	141	137	138	148	140	138	147	463	227	127	145	132	240
S12	169	167	169	168	159	150	170	175	166	171	191	474	195	141	167	235
S13	167	214	200	193	203	197	185	202	244	182	136	204	452	244	250	185
S14	156	185	159	158	123	103	157	172	190	137	169	186	219	508	230	188
S15	200	229	220	213	201	178	196	224	234	208	162	191	202	300	451	196
S16	176	177	176	168	172	167	185	173	177	168	186	193	179	147	179	446

V tabulce 3 (Tab. 16) byly porovnávány snímky 1 a snímky 1 (mezi sebou samotným) a snímky 1 a snímky 2 (pro dva různé subjekty). V tabulce 4 (Tab. 17) to byly 2-2 a 2-1.

Tab. 16 Tabulka 3 v pořadí 1-1 a 1-2

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
S1	1k	305	237	248	199	180	237	228	258	219	186	210	200	228	208	197
S2	218	1k	218	261	197	188	246	235	240	205	189	212	191	205	181	189
S3	210	246	1k	244	191	182	231	218	226	203	181	207	183	201	181	190
S4	247	242	245	1k	215	201	239	246	225	248	183	193	197	222	228	191
S5	241	248	242	244	1k	224	248	226	235	233	166	179	171	152	229	193
S6	207	240	197	217	187	1k	244	245	230	208	189	198	155	198	182	194
S7	235	249	247	230	216	210	1k	247	245	223	170	188	169	164	209	177
S8	229	251	246	243	240	215	238	1k	236	229	162	185	157	157	230	184
S9	206	177	245	237	184	176	227	257	1k	216	181	198	202	248	211	198
S10	229	245	227	200	219	222	222	236	239	1k	158	186	199	176	236	184
S11	152	144	144	142	144	141	145	139	135	147	1k	244	131	141	125	241
S12	175	151	169	149	156	148	163	162	147	162	196	1k	175	141	158	241
S13	198	236	220	242	208	225	191	233	248	218	141	183	1k	210	276	176
S14	180	207	179	179	146	138	184	194	205	180	169	187	218	1k	238	173
S15	181	238	218	208	208	190	188	214	250	194	145	200	267	279	1k	181
S16	152	149	152	158	163	150	165	153	144	154	186	185	154	123	138	1k

Tab. 17 Tabulka 4 v pořadí 2-2 a 2-1

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
S1	1k	223	217	217	202	218	214	188	211	182	198	207	165	206	140	172
S2	243	1k	224	212	200	229	205	203	218	193	182	181	196	210	182	171
S3	241	250	1k	225	256	209	234	246	207	188	199	181	191	174	224	165
S4	250	273	249	1k	194	234	206	193	243	161	185	174	193	207	165	181
S5	247	253	247	250	1k	225	243	235	230	202	172	171	182	181	166	175
S6	226	231	233	238	236	1k	236	212	215	209	169	163	195	165	154	161
S7	220	229	215	200	198	241	1k	188	214	181	187	195	161	193	146	189
S8	229	237	220	213	192	235	229	1k	196	248	192	179	188	196	220	164
S9	249	247	226	218	205	240	224	202	1k	192	175	172	203	233	192	163
S10	232	214	213	229	203	219	291	229	229	1k	190	190	186	211	137	174
S11	142	144	143	147	139	150	137	141	138	137	1k	233	244	128	135	127
S12	174	178	174	166	159	166	163	169	164	170	189	1k	274	172	149	182
S13	235	222	211	243	201	178	191	184	240	222	141	183	1k	251	218	157
S14	179	164	159	175	122	161	131	131	201	146	161	185	182	1k	236	153
S15	234	211	208	231	207	200	213	193	236	196	155	178	212	202	1k	152
S16	171	167	169	171	177	172	161	173	173	173	190	201	168	146	167	1k

U použité metody MIN DISTANCE je shoda hodnocena od 0 do 1000, kdy 1000 je maximální shoda, tedy 100%. V programu jsou hodnoty pod 250 brány jako nevyhovující. Hodnoty nad 250 jsou už nějakým způsobem brány jako vyhovující s minimálním počtem shodujících se markantů, které stačí pro minimální základní shodu, která je akceptována.

Při porovnání dvou rozdílných snímků stejného prstu u jednoho subjektu bylo dosaženo vždy hodnot nad 250 (minimální hodnota pro shodu). U všech subjektů bylo splněno minimální kritérium shody (průměr okolo 480) pro akceptovatelnost. Nejvyšší shody bylo dosaženo u subjektu9 (744 a 779). Při porovnání dvou stejných snímků stejného prstu u jednoho subjektu bylo dosaženo vždy hodnoty 1000, což značí 100% shodu.

