Využití skeneru žilního řečiště v průmyslu komerční bezpečnosti

Daniel Bráník

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Daniel Bráník**
Osobní číslo:	**A11005**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití skeneru žilního řečiště v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. **Seznamte se s problematikou skenování žilního řečiště.**
2. **Analyzujte současné metody skenování žilního řečiště.**
3. **Porovnejte analyzované metody a specifikujte vhodný typ pro průmysl komerční bezpečnosti.**
4. **Navrhněte laboratorní úlohu.**
5. **Experimentálně ověřte navrhovanou laboratorní metodu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RAK, Roman. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.**
2. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**
3. **KOVÁČ, Petr. Ezoterická identifikace, druhy, způsob identifikace, přístrojová identifikační technika,vývoj. Zlín, 2007. 110 s. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.**
4. **RADOMÍR, Ščurek. Biometrické metody identifikace osob v bezpečnostní praxi. [online]. 2008 [cit. 2014-01-28]. Dostupné z: http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf**
5. **JEN-CHUN, Lee. A novel biometric system based on palm vein image. Pattern Recognition Letters. 2012, roč. 33, č. 12.**

Vedoucí bakalářské práce: **Ing. Hana Talandová**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

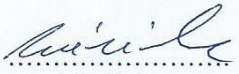
Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové 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

Bakalářská práce pojednává o biometrických systémech, zejména o skeneru žilního řečiště. V úvodní části se práce zabývá objasněním základních pojmů spjatých s biometrikou, principem autentizace, možnosti napadení systému, spolehlivostí a bezpečností systémů. V dalších kapitolách práce zmiňuje historii biometrie a žilního řečiště, princip fungování skeneru žilního řečiště, jeho využití, porovnání s ostatními používanými metodami a jeho výhody a nevýhody. Praktická část se zaměřuje na seznámení s použitým skenerem a jeho vlastnostmi. Dále tato část pojímá laboratorní úlohu a její vypracování.

Klíčová slova:

biometrie, biometrický systém, skener žilního řečiště, identifikační metody, laboratorní úloha

ABSTRACT

The thesis deals with biometric systems, in particular palmvein scanner. In the first part deals with the explanation of basic concepts related to biometrics, authentication principles, the infection of the system reliability and security systems. In other chapters this work refers about the history of biometrics and the palmvein, the operating principle of the scanner palmvein, its usage, compared to other methods which are used for and the advantages and disadvantages. The practical part focuses on the introduction of second-hand scanner and its properties. This section also conceives labs and its elaboration.

Keywords:

biometrics, biometric system, palmvein scanner, identification methods, laboratory task

Rád bych poděkoval vedoucí své bakalářské práce Ing. Haně Talandové za cenné rady, připomínky a odbornou pomoc. Dále děkuji své rodině a partnerce za podporu a trpělivost v době studia.

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

OBSAH

ÚVOD

V rámci této bakalářské práce je zpracována problematika biometrických systémů se zaměřením na skener žilního řečiště. Hlavním cílem těchto systémů je kontrola vstupu, přičemž tyto systémy využívají jedinečných a pokud možno neměnných lidských vlastností. Oblast, která využívá struktury žilního řečiště je v Evropě poněkud novější záležitostí, a proto se tento typ skenerů bohužel často nevyskytuje na zdejším trhu. Právě naopak se na trhu s biometrikou můžete nejčastěji setkat se skenery otisků prstů. Na rozdíl od žilního řečiště jsou skenery otisků prověřeny časem. Dalo by se říct, že žilní řečiště ještě stále čeká na svůj rozmach.

Biometrické skenery bychom v rámci bezpečnostních technologií a systémů mohli začlenit do skupiny přístupových systémů. V této oblasti by skenery mohly zcela nahradit stávající autentizaci předmětem, neboli identifikačními kartami, či tokeny a taktéž autentizaci heslem. Stávající přístupové systémy mají značné nedostatky v bezpečnosti. Hlavním problémem u identifikačních karet, eventuálně hesel, je jejich snadné odcizení nebo duplikování. Závažnost tohoto problému se u biometrických systémů rapidně zmenšuje, protože je obtížné, a někdy i nereálné, duplikovat nebo odcizit lidskou, tedy biometrickou vlastnost.

Biometrie je zajímavou a dosud ne zcela využitou technologií, která by v budoucnu mohla nahradit stávající platební a bankovní systémy jako je tomu v některých japonských bankách.

I. TEORETICKÁ ČÁST

1 BIOMETRIE JAKO VĚDA

Tato kapitola se zaměřuje na bližší seznámení s biometrií jako vědeckou disciplínou. Definuje biometrické systémy, jejich podstatu a obecný princip fungování biometrických systémů. Dále se zaměří na možnosti napadení biometrického systému. Důležitou podstatou je také vymezení základních pojmů, které s biometrickými systémy úzce souvisí. Jejich specifikace nám pomůže lépe chápat souvislosti v dané problematice. Cílem této kapitoly je obeznámit čtenáře s termíny jako jsou identita, identifikace či verifikace.

V současné době obor Bezpečnostní technologie zahrnuje nespočet technických vymožeností, které se díky rozvoji informačních technologií zdokonalují takřka každým dnem. Jejich hlavním úkolem je chránit zdraví a majetek chráněné osoby či osob. Snad ani nemusí být zmiňovat fakt, že nedílný podíl na vývoji bezpečnostních technologií nese stále narůstající kriminalita. Rozpoznávání lidí za pomoci biometrických charakteristik je každodenní záležitostí a je nám známa v různých formách už od pradávna. Náš mozek tedy nahrazuje jakousi databázi. Funguje jako sběrnice dat, která obsahuje ve velké míře hlavně obličeje, tvary postav, a také zaznamenává barvy hlasů našich přátel, kamarádů či známých. Bylo jen otázkou času, kdy se biometrické systémy, které byly zprvu jen součástí smyšlených sci-fi či akčních filmů, začnou používat i v reálném světě. Jejich úroveň se neustále zvyšuje. Musí odpovídat velkému množství požadavků moderní doby, a zároveň naplňovat svůj primární účel.

Označení **biometrie** je složeno ze dvou elementů, původem z řečtiny. Nejprve hovoříme o tzv. „bios“, což v překladu znamená život. Druhým je termín „metron“, jehož význam je měřítko. Jde tedy o složeninu, kterou bychom mohli nahradit českým slovním spojením „měření života“.[1,3,4]

V oboru informačních technologií, respektive v oboru bezpečnostních technologií, vědní obor biometrie, nebo také biometrická identifikace či biometriky představují systém či postup, který napomáhá při rozpoznávání jedinečných biologických charakteristik živé osoby. Tato metoda vychází z faktů, že některé biologické charakteristiky jsou pro každého živého člověka jedinečné a neměnitelné.[1,2,3,4]

1.1 Biometrické systémy

Následující podkapitola specifikuje biometrické systémy. Hlavním cílem biometrických systémů je nahrazení stávajících identifikačních metod. Tyto metody jsou využívány za účelem prokázání identity a v praxi se s nimi můžeme setkat u přístupových

systémů. Přístupové systémy bývají často spojeny s **docházkovými systémy**, které napomáhají k zpřehlednění evidence dění v objektu. Používají se zejména z toho důvodu, že si nepřejeme, aby neoprávněná osoba svým vstupem narušila dění na střeženém místě a eventuálně by tím mohla narušit zájmy, majetek či zdraví osoby oprávněné. Přístupové systémy jsou aplikovány nejčastěji ve středně velkých a velkých firmách, školách, státních institucích apod. Prokázání identity můžeme rozdělit do tří základních skupin, které blíže vymezíme v následující části.

První skupinou pro potvrzení identity tvoří **znalosti.** V tomto případě se jedná o znalost přístupového hesla, PINu či číselného kódu. Výhodou tohoto způsobu identifikace je finanční stránka věci. Tento systém ve velké míře tvoří jen software, který pro přístup požaduje předem registrované heslo. Nevýhodou je, že hesla mohou být prolomena, ztracena či zapomenuta a taktéž odcizena. Častým problémem, hlavně u starších lidí, bývá odcizení PIN kódu či hesla. Hlavním důvodem je to, že si tyto generovaná hesla lidé nepomatují a pro „jistotu“ si je napíší na papír, který může být lehce odcizen.[4]

Další skupinou je **vlastnictví** identifikačního tokenu či karty. U systémů, které využívají přístupové karty, se taktéž můžeme setkat s problémem odcizení karty, zapomenutí karty doma, v obchodě aj., nebo padělání karty neoprávněnou osobou.[4]

V posledním případě jde o **biometrické systémy**. Velkými výhodami je, že biometrické charakteristiky potřebné k identifikaci není možné ztratit nebo zapomenout. Dále biometrie odrazuje útočníky od padělání charakteristik, a to z toho důvodu, že se jedná o složitý proces. Jako další výhody můžeme zmínit, že tyto systémy představují velkou míru komfortu a bezpečí, jelikož si uživatel nemusí nic pomatovat nebo brát se sebou. Nevýhodou je pořizovací cena, která je vyšší než u předchozích dvou identifikačních metod.[1,2,3,4]