Nízké hodnoty (při porovnání dvou rozdílných snímků stejného prstu u jednoho subjektu) okolo 450 jsou dány tím, že při pořizování otisků prstů se musí postupovat systematicky a snažit se pořídit snímek co nejvíce shodný. Prst nesmí být pootočen, nadzvednut, málo přitlačen, moc přitlačen apod. Prst by měl být vycentrovaný nejlépe na střed a bez pohybu (což se u většiny subjektů i na několikátý pokus zdálo jako nemožné), kde se vykytuje nejvíce markantů a smyček. Pohyb po průhledné ploše, pod kterou se nachází snímač, ve většině případů sroloval papilární linie a výsledný snímek byl nečitelný. V takových to případech mizí rozdíly mezi papilárními liniemi a prohlubněmi mezi nimi.

Tab. 18 Tabulka shody mezi ženami

	S1	S3	S4	S5	S6	S8	S15
S1	1000	217	217	202	218	188	140
S3	241	1000	225	256	209	246	224
S4	250	249	1000	194	234	193	165
S5	247	247	250	1000	225	235	166
S6	226	233	238	236	1000	212	154
S8	229	220	213	192	235	1000	220
S15	234	208	231	207	200	193	1000

Pro měření bylo k dispozici 7 žen a 9 mužů. Z tabulky (Tab. 18), ve které jsou uvedeny pouze ženy, lze vyčíst, že nejvyšší shody okolo hodnoty 250 a výše dosáhly tři subjekty. Nejvyšší shody dosáhl subjekt5, a to ve třech srovnáních v rozmezí hodnot 247 až 250. Druhé nejvyšší shody ve dvou srovnáních dosáhl subjekt3 (246 a 256) a subjekt4 (249 a 250). Průměrné nejvyšší shody vůči ostatním dosahoval subjekt3 s hodnotou 343

a subjekt5 s hodnotou 338. Nejnižší průměrné shody vůči ostatním dosahoval subjekt1 s hodnotou 311 a subjekt15 s hodnotou 324. U všech subjektů přesahovala průměrná shoda hodnotu 300.

Tab. 19 Tabulka shody mezi muži

	S2	S7	S9	S10	S11	S12	S13	S14	S16
S2	1000	205	218	193	182	181	196	210	171
S7	229	1000	214	181	187	195	161	193	189
S9	247	224	1000	192	175	172	203	233	163
S10	214	291	229	1000	190	190	186	211	174
S11	144	137	138	137	1000	233	244	128	127
S12	178	163	164	170	189	1000	274	172	182
S13	222	191	240	222	141	183	1000	251	157
S14	164	131	201	146	161	185	182	1000	153
S16	167	161	173	173	190	201	168	146	1000

Z tabulky (Tab. 19), ve které jsou uvedení pouze muži lze vyčíst, že nejvyšší shody okolo hodnoty 250 a výše dosáhly čtyři subjekty. Nejvyšší shody dosáhl subjekt10, a to v jednom srovnání, jehož hodnota byla 291. Druhé, třetí a čtvrté nejvyšší shody dosáhl subjekt12, subjekt13 a subjekt9 každý po jednom srovnání v hodnotách 274, 251 a 247. Průměrné nejvyšší shody vůči ostatním dosahoval subjekt10 s hodnotou 298 a subjekt9 a subjekt13 se shodnou hodnotou 289. Nejnižší průměrné shody vůči ostatním dosahoval subjekt11 s hodnotou 254 a subjekt14 s hodnotou 258. U všech subjektů nepřesáhla průměrná shoda hodnotu 300.

Ze všech získaných výsledků vyplývá, že ženy mezi sebou i v menším počtu (7) mají vyšší průměrnou shodu, která přesahovala vždy přes hodnotu 300, než muži, kterých bylo více (9) a shoda dosahovala max. do hodnoty 300. I mezi jednotlivci měly ženy mezi sebou vyšší výsledky, než muži. Kdyby bylo k dispozici mnohem více lidí a bylo by to genderově vyrovnanější, možná by se rozdíly ještě více prohloubily, vyrovnaly nebo naopak úplně otočily.

Tab. 20 Tabulka shody rodinných příslušníků

	S2	S10	S4	S7	S15	S5	S6	S12	S13
S2	1000	193							
S10	214	1000							
S4			1000	206	165				
S7			200	1000	146				
S15			231	213	1000				
S5						1000	225	171	182
S6						236	1000	163	195
S12						159	166	1000	274
S13						201	178	183	1000

Do tabulky (Tab. 20) s rodinnými příslušníky byly vybrány 3 skupiny. Zeleně označená skupina byly dva sourozenci, resp. bratři. Vzájemná podobnost u subjektu2 (193) nepřekročila hodnotu 200, u subjektu10 (214) byla vyšší, kdy překročila hodnotu 200. V modře označené skupině se nacházeli dva sourozenci (bratr - subjekt7 a sestra - subjekt15) a sestřenice (subjekt4). Zde jsou hodnoty trochu vyšší, než u předchozí skupiny. Nejvyšší shody dosahuje subjekt15, který se vůči dalším dvěma pohybuje nad hodnotou 200 (231 a 213). U subjektu4 (206 a 165) a subjektu7 (200 a 146) v jednom případě u obou subjektů hodnota přesáhla 200. Průměrná hodnota shody byla nejvyšší opět u subjektu15 (148), subjektu4 (123,66) a subjektu7 (115,33). Poslední žlutá skupina obsahovala nejvíce zástupců. Přesněji to byli dva sourozenci (bratr - subjekt13 a sestra - subjekt6), jejich matka (subjekt5) a jejich bratranec (subjekt12). Nejvyšší hodnoty dosáhl subjekt12 s hodnotou 274 (shoda mezi bratrancem a bratrem). Průměrně nejvyšší shody dosáhl subjekt12 (149,75), následovaný subjektem6 (148,5), subjektem5 (144,5) a subjektem13 (140,5).

Změřená data nejsou průkazná. Jestli existuje nějaká hypotetická shoda mezi rodinnými příslušníky, muselo by být pořízeno mnohem větší množství dat, které by mohly nějakou podobnost prokázat a použita výkonnější a přesnější kriminalistická technika. Ale osobně si myslím, že i s mnohem větším počtem rodinných příslušníků se neprokáže o mnoho vyšší shoda, která by nebyla i mezi ostatními lidmi mimo rodinu.

7 PŘECHOD Z KREVNÍHO ŘEČIŠTĚ NA OTISKY PRSTŮ

Pro měření praktické části mojí diplomové práce byl vybrán terminál MorphoAccess VP. Tento terminál byl vybrán ve výběrovém řízení a do školy dodán 24. ledna. Po prvních pár pokusech o získání snímku krevního řečiště, bylo zjištěno, že terminál tyto snímky ukládá do svojí vnitřní paměti, ke které není žádný přístup (v plánu bylo vložit snímky krevního řečiště do diplomové práce a různě s nimi pracovat a hlavně u nich měřit shodu podobnosti u rodinných příslušníků). Na tento problém byli nasazeni dva programátoři, kteří by se pokusili o prolomení přístupu do paměti. Později se zjistilo, že by to hypoteticky šlo, ale na vytvoření programu, který by umožňoval přístup do paměti, nebylo dostatek času. Po konzultacích s několika programátory mě bylo shodně řečeno, že takový to program by trvalo vytvořit minimálně půl roku s menší skupinou programátorů. Kvůli časové náročnosti o pokus vytvořit vlastní program pro získání snímků jsem se obrátil s problémem na našeho dodavatele firmu Abbass. U nichž jsem se snažil o získání programu, který by umožňoval data získat. Ukázalo se, že takovým to programem nedisponují. Se stejným dotazem jsem se obrátil na jinou firmu (Movibio) dodávající tyto přístroje na český trh. Bylo mi odpovězeno, že je tento terminál pro zamýšlené (studijní) užití absolutně nevhodný a že mi nemůže moc pomoci, protože to nejde, resp. výrobce tyto informace neposkytuje. Oznámili mi, že se mám informovat u našeho dodavatele. Zde jsem také nepochodil.

V další emailu jsem komunikoval s pracovníkem firmy Movibio, kterému jsem sdělil, že mám k dispozici program Easy2Enroll, který je v tomhle směru je velmi omezený. Ukazuje jen otisky prstů při registraci do systému a základní informace o uživatelích. Z odpovědi jsem se dozvěděl, že žádný z výrobcem dodávaných programů pro tuto čtečku takové informace neposkytuje a vzhledem k účelu, ke kterému čtečka slouží, by nemělo ani žádný smysl. Pro výrobce je důležitá také ochrana důvěrných informací o snímači a algoritmu, takže nejsou ochotni uvolnit ani pro takové studijní využití. A že ani programátor nemůže moc pomoci, protože není možné se k těmto informacím dostat ani přes dodávané SDK. Zpracování dat probíhá uvnitř terminálu a tato data se vůbec k PC nedostanou.

Po dalším dotazu, zda vůbec neexistuje další žádná metoda, jak data z paměti získat, mě bylo odpovězeno, že ne. Pokud výrobce nějaký takový způsob pro testování má, rozhodně jej neprozradí, o což se už v minulosti pokoušeli, ale nikdy neuspěli.

Po několika pokusech jsem se znova obrátil na jednoho ze zaměstnanců firmy Abbas s problémem, že žádným způsobem nelze získat data z paměti. Byl jsem pověřen zjistit, jestli by výrobce (Morpho) nebyl ochoten pomoci s tímto problémem. Např. možnost odkoupení přístroje, který data z terminálu získává, nebo zda by nebyl ochoten poradit jakým způsobem data z terminálu získat. Pokud by toto nebylo možné, jestli by neměli k dispozici databázi snímků krevního řečiště.