1.1.1 Obecný princip biometrického systému

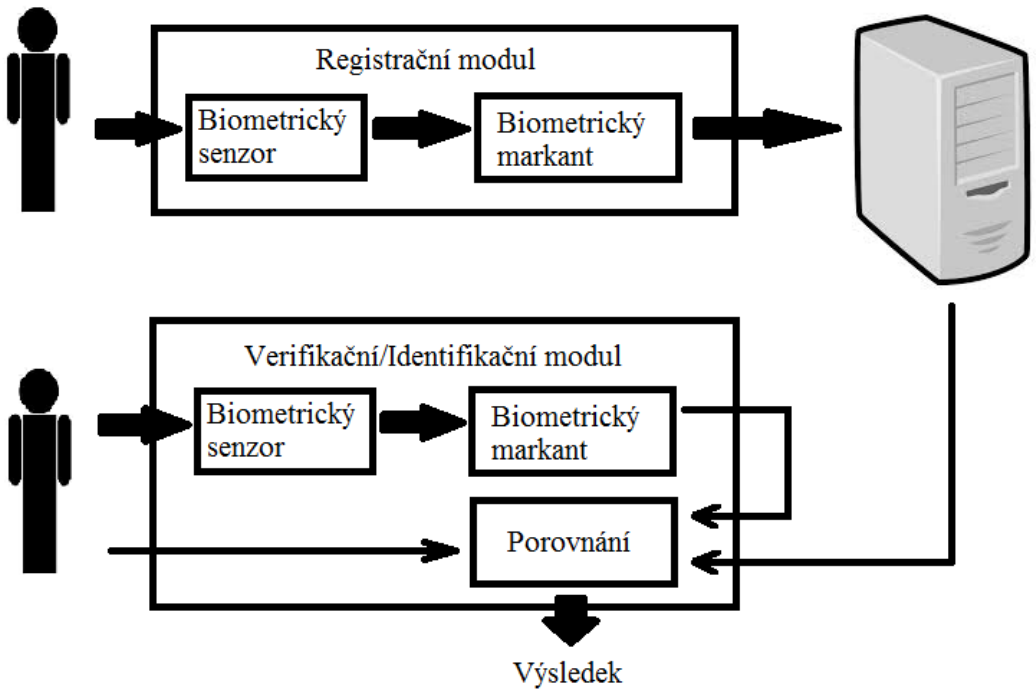
Biometrický systém tvoří dva moduly, registrační a verifikační (identifikační). Tyto moduly ovšem bývají integrovány v jednom softwarovém balíku. Biometrické systémy zpracovávají **biometrický vzorek**, který představuje odraz anatomicko-fyziologické nebo behaviorální charakteristiky do vnějšího světa. Tímto vzorkem se pro nás může stát kapka krve, zvukový záznam, podpis, obraz žilního řečiště aj. Všechna přijatá data a měřitelné údaje z biometrického vzorku označujeme jako **biometrické charakteristiky**. Tyto získané záznamy je nějakým způsobem možné měřit nebo popsat ovšem ne všechny jsou pro identifikaci žádoucí potřebné.[1,2,3,4]

Nejprve se zaměříme na registrační modul. Registrační modul v sobě zahrnuje registraci biometrické informace a zároveň obsahuje dvě složky a to biometrický senzor a biometrický markant. **Biometrický senzor**, slouží k extrakci konkrétní biometrické charakteristiky. **Biometrický markant**, představuje část biometrických charakteristik, které využíváme pro identifikaci daného subjektu. Jedná se tedy o zjednodušenou formu konkrétní charakteristiky. Ve specifickém vzorku nalézáme ve většině případů daleko větší množství upotřebitelných markantů, než je potřebné pro verifikaci. Například díky mapě žilního řečiště získáváme rozsáhlou strukturu žil. Biometrický markant je v konečné fázi registračního procesu uložen do databáze.[1,2]

Verifikační modul provádí ty samé operace jako registrační modul, ale neukládá biometrické rysy do databáze. Rozdíl je v tom, že načítá data z databáze za účelem porovnání s rysy identifikované osoby. Po provedení porovnání, získáme výsledek, který nám určuje míru nalezené shody. Výstupem mohou být pouze hodnoty „ano“ nebo „ne“. Žádné alternativy na pomezí těchto dvou výsledků nejsou možné.[1,2]

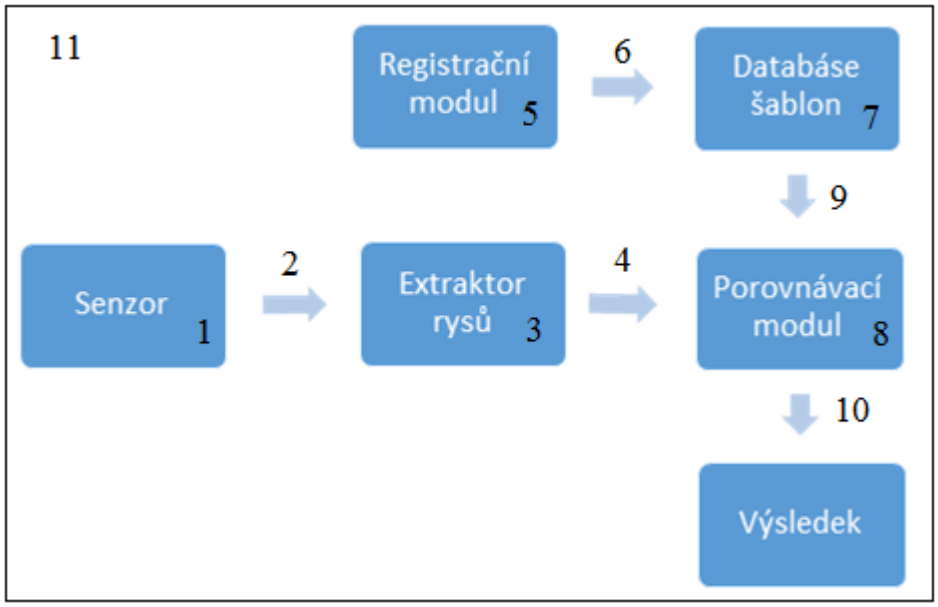
Všechny naměřené hodnoty, charakteristiky, informace a funkční závislosti daného minimálního počtu markantů, které slouží pro jednoznačnou identifikaci nebo identifikaci, představují **biometrické šablony**. Tyto šablony jsou konečným výsledkem maximální formalizace a optimalizace biometrického vzorku a slouží pro identifikační nebo verifikační účely. [1,2]

Následující schéma zobrazuje zjednodušené znázornění biometrického systému, které se skládá ze dvou výše popsaných modulů a jejich specifických komponentů. Konkrétně se tedy jedná o registrační modul, který obsahuje snímač biometrické vlastnosti. Tento snímač převede získaný snímek do požadované formy a uloží jej do databáze, která je vpravo. Dále zde můžeme vidět verifikační/identifikační modul, který taktéž obsahuje snímač a tentýž způsobem získá snímek. Ovšem jak je na obrázku znázorněno, tento snímek se neukládá do databáze, ale porovnává shodu s konkrétním uloženým snímkem nebo snímky.



Obrázek 1 Registrační a verifikační/identifikační modul. [1]

1.2 Možnosti napadení biometrického systému



Obrázek 2 Základní komponenty biometrického systému se zranitelnými místy. [1]

Tak jako všechny technické prvky používané v průmyslu komerční bezpečnosti, i biometrické systémy mají svá slabá místa, která mohou být napadnutelná. V praxi se často můžeme setkat s upřednostňováním rychlosti a spolehlivosti identifikace, či verifikace před samotným zabezpečením. Z toho důvodu je nutné, abychom dbali na určitý kompromis těchto složek a neupřednostňovali jednu před druhou. Na obrázku č. 2 můžeme vidět potenciální zranitelná či napadnutelná místa, která jsou označena čísly. Funkce a obsah činnosti jednotlivých složek jsou definovány dle čísla určení v daném obrázku (Obrázek č. 2.):

1.Předložení falešného biometrického rysu senzoru

U některých biometrických metod se můžeme setkat s odcizení biometrických vlastností. Tyto vlastnosti jsou následně zfalšovány a použity pro přístup do systému.

2.Opětovné zaslání již dříve použitých biometrických údajů

Již použitý biometrický signál v digitální podobě, který také může být uložen v databázi, je opětovně použit na vstupu.

3.Ovlivnění extraktoru rysů

Některé viry mohou způsobit vygenerování předem dané množiny rysů, která následně zapříčiní chybné vygenerování šablony.

4.Změna biometrických rysů

Mezi přenosem dat mezi extraktorem rysů a porovnávacím modulem může dojít ke změně přenášených dat.

5.Útok na registrační centrum

U registrace je využíván senzor, jak je zmíněno víše a proto může dojít ke stejnému problému jako u bodu číslo 1.

6.Útok na přenosový kanál mezi registračním modulem a databází

Při přenosu právě vzniklé registrační šablony může dojít k záměně za šablonu jinou.