V emailu mě bylo odpovězeno, že z paměti terminálu snímky krevního řečiště nelze nijak získat. Byly mi zaslány příkazy sloužící k získání snímků přes SDK, ale bohužel ani s poskytnutými příkazy jsem snímky nezískal. Žádnou databázi nemají k dispozici ve firmě Abbass ani v Morphu. Byl jsem odkázán na odbornou literaturu.

Současně s tím jsem psal email do krajské nemocnice Tomáše Bati ve Zlíně na oddělení zobrazovacích metod, zda by nebyla možnost nasnímat prsty jednotlivých osob, kolik by snímání stálo a jak dlouho by trvalo. Bylo mě odpovězeno, že na oddělení zobrazovacích metod by to nebylo možné, ale že se mám dotázat na jiném oddělení. Potřeboval bych souhlas vedení nemocnice, jehož získání může trvat několik týdnů. Po dohodě s vedoucím jsme tuto možnost z časových důvodů vyloučili.

Po pokusech o získání snímků krevního řečiště jakýmkoliv způsobem, bylo po konzultaci domluveno, že v praktické části bude měřena citlivost (threshold) pro snímání a porovnávána na různých hodnotách pro rodinné příslušníky. Z toho měření nakonec také sešlo, protože při pokusu o změnu thresholdu (v programu Easy2Enroll pojmenovaný jako Minimum Level Of Quality For Enrolment) vyskakovala chybová hláška, kterou nebylo možno žádným způsobem odstranit. Po opětovném kontaktování dodavatele mě bylo odpovězeno, že komunikovali přímo s Morphem, a že verze programu, kterou mě poskytli, byla beta verze (E2E1.0.0.7b). Ale ani nová verze bohužel nic neopravila a chybová hláška se stále objevovala.

Bylo rozhodnuto, že pojedeme přímo do Brna, kde sídlí firma Abbass. Důvodem byla stále se objevující chybová hláška při změně thresholdu i jiných hodnot. Ještě před odjezdem jsem se zeptal přes email, zda se budou v danou dobu, kdy jsme měli přijet, ve firmě nacházet. V plánu bylo vzít notebook i terminál krevního řečiště. Bylo mi odpovězeno, že v danou dobu se v kancelářích nebude nacházet pracovník, se kterým jsem již dříve komunikoval ani nikdo jiný. Problém nebyl ani tak v době, kdy jsme tam chtěli přijet, ale v tom, že zaměření firmy je jiné (nejsou programátoři) a s tímto problémem mě nedokážou pomoci.

Po rozhodnutí vedoucího diplomové práce byla v práci zpracována problematika měření shody snímků otisků u rodinných příslušníků místo měření shody krevního řečiště. Morpho dodává terminál MorphoAccess VP a MorphoSmart VP jako kompletní balení, proto pro snímání otisků prstů mohl být použit terminál MorphoSmart VP, který byl pro tento účel použit.

Ačkoliv jsem s terminálem strávil několik měsíců, psal do několika dodavatelských firem, psal do Morpha ve Francii, žádným způsobem se mě nepovedlo zjistit, zda existuje nějaký přístup k těmto datům. Oficiálně asi existuje nějaké zařízení, které tohle umožňuje, ale to slouží jenom pro techniky nebo vývojáře přímo z firmy Morpho. Bylo mě potvrzeno z několika zdrojů, že se pokoušeli získat tohle zařízení, ale výrobce to neumožňuje, protože přes toto zařízení lze zjistit i používané algoritmy, které získávají a zpracovávají data.

Tento terminál nic méně nemohu doporučit ke studijním účelům, protože stěžejním prvkem tohoto zařízení je práce s krevním řečištěm, ale když neexistuje žádný nám povolený přístup k těmto snímkům, nelze s daty ani jinak pracovat. Jediné dva dostupné programy Easy2Enroll a MorphoEnroll neumožňují ani žádným způsobem porovnávat např. podobnost krevního řečiště dvou nebo více vzorků.

8 ÚLOHA PRO LABORATOŘE

a) Praktická část

1. Seznamte se hardwarovým připojením čtečky MorphoAccess VP do přístupového systému tvořeném čtečkou od Safran Morpho, programem Easy2Enroll, PC a síťovým kabelem.
2. Zapněte program Easy2Enroll. Založte si nový účet. Napravo ve sloupci vybereme **Add** -> typ instalace **Access Database** -> název databáze **New Installation 1** -> zaškrtneme všechny dny -> **Confirm**.
3. Otevřete si položku **New Installation 1** -> klikněte na **Open** -> vyberte **Administrator** a potvrďte **OK**. Vyskočí okno, kde si vytvořte vhodné administrátorské heslo a spusťte program.
4. Popište postup u bodu 2. a 3. A doplňte o příslušné obrázky.
5. Spusťte program Easy2Enroll. Vyberte jazyk **English** a potvrďte **OK**. Vyberte si svůj již vytvořený účet **New Installation 1** -> klikněte na **Open** -> vložte Vámi vytvořené administrátorské heslo a klikněte na OK. Tím se dostanete na úvodní stranu programu.
6. Připojte čtečku MorphoAccess VP. Vlevo klikněte na **Morpho readers** -> **Add a reader**. Objeví se okno se 4 záložkami. Popište funkce záložek Configuration, Network, Access control, Messages.
7. Propojte čtečku s programem Easy2Enroll za pomocí síťového kabelu Ethernet. K dispozici máte IP adresu terminálu (134.1.32.214), IP adresu brány (134.1.6.20), masku subsítě (255.255.240.0).
8. Popište postup u bodu 5. až 7. A doplňte o příslušné obrázky.
9. Po nainstalování programu, založení nové databáze a účtu a připojení funkční čtečky zkuste vytvořit alespoň tři záznamy.
10. Vytvořte záznam prsteníčku levé ruky přes Enroll a finger a záznam prostředníčku a ukazováčku levé ruky přes Enroll two fingers a záznam ukazováčku pravé ruky přes Enroll a finger a záznam prostředníčku a prsteníčku pravé ruky přes Enroll two fingers. Celkově budou vytvořeny 4 záznamy. Zaznamenejte úspěšnost a kvalitu skóre do tabulky.

11. Popište postup u bodu 9. a 10. A doplňte o příslušné obrázky

b) Teoretická část

12. Popište základní funkce programu Easy2Enroll. Settings, Schedule and Access Rights, Users, Events, Map, Administration.
13. Popište typy cév v lidském těle.
14. Napište využití krevního řečiště v policejně-soudních a komerčně-bezpečnostních aplikacích.
15. Popište reflexivní a transmisivní metodu pro snímání krevního řečiště.
16. Jaké jsou 4 oblasti snímání krevního řečiště na ruce. Popište je.
17. K jakým účelům může sloužit snímač krevního řečiště.
18. Popište cévní systém lidského těla.
19. Uveďte příklady metod biometrické autentizace.
20. Vysvětlete pojmy verifikace a identifikace.

ZÁVĚR

V dnešní době je pojem bezpečnost spojována s mnoha obory. Jedná se hlavně o obory zabývající se ochranou objektů, kriminalistickou činností apod. Na tato dvě odvětví je zaměřena i tato práce. V oborech, které jsou zaměřeny na ochranu objektů, jsou v kurzu bezpečnostní systémy založené na biometrických charakteristikách lidí a jejich obliba stále roste. Naopak v kriminalistických aplikacích jsou lidské charakteristiky už dlouhodobým pomocníkem, bez kterých se vyšetřovatelé zločinů neobejdou.

Cílem diplomové práce bylo přednést čtenářům problematiku existujících biometrických metod a uvést zde známé metody, které se běžně používají v policejně-soudních a bezpečnostně-komerčních aplikacích, ale i ty méně používané nebo téměř neznámé. S biometrickými metodami a systémy je úzce spojena i spolehlivost, která je dána hodnotami FAR a FRR. Práce je zaměřena na krevní řečiště a biometrické systémy na snímání krevního řečiště, jejich využití v praxi, popis částí těla, kde je možné krevní řečiště snímat a příklady biometrických systémů, které pro svoji funkci využívají snímání krevního řečiště.

Praktická část je zaměřena na terminál MorphoAccess VP, detailní popis rozhraní, se kterými terminál pracuje, popis možností propojení s počítačem, technický popis uvedený v tabulkách a jeho komunikaci a spolupráci s programem Easy2Enroll.

V praktickém měření byl cílem výpočet chybovosti terminálu MorphoAccess VP a měření shody otisků prstů (původně krevní řečiště) rodinných příslušníků a dalších osob. Pro měření chybovosti bylo k dispozici 30 osob, kdy každá z nich prošla 3x otestováním průchodu přes terminál. Z těchto hodnot vychází, že nejvyšší hypotetickou pravděpodobnost odmítnutí oprávněného uživatele je 6,66% u ukazováčku levé ruky. Nejnižší je 2,22% při použití libovolného prostředníčku nebo prsteníčku libovolné ruky. Pro měření shody otisků prstů byl použit terminál MorphoSmart a programy MorphoEnroll a eFinger. Pro toto měření bylo k dispozici 16 lidí, z toho 9 rodinných příslušníků. Od každého subjektu bylo k dispozici 12 otisků prstů. Do prvních čtyř tabulek bylo uvedeno všech 16 účastníků a měřena shoda každý proti každému, do dalších tabulek byly uvedeni jenom muži, potom jenom ženy a nakonec jen rodinní příslušnici. Z výsledků nelze říct, že mezi rodinnými příslušníky je shoda, která by dokazovala to, že dané dvojice jsou příbuzní. Proto jsou údaje neprokazatelné. S větším množstvím subjektů a testů by hypotetická shoda byla prokazatelnější.