7.Změna biometrické šablony

Uložená šablona v databázi může být nahrazena šablonou útočníka.

8.Ovlivnění porovnávacího modulu

Určité viry mohou předem vygenerovat rozhodnutí pro vyhodnocení a nezáleží tak na samotném porovnání šablony s vloženým biometrickým rysem.

9. **Útok na přenosový kanál mezi databází uložených šablon a porovnávacím modulem**

   Při načítání šablony k porovnání může být tato šablona napadnutelná.

10. **Změna finálního výsledku**

    Výsledek z porovnávacího modulu může být změněn bez ohledu na identičnost vzoru s charakteristikou.

11. **Útok na samotnou aplikaci**

    Samostatná aplikace může být napadnutelná. Při útoku dochází k vyřazení biometrické autentizace. [1]

1.3 Vymezení základních pojmů biometrie

Následující podkapitola shrnuje a objasňuje základní pojmy používané v biometrii. Každý jedinec je nějak odlišný a díky tomu se stává jedinečným. Dalo by se říct, že tyto odlišnosti tvoří jeden ze základních pojmů, kterým je identita. Biometrie využívá právě těchto odlišností a za pomoci verifikace či identifikace rozhoduje o majiteli předložených biometrických vlastností.

1.3.1 Identita

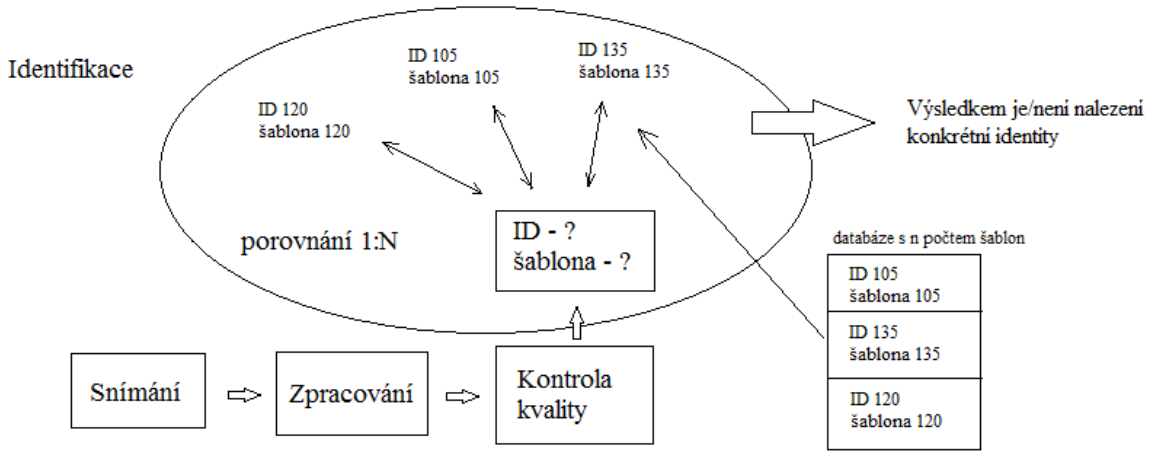
Identita je určitá neměnná jednoznačná charakteristika nejen lidí, ale také zvířat, či objektů. Díky této charakteristice je možné jednotlivé lidi, či jiné subjekty rozpoznávat. Pojem identita je původem z latiny (*identitas*, odvozené od *idem* -stejný), můžeme jej také nahradit slovem **totožnost.** V praxi se setkáváme s pojmy fyzická nebo také lidská identita, elektronická identita, biologická identita a sociální identita. **Fyzická identita** je neměnná vlastnost každého z nás, tato vlastnost je definována naším chováním a fyzickými rysy. Na světě se nemůžete setkat s člověkem, který by měl stejnou fyzickou identitu jako někdo jiný. Dokonce i jednovaječná dvojčata mají tuto identitu odlišnou, i když to tak na první pohled nevypadá, mohou se lišit třeba jen v DNA. **Elektronická identita** je spjata se světem počítačů, kde si každý člověk může vytvořit tolik identit, kolik potřebuje. Konkrétně se jedná o přístupové účty, e-mailové schránky, profily na sociálních sítích, aj. **Biologická identita** je kombinace biologických charakteristik a to jak vrozených, které jsou často dědičné, tak i získaných. Tyto charakteristiky jsou nezávislé na vědomí člověka. Biologická identita je jednoznačně prokázána strukturou DNA (deoxyribonukleová kyselina). Díky **sociální**

identitě můžeme lidi řadit do skupin, které se projevují stejnými společenskými, geografickými, kulturními, náboženskými a jazykovými vlastnostmi.[2]

1.3.2 Identifikace

Identifikace je určitý **proces**, který má za úkol zjištění identity osoby na základě jejich shod či rozdílů v daných vlastnostech či chování. Identifikace se také označuje jako porovnání jeden k mnoha (1:N) nebo rekognice, což je v kriminalistice udáváno jako vizuální identifikace laického charakteru. [1,2,3,4]

Při tomto procesu dochází k nasnímání biometrického vzorku, který se porovnává se všemi referenčními šablonami uloženými v databázi. Délka tohoto procesu je závislá na počtu šablon, se kterými se vložený vzorek porovnává. Výstupem tohoto porovnávání je nalezení totožné šablony, která nám poskytne odpověď na otázku, komu tato šablona patří. Hlavním úkolem identifikace je ověření identity osoby oprávněné a potvrdit, že je opravdu tou osobou, za kterou se vydává. A také naopak musí prokázat osobám neoprávněným, že nejsou tím, za koho se vydávají.[2]

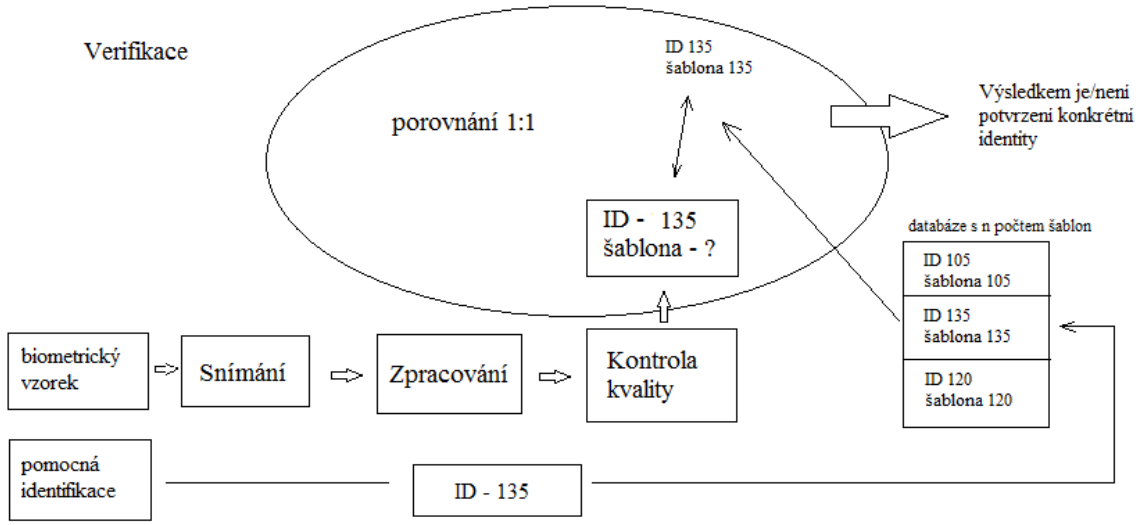


Obrázek 3 Identifikační proces [2]

1.3.3 Verifikace

Verifikace je **proces,** který má za úkol porovnat předložený biometrický vzorek s konkrétní šablonou uloženou v databázi. Taktéž se můžeme setkat s označením jedna k jedné (1:1). Při tomto procesu nejprve prověřovaná osoba vloží do systému svou elektronickou identitu, například ID, PIN, apod., dále pak svou biometrickou vlastnost. Na

základě těchto vložených údajů nemusí systém hledat shodu mezi všemi šablonami, ale jen mezi konkrétní šablonou, která přísluší prověřované osobě. Výstupem verifikace je tedy potvrzení nebo vyvrácení identity konkrétní osoby. Verifikace je v porovnání s identifikací méně časově náročná, protože systém nehledá shodu u všech šablon nýbrž jen u jedné. [1,2,3,4]



Obrázek 4 Verifikační proces [2]

1.4 Využití biometrických systémů v moderní společnosti

V minulosti byla biometrická identifikace uplatňována především policejně-soudními a bezpečnostními aplikacemi. Nyní se s biometrickými systémy setkáváme i v civilní a komerční sféře. Rozvoj těchto technologií jde neustále kupředu, a proto se s těmito vymožeností moderní společnosti setkáváme stále častěji ve všech směrech a oborech lidské činnosti. Takřka každý den přicházíme do kontaktu s elektronickými zařízeními, která po nás vyžadují identifikaci. Mohli bychom zmínit alespoň základní elektronická zařízení, jako jsou například mobily, počítače, notebooky, bankomaty, kontrola vstupu aj. Všechna tato zařízení využívají elektronickou identifikaci na základě vlastnictví identifikátoru či znalosti hesla. Jak již bylo zmíněno, identifikace na základě vlastnictví či znalosti je snadno zneužitelná, a proto je zapotřebí nahradit tyto stávající systémy za biometrické systémy, které mají velký potenciál v technologickém růstu naopak od metod využívaných.

Biometrickou identifikaci tedy můžeme využít v následujících oblastech:

Policejně-soudní oblast

- Identifikace podezřelých osob,
- identifikace obětí a pohřešovaných osob,
- identifikace vězňů,
- sledování a identifikace jiných zájmových osob.

Bezpečnostně-komerční oblast

- Ochrana platebních a bankovních karet,
- ochrana vstupu do objektů a zařízení,
- cestování a turismus,
- udržování dobrých vztahů se zákazníky,
- ochrana majetku,
- telekomunikace a ochrana elektronických transakcí,
- kontrola pracovní docházky a přítomnosti na pracovišti,
- ochrana zbraňových systémů i individuálních zbraní,
- automobilový průmysl.

Oblast státní správy

- Hraniční kontroly
- vystavování dokladů totožnosti,
- přidělování podpory nezaměstnaným, zdravotní a sociální dávky,
- volby, sčítání lidu. [2,3]

První kapitola byla věnována základním informacím a pojmům, které souvisí s biometrickými systémy. Byly zde nastíněny oblasti využití, základní principy a vlastnosti. Dále byly objasněny některé základní pojmy, které souvisí s biometrickými postupy. Na tuto část logicky navazuje další kapitola, která pojednává o biometrických identifikačních systémech.

2 BIOMETRICKÉ IDENTIFIKAČNÍ SYSTÉMY

Kapitola biometrické identifikační systémy se bude věnovat základnímu rozdělení identifikačních metod. Pro identifikační účely se v praxi využívá unikátních časově neměnných anatomických a fyziologických vlastností člověka. Můžeme se také setkat s využitím behaviorálních vlastností, které ovšem nejsou natolik přesné. Dále si objasníme pojmy unimodální a multimodální systémy. V dalších podkapitole se zaměříme na konkrétní požadavky, které by kvalitní biometrické systémy měly splňovat. V poslední podkapitole se budeme věnovat pojmům FAR a FRR, neboli spolehlivosti těchto systémů.

U **anatomicko-fyziologických vlastností** se využívá jedné konkrétní vlastnosti lidského těla, jako je například struktura žilního řečiště, nebo otisk prstu. Jak již bylo zmíněno, tyto rysy jsou neměnné, vždy přítomné a také nejsou ovlivnitelné psychickým stavem člověka. Metoda analýzy anatomicko-fyziologických vlastností se také označuje jako **statická** metoda.[1,2,3,4]

Skupina **behaviorálních vlastností** je spojena s konkrétní činností člověka. Například můžeme pozorovat odlišnosti při chůzi, podpisu nebo při mluvení. Tyto vlastnosti jsou ovšem lehce ovlivnitelné aktuálním psychickým či jiným stavem člověka. V důsledku ovlivnění nejsou tyto nasnímané vzorky identické, a tudíž jsou v daném případě nepoužitelné. Metoda analýzy behaviorálních vlastností se také označuje jako **dynamická** metoda. Dynamika se projevuje zejména v jejich neustálém vývoji a poměrné proměnlivosti. [1,2,3,4]

Následující tabulka obsahuje přehledné rozdělení využívaných biometrický charakteristik do jednotlivých skupin:

Tabulka 1 Rozdělení biometriky dle měřitelných vlastností [2]

Anatomické vlastnosti	Otisk prstu; obličej; duhovka oka; sítnice oka; geometrie ruky a prstů; dlaň; termogram ruky a obličeje; dentální obraz; podpis (statická forma); tvar ucha; snímek nehtu; DNA; topografie žil; pach lidského těla
Behaviorální vlastnosti	Hlas; řeč; mimika obličeje a pohyby rtů; podpis (dynamická forma); chůze; dynamika stisku kláves; lokomoce

Dále mohou být biometrické identifikační systémy děleny na unimodální a multimodální. **Unimodální systémy** využívají k identifikaci pouze jednu biometrickou vlastnost. S využitím pouze jedné vlastnosti se často setkáváme v praxi a to z toho důvodu že tyto systémy jsou levnější, naopak jejich hlavní nevýhodou je nižší spolehlivost. Z toho tedy vyplívá, že **multimodální systémy** využívají více biometrických vlastností nebo více příznaků jedné biometrické vlastnosti, jako je tomu například u použitého skeneru. Tento skener porovnává otisk prstu i strukturu žilního řečiště. Tyto multimodální systémy nesou značnou výhodu ve spolehlivosti rozpoznání. Díky využití dvou metod jsou také odolnější proti zfalšování biometrického rysu, a odráží tak možné riziko napadnutí. Jedinou nevýhodou je pořizovací cena, která zpravidla bývá vyšší než u unimodálních systémů.[1]

2.1 Požadavky na biometrický systém

Pokud se hodláme zavést biometrický identifikační systém, musíme dbát na určitá kritéria, která jsou u konkrétních systémů odlišná. Měli bychom si vymezit důležitost jednotlivých kritérií, která nám napomohou zvolit nejvhodnější systém. Tyto základní vlastnosti bychom mohli zařadit do následujících skupin[2]:

- **Operační kritéria**
  - Jedinečnost,
  - neměnnost,
  - měřitelnost,
  - uchovatelnost,
  - spolehlivost,
  - exkluzivita,
  - praktičnost,
  - přijatelnost,
  - uživatelská přívětivost.

- **Technická kritéria**
  - Minimální čas zpracování identifikačních charakteristik,
  - přijatelná chybovost,
  - flexibilita,
  - odolnost,
  - efektivnost,

- výkonnost,
- standardizace (kompatibilita),
- skladovatelnost identifikačních charakteristik,
- přesnost,
- jednoduchost,
- rychlost,
- nezávislost na vnějším prostředí.

- **Výrobní kritéria**
  - Kvalita,
  - podpora,
  - záruky,
  - perspektivnost,
  - reference.

- **Finanční kritéria**
  - Pořizovací cena,
  - náklady na údržbu,
  - náklady na instalaci a provoz.

- **Metodologická, algoritmická kritéria a bezpečnostní kritéria**
  - Správnost a bezpečnost algoritmů,
  - kódování.

2.2 Spolehlivost biometrických identifikačních systémů

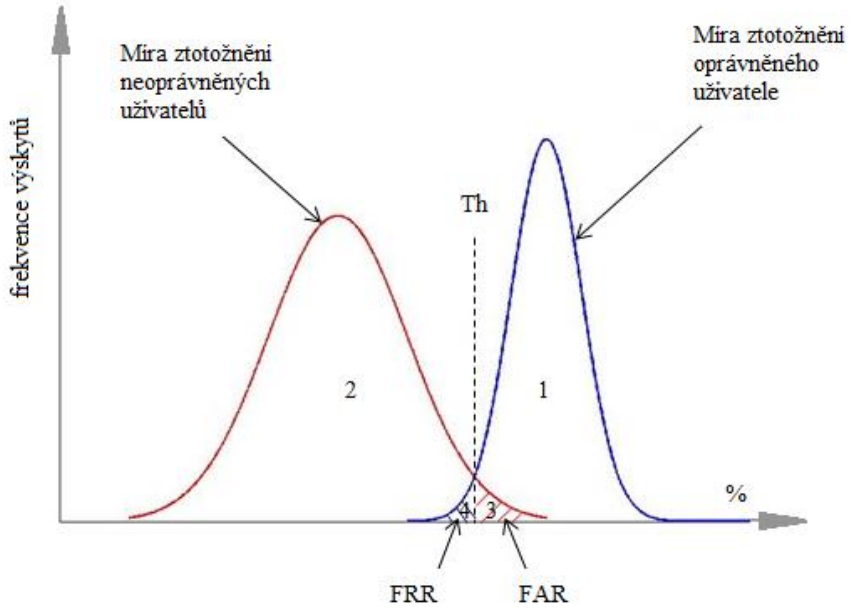
Jak již bylo zmíněno, biometrické identifikační systémy mají mnoho různých kritérií. Od nich se odvíjí konkrétní výběr daného systému. Mezi nejdůležitější kritéria můžeme zařadit právě spolehlivost a přesnost. Na trhu se můžeme setkat se spoustou biometrických snímačů, které využívají jedinečné biometrické charakteristiky za účelem verifikace či identifikace. Ovšem ne všechny tyto systémy jsou od jednoho výrobce. Nejsou tudíž identické a nevyužívají stejných fyzikálních principů potřebných k ověřování identity.

Proto musíme vnímat fakta, zda je konkrétní systém vhodný pro praxi, je dostatečně spolehlivý a přesný.