Jako největší problém se ukázala možnost z terminálu získat jakýmkoliv způsobem snímky krevního řečiště. Z důvodů popsaných v kapitole 6.3 se tyto snímky nepodařilo získat. Tento terminál je podle mého názoru pro laboratorní, resp. školní použití zcela nevhodný. Bez snímků krevního řečiště je terminál pouze přístupovým biometrickým systémem, který neumožňuje hlubší pochopení toho, co terminál umí, jak pracuje a jak takové snímky ve výsledku vypadají. Poslední nadějí pro terminál jsou programátoři, kteří by se pokusili nějakým způsobem o prolomení paměti, do které se snímky ukládají. Menší náhradou mohou být otisky prstů, pro které existují určitě lepší zařízení než je MorphoAccess VP. Další problém vidím v programu Easy2Enroll, který vykazoval velkou chybovost. Díky těmto chybám, se kterými mi nepomohli ani oficiální distributoři a technici, nebylo možné program využít na 100%, tak jak by se od oficiálního programu očekávalo. Tento program neobsahoval ani žádnou funkci srovnání dvou snímků.

Pokud se objeví způsob, jak z paměti terminálu snímky získat a bude k dispozici lepší a vybavenější program, stane se z terminálu MorphoAccess VP skvěla a užitečná školní pomůcka, na kterou by šlo vypracovat další bakalářské, diplomové a disertační práce. A splnit všechny podmínky diplomové práce, které se nepovedly v mojí práci.

SEZNAM POUŽITÉ LITERATURY

[1] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Vyd. 1. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

[2] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka: ve forenzních a komerčních aplikacích. Vyd. 1. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.

[3] BLAŽEK, Vladimír a Radek TRNKA. Lidský obličej: Vnímání tváře z pohledu kognitivních, behaviorálních a sociálních věd. Vyd. 1. Praha: Karolinum, 2009. ISBN 978-80-246-1556-1.

[4] LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.

[5] BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.

[6] ARIEB, Elaine Nicpon a Jon MALLATT. Anatomie lidského těla. Vyd. 1. Brno: CP Books, 2005, xvi, 863 s. ISBN 8025100669.

[7] KONVIČKOVÁ, Svatava a Jaroslav VALENTA. Biomechanika srdečně cévního systému člověka. Vyd. 2. Praha: Česká technika - nakladatelství ČVUT, 2006c1997, 275 s. ISBN 80-01-03425-9.

[8] DYLEVSKÝ, Ivan. Lymfa: míza. V Olomouci: Poznání, 2006, 109 s. ISBN 80-86606-42-2.

[9] VACH, Martin. Historie biometrik a jejich využití ve výpočetní technice. In: [online]. Brno [cit. 2014-02-07]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm

[10] SULOVSKÁ, Kateřina. Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu. In: [online]. 2011 [cit. 2014-02-07]. Dostupné z: http://www.posterus.sk/?p=11511

[11] SVOZIL, Lukáš. Aspekty biometrické identifikace osob s využitím rozpoznávání tváře. Zlín, 2009. Dostupné z: http://dspace.k.utb.cz/bitstream/handle/10563/7953/svozil_2009_bp.pdf?sequence=1. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Ing. Rudolf Drga, Ph.D.

[12] KONČICKÝ, Martin. *Biometrický snímač otisku prstů*. Zlín, 2013. Dostupné z: http://dspace.k.utb.cz/handle/10563/24672. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Ing. Rudolf Drga, Ph.D.

[13] STANÍK, Libor. *Biometrické identifikační metody*. Zlín, 2009. Dostupné z: http://dspace.k.utb.cz/handle/10563/8124. Diplomová práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky, Ústav elektrotechniky a měření. Vedoucí práce JUDr. Vladislav Štefka.

[14] ONDRŮŠEK, Roman. *Identifikační biometrické prostředky*. Zlín, 2006. Dostupné z: http://dspace.k.utb.cz/handle/10563/743. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky, Ústav elektrotechniky a měření. Vedoucí práce Ing. Mgr. Milan Kvasnica,CSc.

[15] Biologie: Oběhová soustava člověka [online]. 2013 [cit. 2014-02-20]. Dostupné z: http://www.nabla.cz/obsah/biologie/kapitoly/biologie-cloveka/obehova-soustava-cloveka.php

[16] Oběhová soustava. In: Lidské tělo: Oběhová soustava [online]. 2014 [cit. 2014-02-20]. Dostupné z: http://www.latinsky.estranky.cz/fotoalbum/obehova-soustava/obehova-soustava/hlavni-tepna-rez.png.html

[17] DYLEVSKÝ, Ivan. Funkční anatomie. Vyd. 1. Praha: Grada Publishing, 2009, 532 s. ISBN 978-80-247-3240-4.

[18] MACHOVÁ, Jitka. Biologie člověka pro učitele. Vyd. 1. Praha: Karolinum, 2002, 269 s. ISBN 80-7184-867-0.