Abychom mohli popsat míru spolehlivosti, byly v praxi zavedeny dva pojmy[1,2,3,4]:

- **Pravděpodobnost chybného odmítnutí** (autorizované osoby) **FRR**
- **Pravděpodobnost chybného přijetí** (neoprávněné osoby) **FAR**

Při identifikaci či verifikaci dochází k porovnání vložené vlastnosti s šablonou, která je uložena v databázi. Jelikož jsou biometrické vlastnosti mírně nestálé, musíme právě při jejich porovnání počítat s určitou odchylkou. Porovnávacímu výsledku se také říká **míra ztotožnění** nebo skóre. A jelikož toto skóre není vždy stoprocentně identické, nastavuje se v aplikacích určitý **práh citlivosti**, který umožňuje nastavení citlivosti. Práh citlivosti můžeme označit jako Th. [1,2,3,4]



Obrázek 5 Výsledek porovnání [1]

Tento obrázek zobrazuje míry ztotožnění oprávněných a neoprávněných uživatelů. Tyto křivky se navzájem protínají a zároveň je rozděluje práh citlivosti do čtyř sekcí, které jsou označeny čísly 1 až 4.

1. První oblast představuje **přijetí oprávněného uživatele**.
2. Druhá oblast představuje **odmítnutí neoprávněného uživatele**.
3. Třetí oblast představuje **přijetí neoprávněného uživatele**.

4. Čtvrtá oblast představuje **odmítnutí oprávněného uživatele**.

Míru ztotožnění, která rozhoduje o tom, zda je osoba oprávněná či neoprávněná může představovat následující rovnice[2]:

s = Sim (X,X´)

s = míra ztotožnění

X = vložená biometrická vlastnost

X´ = biometrická vlastnost uložená v databázi

Pokud s ≥ Th potom platí X = X´. To tedy znamená, že osoba, která je vlastníkem vzorku, je osobou oprávněnou.

Pokud s < Th potom platí X ≠ X´. To tedy znamená, že osoba, která je vlastníkem vzorku, je osobou neoprávněnou.

2.3 Pravděpodobnost chybného odmítnutí

Pravděpodobnost **chybného odmítnutí**, neboli **FRR** (False Rejection Rate) udává, s jakou pravděpodobností bude oprávněný uživatel, který má již v databázi svou biometrickou šablonu chybně odmítnut. Takovéto odmítnutí není nijak závažná věc, uživatel se musí znovu pokusit o identifikační/verifikační proces a doufat, že se tato chyba nebude opakovat. U biometrických systémů se klade velký důraz na to, aby tato pravděpodobnost chybného odmítnutí byla co nejmenší. To z toho důvodu, abychom neodradili potencionální zákazníky jen tím, že budou muset identifikační/verifikační proces několikrát opakovat než budou přijati. [1,2,3,4]

Definice pravděpodobnosti chybného odmítnutí[2]:

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

Kde značíme:

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).

Taktéž můžeme FRR definovat jako podíl dvou ploch (dle obrázku č. 4) [2]:

$$FRR = \frac{P_4}{P_{1,3,4}}$$

Kde značíme:

P_4 – Plocha číslo 4.

$P_{1,3,4}$ – Plocha číslo 1, 3, 4.

2.4 Pravděpodobnost chybného přijetí

Pravděpodobnost **chybného přijetí** neboli **FAR** (False Acceptance Rate) udává, s jakou pravděpodobností bude neoprávněný uživatel, který nemá v databázi svou biometrickou šablonu chybně přijat. Takovéto přijetí je chápáno jako závažný problém. V důsledku přijetí nežádoucí osoby či osob hrozí nebezpečí, při kterém by mohlo dojít k poškození či ztrátě majetku, narušení stability objektu nebo k jiným nežádoucím činům. V praxi se snažíme o eliminaci takovýchto přístupů. [1,2,3,4]

Definice pravděpodobnosti chybného odmítnutí[2]:

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

Kde značíme:

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).

Taktéž můžeme FAR definovat jako podíl dvou ploch (dle obrázku č. 4) [2]:

$$FRR = \frac{P_3}{P_{2,3,4}}$$

Kde značíme:

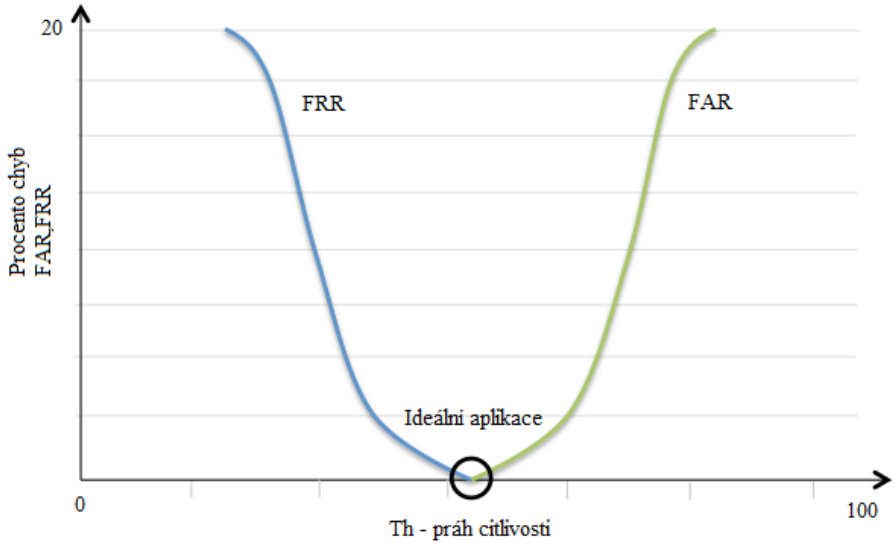
P_3 – Plocha číslo 3.

$P_{2,\ 3,\ 4}$ – Plocha číslo 2, 3, 4.

2.5 Vztah mezi FRR a FAR

V ideálním případě bychom po biometrickém systému vyžadovali, aby nevykazoval žádnou chybovost a nespolehlivost. Ovšem s tímto příkladem se v praxi nesetkáme, protože neexistuje takové zařízení, které by tyto podmínky splňovalo. V ideálním případě by se tedy křivky FRR a FAR neproťaly a práh citlivosti by byl umístěn přesně mezi nimi, tak jako to můžeme vidět na obrázku č. 6. V takovém případě bychom mohli danou skutečnost vyjádřit pomocí rovnice[1,2,3,4]:

$$FAR = FRR = 0$$



Obrázek 6 Ideální biometrická aplikace [2]

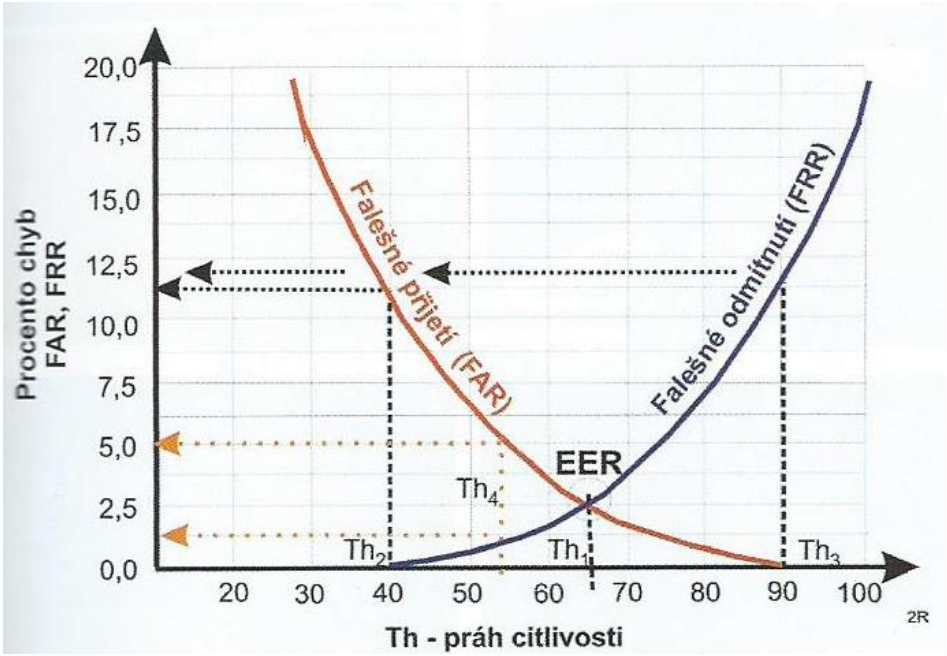
Jak již bylo řečeno, v praxi se s takovým případem nesetkáme, protože se křivky FRR a FAR vždy protnou, a to z toho důvodu, že skenery jsou citlivé na okolní vlivy. Tyto vlivy negativně ovlivňují výsledek, což můžeme lépe spatřit na obrázku č. 7. V tomto případě lze

u některých aplikací libovolně volit práh citlivosti. Potom se setkáme s rozhodnutím, zda hodláme upřednostňovat FRR, FAR nebo zvolíme zlatou střední cestu.

Pokud chceme dbát na **komfort**, musíme nastavit práh citlivosti tak, aby FRR bylo rovno nule. V praxi to znamená, že všichni registrovaní uživatelé budou bez jakýchkoli chyb přijati, ovšem roste s tím i počet nežádoucích přijetí od neregistrovaných uživatelů. [1,2]

Naopak, klademe-li důraz na **bezpečnost**, musíme nastavit práh citlivosti tak, aby FAR bylo rovno nule. Tentokrát se ovšem budeme muset smířit s tím, že hodnota komfortu klesne a registrovaní uživatelé budou více odmítáni. Výhodou ovšem je, že nikdo neoprávněný tento systém nenaruší.[1,2]

Jestliže chceme zvolit **kompromis** mezi komfortem a bezpečností, měli bychom práh citlivosti nastavit v průsečíku FRR a FAR. Místo, kde se tyto křivky setkávají, se označuje jako ERR (Equal Error Rate), neboli **míra vyrovnání chyb**. ERR nemá žádný fyzikální význam a slouží k orientačnímu porovnání dvou aplikací.[1,2]



Obrázek 7 Reálná biometrická aplikace [2]

2.6 Míra spolehlivosti biometrických systémů

V následující podkapitole jsou uvedeny jednotlivé stupně spolehlivosti. Tuto spolehlivost představují míry FAR a FRR. Díky odlišným mírám FAR a FRR můžeme spolehlivost rozdělit do následujících stupňů:

- Nízká míra spolehlivosti

  FAR vetší než 0,1%

  FRR vetší než 1%
- Střední míra spolehlivosti

  FAR v rozmezí 0,1% až 0,001%; včetně těchto hodnot

  FRR v rozmezí 1% až 0,1%; včetně těchto hodnot
- Vysoká míra spolehlivosti

  FAR menší než 0,001%

  FRR menší než 0,1% [3]

Tato kapitola byla zaměřena na základní rozdělení biometrických systémů, konkrétně na systémy s využitím anatomických a behaviorálních vlastností, na systémy unimodální a multimodální. Dále byly zmíněny nejdůležitější požadavky, které by tyto systémy měli splňovat. Poslední část této kapitoly byla věnována spolehlivosti systémů.

3 HISTORICKÝ VÝVOJ BIOMETRIE A ŽILNÍHO ŘEČIŠTĚ

První zmínky o biometrické identifikaci sahají až do faraonské dynastie Egypta, kde se lidé přeměřovali za účelem identifikace. Dochovali se písemné zmínky o zjišťování příslušnosti dělníků a farmářů v povodí řeky Nil. Tito dělníci a farmáři byli rozčleněni do specifických skupin na základě jejich vzhledu, postavy, barvy pleti a očí, a také díky jedinečným jizvám či poraněním, ke kterým přišli během svého života. Tato identifikace sloužila především k vyplácení mezd dělníkům a odměňování farmářů za jejich materiální přínos do státních rezerv.[2,3]

Za zmínku stojí i fakt, že se biometrická identifikace objevila i ve Starém zákoně (12:5-6). „*[5]Gileáďané tehdy Efraimcům obsadili jordánské brody, a kdykoli někdo z efraimských uprchlíků žádal: „Nechte mě přejít,“ Gileáďané se ho ptali: „Nejsi Efraimec?“ Když odpověděl: „Nejsem,“ [6]vyzvali ho: „Tak řekni: Šibolet.“ Když ale řekl: Sibolet (protože to neuměl vyslovit správně), popadli ho a zamordovali. Tenkrát u těch jordánských brodů padlo 42 000 Efraimců.“*[19]

Píše se zde o izraelitských uprchlících, kteří prchali z Egypta a byli pronásledováni faraonovým vojskem. Vojáci rozpoznávali tyto uprchlíky díky jejich výslovnosti konkrétního slova šibolet. V dnešní době, bychom tento způsob ověřování mohli označit za hlasovou verifikaci.

Biometrie se tedy využívala odjakživa. Důkazem toho jsou i dochované otisky prstů u skalních maleb, které potvrzovali identitu autora určité malby. Podobně tomu bylo i u otisků prstů použitých místo podpisu při obchodních dohodách, které se objevovaly již u starých Babyloňanů, Číňanů nebo Peršanů.[1,2,3]

V novodobé historii se na rozvoji podíleli významní profesoři, vědci, lékaři a ostatní neméně významní lidé. Jejich konkrétní přínos a činnost v oblasti biometrie přiblížíme v následující části práce:

Marcello Malpighi (1628 – 1694)

Italský profesor anatomie, který v roce 1686 jako první popsal otisky prstů, které jsou tvořené vrstevnicemi, spirály a smyčkami. V tomto roce ovšem neměly žádné konkrétní využití, vzhledem k tomu, že obor identifikace osob nebyl natolik rozvinutý. [1,2]

Obrázek 8 Marcelo Maplighi [6]

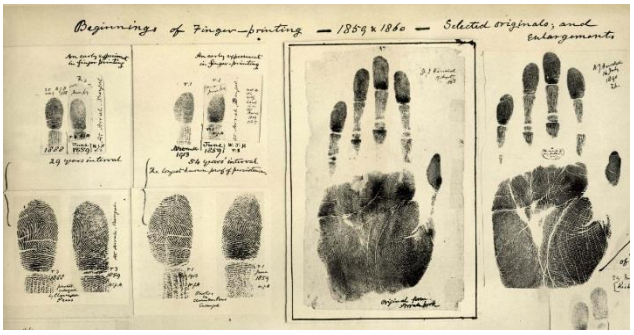
Jan Evangelista Purkyně (1787 – 1869)

Český přírodovědec lékař, který se roku 1823 taktéž podrobně zabýval geometrickými vlastnostmi otisků prstů. Jeho studie lidských otisků byla zaměřena spíše z lékařského a přírodovědeckého hlediska. [1,2]

Obrázek 9 J. E. Purkyně [7]

William James Herschel (1833-1917)

Anglický guvernér působící v Indii. Roku 1858 tam podobně jako tomu bylo kdysi v Egyptě, využil otisků pro ověření identity a k následnému vyplácení mezd zaměstnancům dráhy. Spousta tamních dělníků byla negramotná a toto byla jediná možnost jak potvrdit převzetí peněz. [1,2]



Obrázek 10 Otisky prstů a dlaní pořízené W.J. Herschelem [8]

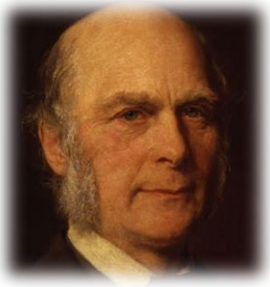
Dr. Henry Faulds (1843-1930)

Skotský misionář, lékař a vědec, který se v období kolem roku 1860 taktéž zasloužil o rozvoj biometrie, a to konkrétně v oblasti využití otisků prstů. Faulds, působící v Japonsku a Indii začal využívat nalezené daktyloskopické stopy k identifikaci podezřelých, předem vytipovaných osob. [1,2]

Obrázek 11 Dr. Henry Faulds [9]

Francis Galton (1822-1911)

Anglický vědec, který se zasloužil o největší posun v dané oblasti. Společně s Edwardem Henrym roku 1880 založili třídící a registrační systém využitelný v praxi. Tento obor, zabývající se tříděním a registrací se nazývá antropometrie. Sám Galton se zabýval problematikou dědičnosti fyzických vlastností. Dále se stal zakladatelem oboru eugenika. Tento obor se zabývá dědičnými chorobami a vadami u lidského plodu. Roku 1892 se Galton zasloužil také o dílo Fingerprints. Toto dílo bylo oporou pro zavedení daktyloskopie do praxe (1900).[1,2]



Obrázek 12 Francis Galton [10]

Juan Vucetich (1858-1925)

Chorvatský antropolog a policejní úředník působící v Argentině, který od roku 1891 začal snímat otisky obviněným osobám, a začal tak bojovat proti kriminalitě.[2]

Obrázek 13 Juan Vucetich [11]

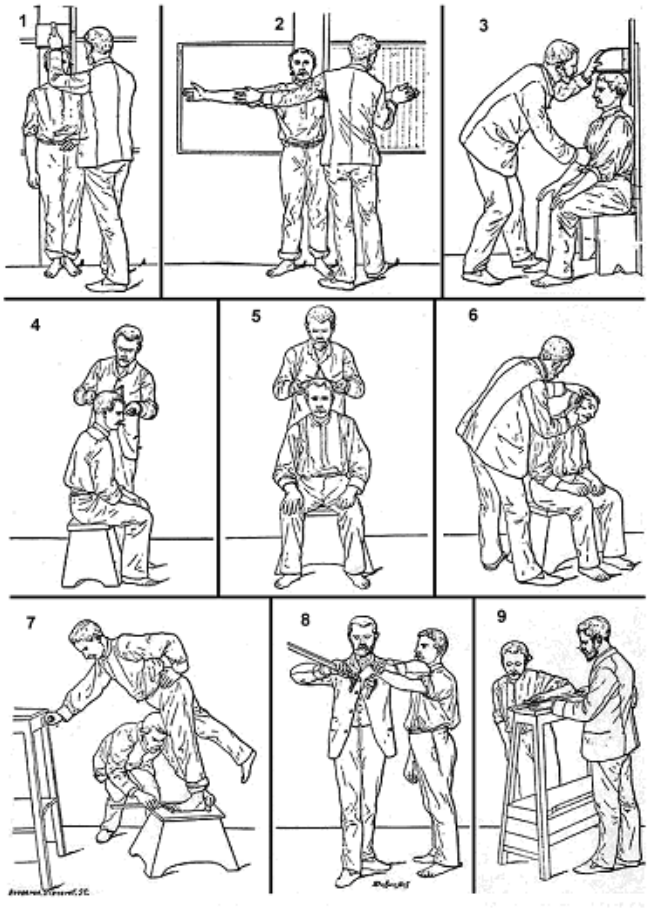
Alphonse Bertillon (1853-1914)