[19] ADAMEC, Lukáš. Srovnávací testy vybraných biometrických zařízení. Brno, 2009. Dostupné z: http://is.muni.cz/th/208425/fi_b/Srovnavaci_testy_vybranych_biometrickych_zarizeni.pdf. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce doc. RNDr. Václav Matyáš, M.Sc., Ph.D.

[20] OLZAK Tom. Reduce multi-factor authentication costs with behavioral biometrics. TechRepublic. [online]. 2007 [cit. 2014-02-20]. Dostupné z: http://www.techrepublic.com/article/reduce-multi-factor-authentication-costs-with-behavioral-biometrics/6150761

[21] JORGENSEN, Z a T. YU. On Mouse Dynamics as a Behavioral Biometric for Authentication. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. 2011; 476-482

[22] HALADOVÁ, Eva a Ludmila NECHVÁTALOVÁ. Vyšetřovací metody hybného systému. Vyd. 2., nezměn. Brno: Národní centrum ošetřovatelství a nelékařských zdravotnických oborů, 2003, 135 s. ISBN 8070133937.

[23] BITTO, Ondřej. User Authentication Based On Hands. Brno, 2005. Dostupné z: http://is.muni.cz/th/72535/fi_b/. Diplomová práce. Fakulta informatiky Masarykovy univerzity.

[24] BITTO, Ondřej. Biometriky nejen v pasech (1.). In: Lupa.cz [online]. 2005 [cit. 2014-03-02]. Dostupné z: http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/

[25] OLEVSKI, Slobodan. Poroskopie jako metoda identifikace osob. Kriminalistický sborník, 2010, č. 5. S. 52-53

[26] AHMED, Awad E. Ahmed a Issa TRAORÉ. A New Biometrics Technology based on Mouse Dynamics. IEEE Transactions on Dependable and Secure Computing. 2007; 4: 165-179.

[27] NAZAR, Akif, Issa TRAORÉ a AHMED Awad E. Ahmed Inverse Biometrics for Mouse Dynamics. International Journal of Pattern Recognition and Artificial Intelligence. 2008; 22: 461-495.

[28] Kriminalistické metody. Policiebrusperk.estranky.cz [online]. 2013 [cit. 2014-03-02]. Dostupné z: http://www.policiebrusperk.estranky.cz/clanky/kriminalisticke-metody.html

[29] ŠČUREK, Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. [online]. Ostrava: VŠB TU Ostrava, 2008 [cit. 2014-03-02]. Dostupné z: http://www.biometrickypodpis.cz/PDF/biometricke_metody.pdf

[30] Fujitsu Palmsecure. Fujitsu [online]. 2014 [cit. 2014-03-04]. Dostupné z: http://www.fujitsu.com/cz/solutions/high-tech/palmsecure/

[31] VÁCLAVÍK, Lukáš. Zapomeňte na otisky prstů. PalmSecure od Fujitsu skenuje žíly v dlani [CeBIT]. In: CNEWS.cz / Notebooky [online]. 2014 [cit. 2014-03-04]. Dostupné z: http://extranotebook.cnews.cz/zapomente-na-otisky-prstu-palmsecure-od-fujitsu-skenuje-zily-dlani-cebit

[32] ROBENEK, Jan. PalmSecure vrací identitu do vašich rukou. In: HW.cz [online]. 2013 [cit. 2014-03-04]. Dostupné z: http://www.hw.cz/teorie-a-praxe/palmsecure-vraci-identitu-do-vasich-rukou.html

[33] JAVŮREK, Karel. Brýle Eyes-On pro rozšířenou realitu umožňují vidět žíly pod kůží [CES]. In: Zive.cz [online]. 2014 [cit. 2014-03-08]. Dostupné z: http://www.zive.cz/bleskovky/bryle-eyes-on-pro-rozsirenou-realitu-umoznuji-videt-zily-pod-kuzi-ces/sc-4-a-172039/default.aspx

[34] Eyes-On vidí nové obzory medicíny. In: GGX [online]. 2014 [cit. 2014-03-08]. Dostupné z: http://www.ggx.cz/2014/01/obzory-nove-mediciny-s-brylemi-eyes-on/

[35] Biometrická čtečka krevního řečiště prstu. In: ADI Global Distribution [online]. 2014 [cit. 2014-03-08]. Dostupné z: http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/web_category_panel3_cenik_asc/D8540430DB7ABA0EC12577880049B08D

[36] MorphoAccess VP Series User Guide

[37] SAFRAN MORPHO. Think Excellence, Choose Multimodality. Francie, 2012. Dostupné z: http://www.morpho.com/IMG/pdf/Multimodality_EN-6.pdf

[38] ARGUS GLOBAL. MorphoAccess VP Series: Multimodal Finger vein & Fingerprint Technology. Francie, 2012. Dostupné z: http://www.argus-global.com/wp-content/uploads/2012/10/Morpho-VP-Series.pdf