Francouzský vědec a policejní důstojník, který přišel s identifikačním postupem, který obecně označujeme jako Bertillionáž. Tento postup byl velice podobný antropometrii, což zapříčinilo jistou neurčitost v tom, který z těchto dvou názvů se bude pro tuto metodu používat. Bertillionáž popisovala geometrické vlastnosti lidského těla a hlavy (tyto vlastnosti jsou po 20. roce života neměnné), Bertillon mohl identifikované osoby rozdělit do 243 kategorií. S využitím barvy očí a vlasů se počet kategorií zvýšil až na 1701. Postupem času byla antropometrie (bertillionáž) nahrazena daktyloskopií, která se využívá dodnes.[1,2,3]

Obrázek 14

Alphonse Bertillon [12]

V historii se můžeme setkat s různými způsoby identifikace osob. V následujícím obrázku si přiblížíme, které konkrétní oblasti měření byly pro lidské tělo zásadní.

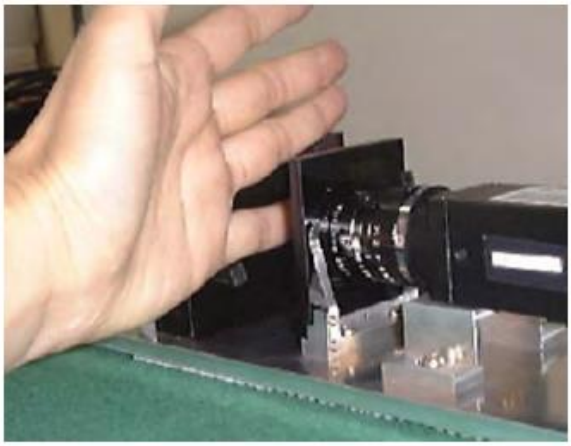


Obrázek 15 Antropometrie [1]

K měření lidského těla se využívalo následujících jedenácti rozměrů[1]:

- Tělesná výška (obr. 1),
- délka natažené paže (obr. 2),
- výška v sedu (obr. 3),
- délka hlavy (obr. 4),
- šířka hlavy (obr. 5),
- délka a šířka pravého ucha (obr. 6),
- délka levé nohy (obr. 7),
- délka levého prostředníčku a malíčku (obr. 8),
- délka pravého předloktí (obr. 9).

Skenování žilního řečiště se zdá být velmi novodobou záležitostí, ovšem opak je pravdou. Joseph Rice (USA) se začal věnovat žilnímu řečišti již v roce 1984. V následujícím roce si nechal vystavit patent pro využití žilního řečiště jako identifikační metody a vytvořil prototyp skeneru žilního řečiště. Následně byla tato technologie zkoumána a vyvíjena. V roce 1997 se ve Spojených státech objevilo první zařízení pro ověřování totožnosti žil na dlani, toto zařízení bylo ale velmi nepřesné a muselo se dále vylepšovat. V roce 2003 se o tento produkt začala zajímat firma Fujitsu (Japonsko) a v roce 2004 začala sériově vyrábět svá zařízení pro tamní finanční instituce. Firma Fujitsu byla za svůj přínos v roce 2005 oceněna cenou ‘‘Wall Street Journal’s 2005 Technology Innovation Award for Security in Networks’’. V České republice byly skenery žilního řečiště dostupné od roku 2007. V současnosti se na trhu s biometrickými čtečkami můžeme setkat s firmami, jako jsou Fujitsu (PalmSecure), Hitachi, Safran (Morpho).[3,13]



Obrázek 16 Prototyp skeneru žilního řečiště

[13]

Tato kapitola byla zaměřena zejména na vývoj celé biometrie, dále byli čtenáři seznámeni s významnými představiteli a průkopníky v dané problematice. Poslední část byla zaměřena na vývoj biometrické metody, která využívá žilní řečiště. Byl zde představen autor prvního skeneru žilního řečiště. A na konec se v této části objevili i nynější představitelé, kteří se věnují vývoji skenerů žilního řečiště.

4 SKENER ŽILNÍHO ŘEČIŠTĚ

Následující kapitola se zaměřuje na funkční princip skeneru žilního řečiště. Především se bude věnovat principu třem základním metodám, které jsou skenování hřbetu, dlaně a prstu ruky. Dále se zaměří na konkrétní využití v praxi. Shrne výhody a nevýhody této metody a srovná metodu snímání žilního řečiště s ostatními nejpoužívanějšími metodami.

Skener žilního řečiště využívá ke své identifikaci rozpoložení cévního řečiště. Konkrétně se jedná o žilní řečiště ruky, to z toho důvodu, že tepny v ruce jsou umístěny příliš hluboko na to, aby je skener dokázal zachytit. Struktura žilního řečiště se vyvíjí již před narozením člověka a jeho rozpoložení je neměnné, v důsledku dospívání se mění pouze velikost a odstup jednotlivých žil.[1,2,3,4,5,13,14]

4.1 Princip identifikace

Identifikaci za pomocí žilního řečiště lze provádět několika způsoby:

- Skenování žil na hřbetu ruky,
- skenování žil na dlani ruky,
- skenování žil na prstu ruky.

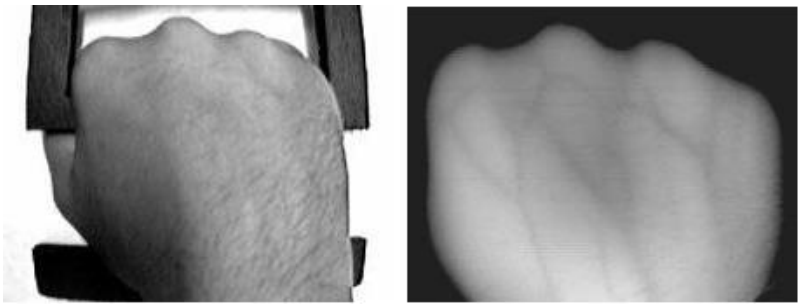
4.1.1 Skenování žil na hřbetu ruky

Proces snímání žil můžeme rozdělit do několika etap[3,4,13,14]:

- Segmentace (hand region segmentation),
- Vyhlazení a redukce šumu (difussion smoothing),
- Lokální prahování (local tresholding),
- Postprocessing

Nejprve je však zapotřebí získat snímek žilního řečiště. Ve viditelném spektru není struktura žil zcela zřejmá, proto se využívá záření, které je na hranici infračerveného a viditelného spektra (IR záření má vlnovou délku mezi $7{,}6\text{x}10^{-4}$ mm a 1 mm). Záření tak zvýrazní kontrast mezi žilním řečištěm a okolní kůží. Toto zvýraznění může proběhnout díky okysličenému hemoglobinu, který koluje v žilách. Hemoglobin pohlcuje světlo o vlnové délce $7{,}6\text{x}10^{-4}$ mm. IR záření proniká zhruba 3mm pod živou tkáň, díky tomu je možné zvýraznit pouze povrchové cévy na hřbetu ruky. [3,4,13,14]

V následujícím obrázku můžeme vidět snímek ruky. Vlevo je tento snímek zachycen za pomocí klasického fotoaparátu a vpravo potom můžeme vidět snímek pořízený skenerem. Na první pohled je zřejmé, že skener za pomoci IR světla značně zvýrazní strukturu žilního řečiště, která na normálním snímku není úplně jasná.

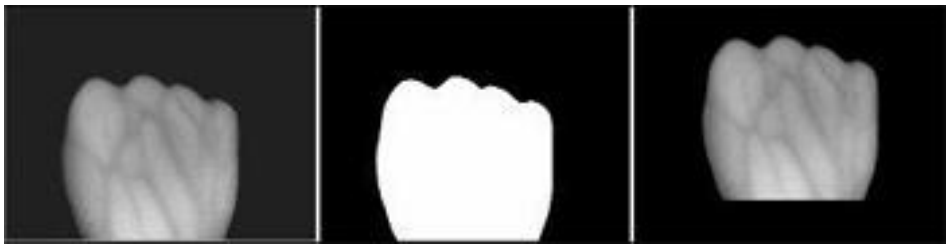


Obrázek 17 Snímek ruky – vlevo zobrazení viditelným světlem, vpravo zobrazení IR zářením [14]

4.1.1.1 Segmentace

Po získání snímku je třeba získat tu část, na které je pouze ruka. To znamená, že se získaný snímek rozdělí na dvě části, část ruky a pozadí, které je dále nepoužitelné. V dalším procesu se využije jen vybraný a vycentrovaný snímek ruky.[4,13,14]

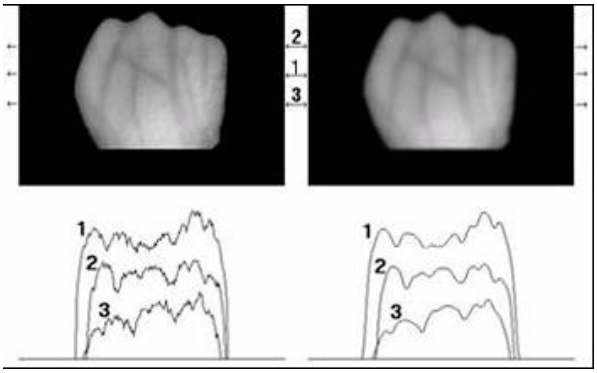
Obrázek číslo 18. je rozdělen na tři části, v první části můžeme vidět získaný snímek řečiště za pomocí skeneru. Na druhém obrázku vidíme ořezání původního snímku a na třetím obrázku vidíme finální vycentrovaný obraz ruky bez původního pozadí.