[39] SAFRAN MORPHO. MorphoAccess VP Series Product Technical Datasheet. Francie, 2012. Dostupné z: https://www.google.cz/search?q=MorphoAccess_VP_Series_Product_Technical_Datasheet_Rev01_3+filetype%3Apdf&oq=MorphoAccess_VP_Series_Product_Technical_Datasheet_Rev01_3+filetype%3Apdf&aqs=chrome..69i57.14227j0j7&sourceid=chrome&es_sm=93&ie=UTF-8

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

°C	Stupeň celsia
°F	Stupeň fahrenheit
2D	Two-Dimensions
3D	Three-Dimensions
A	Ampér
AC	Alternating Current
ACS	Access Control Systems
AR	Augmented Reality
BMP	Windows Bitmap
CCD	Charge-Coupled Device
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DNA	Deoxyribonucleic Acid
ERR	Equal Error Rate
FAR	False Acceptance Rate
FAT	File Allocation Table
FIR	Far-Infra Red
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FTA	Failure to Acquire
FTE	Failure to Enroll
GB	Gigabyte
GIF	Graphics Interchange Format
GND	Ground

HW	Hardware
ID	Identification
IP	Internet Protocol
IR	Infra Red
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LED	Light-Emitting Diode
MDI	Medium Dependent Interface
MDIX	Medium Dependent Interface Crossover
NIR	Near-Infra Red
OS	Operační systém
PC	Personal Computer
PCA	Principal Component Analysis
PDA	Personal Digital Assistant
PNG	Portable Network Graphics
POE	Power Over Ethernet
RFID	Radio Frequency Identification
RJ45	Registered Jack 45
RNA	Ribonucleic Acid
RS485	Recommended Standard 485
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
Th	Threshold
TIF	Tag Image File
USB	Universal Seriál Bus

V	Volt
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

V příloze se nachází CD:

- fulltext.pdf
- fulltext.docx

PŘÍLOHA P I: TABULKA NAMĚŘENÝCH ÚDAJŮ PRO VÝPOČET SPOLEHLIVOSTI

First Name	Last Name	Ruka	Snímaný prst		Skóre			Ident. 1		Ident. 2		Ident. 3	
			U	Pr,Ps	U	Pr	Ps	U	Pr,sP	U	Pr,Ps	U	Pr,sP
1	Subjekt1	P	ok	ok	96	103	120	A	A	N	A	A	A
2	Subjekt2	L	ok	ok	131	101	108	A	A	A	A	A	A
3	Subjekt3	P	ok	ok	111	121	126	A	A	A	A	N	A
4	Subjekt4	L	ok	ok	120	89	100	A	A	A	A	A	A
5	Subjekt5	P	ok	ok	101	111	100	A	A	A	A	A	A
6	Subjekt6	L	ok	ok	105	102	107	A	A	A	A	A	A
7	Subjekt7	P	ok	ok	80	100	59	A	A	A	A	A	A
8	Subjekt8	L	ok	ok	99	101	117	A	A	A	A	A	A
9	Subjekt9	P	ok	ok	89	112	92	A	A	A	A	A	A
10	Subjekt10	L	ok	ok	88	114	89	A	A	A	A	A	A
11	Subjekt11	P	ok	ok	109	107	121	A	A	A	N	A	A
12	Subjekt12	L	ok	ok	111	134	116	A	A	A	A	A	A
13	Subjekt13	P	ok	ok	122	99	113	A	A	A	A	A	A
14	Subjekt14	L	ok	ok	93	111	100	N	A	A	A	A	A
15	Subjekt15	P	ok	ok	90	117	103	A	A	A	A	A	A
16	Subjekt16	L	ok	ok	79	131	96	A	A	A	A	A	A
17	Subjekt17	P	ok	ok	95	106	92	A	A	A	A	A	A
18	Subjekt18	L	ok	ok	100	97	114	N	A	A	A	A	A
19	Subjekt19	P	ok	ok	127	99	110	A	A	A	A	A	A
20	Subjekt20	L	ok	ok	120	119	123	A	A	A	A	A	A
21	Subjekt21	P	ok	ok	117	85	97	A	A	A	A	A	A
22	Subjekt22	L	ok	ok	109	119	110	A	A	A	A	A	A
23	Subjekt23	P	ok	ok	99	121	115	A	A	A	A	A	A
24	Subjekt24	L	ok	ok	93	103	114	A	A	A	A	A	N
25	Subjekt25	P	ok	ok	104	98	100	A	A	A	A	A	A
26	Subjekt26	L	ok	ok	123	101	90	A	A	A	A	A	A
27	Subjekt27	P	ok	ok	66	99	116	A	A	A	A	A	A
28	Subjekt28	L	ok	ok	97	118	94	A	A	A	A	A	A
29	Subjekt29	P	ok	ok	97	124	95	A	A	A	A	A	A
30	Subjekt30	L	ok	ok	128	126	111	A	A	N	A	A	A