Obrázek 18 Segmentace [14]

4.1.1.2 Vyhlazení a redukce šumu

Pro redukci šumu a vyhlazení snímku se využívá převážně Gaussovského filtru rozmazání (nezanechává hrany), nebo nelineárního filtru rozptýlení (zanechává hrany). Účelem je vyhlazení obrazu a potlačení nerovností tvaru ruky. [4,13,14]



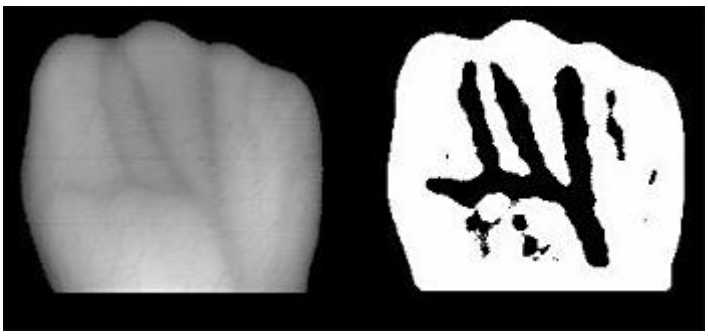
Obrázek 19 Vyhlazení snímku ruky [14]

4.1.1.3 Lokální prahování

Hlavním úkolem lokálního prahování je oddělení struktury žil od zbytku snímku. V praxi je možno využít čtyři **hlavní metody**[4,13,14]:

1. Segmentace prahováním,
2. segmentace pomocí hran,
3. segmentace pomocí oblastí,
4. segmentace porovnáním.

Nejrychlejší a nejméně náročná je první metoda, tedy segmentace prahováním. U této metody se využívá výpočet průměrné hodnoty z okolních pixelů a použití této průměrné hodnoty jako hodnoty prahu. [4,13,14]



Obrázek 20 Lokální prahování [14]

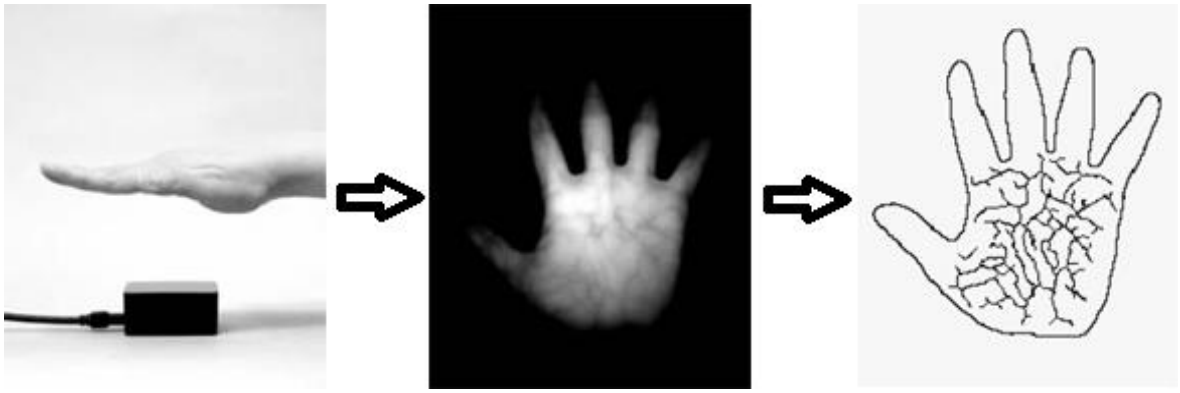
4.1.1.4 Postprocessing

Finálním krokem je postprocessing, kde se po konečných úpravách na snímku zobrazuje jen sktruktura žilního řečiště. Takovýto snímek je zřetelný a dvourozměrný, lze jej označit jako šablonu, kterou lze uložit do databáze. [3,4,13,14]

Obrázek 21 Postprocessing [14]

4.1.2 Skenování žil na dlani ruky

Princip skenování žil na dlani se nijak výjimečně neliší od snímání na hřbetu ruky. V praxi se využívá bezdotykového snímače, který automaticky rozpozná dlaň bez ohledu na pozici a pohyb ruky. [3,4,13,14]



Obrázek 22 Proces skenování dlaně[14]

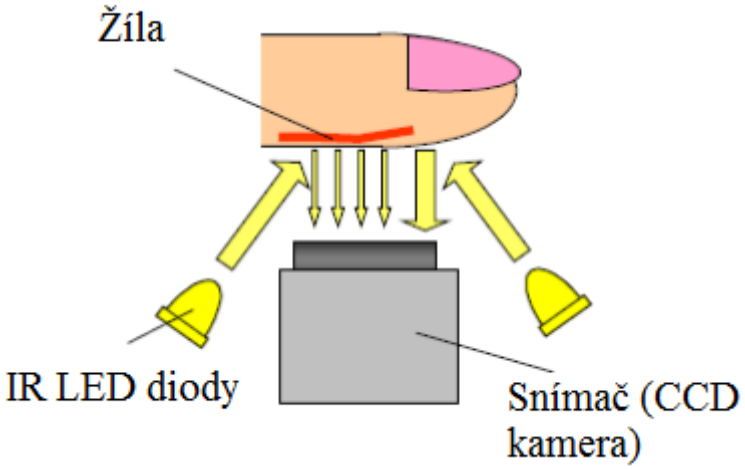
Na obrázku můžeme vidět postup při skenování. Nejprve se ruka přiloží k snímači, který za pomoci IR záření získá snímek Na tomto snímku je díky hemoglobinu viditelná struktura žil. Ze získaného snímku je možné vytvořit extrakci žil, kterou je možno umístit v novém snímku. Tento nový a poslední snímek je možno uložit do databáze a použít jej jako šablonu.

4.1.3 Skenování žilního řečiště na prstu ruky

Metoda skenování žil prstu je z těchto tří metod nejmladší a přináší s sebou jistou výhodu, která by u předešlých metod byla těžko realizovatelná. Jedná se o využití multimodálního snímání, které přináší značnou výhodu v bezpečnosti celého systému. Pokud je tedy snímáno žilní řečiště prstu, je možné zároveň snímat otisk prstu, čímž je sníženo riziko oklamání systému. Skenery žilního řečiště v prstu využívají několika metod.

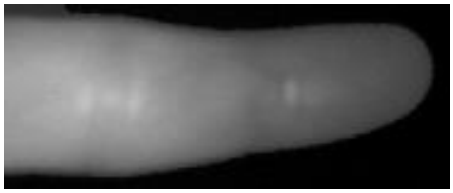
Zpracování obrazu se ovšem nijak neliší od zpracování, které je zmíněno u skenování hřbetu ruky. [4,13,14]

Na následujícím obrázku je vidět snímání, za pomocí reflexivní metody. Je zde znázorněn prst s vyznačenou žílou, dále pak snímač, který zachycuje odražené světlo a diody, které vyzařují světlo blízké IR spektru.[13,14]

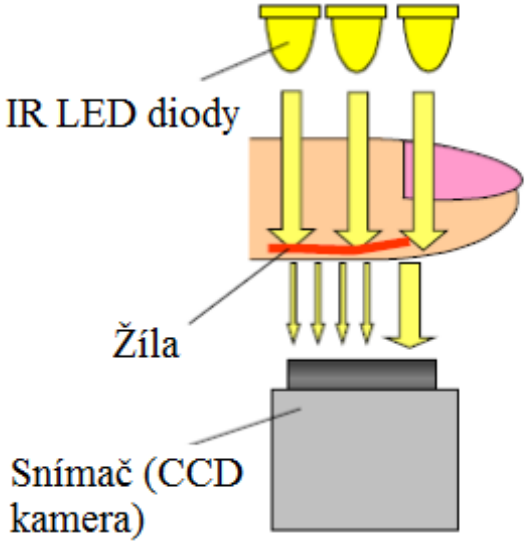


Obrázek 23 Reflexivní metoda[15]

První je metoda **reflexivní,** neboli **metoda s odrazivým světlem**, při které je prst ozařován zespodu. Tato metoda využívá nepatrných rozdílů intenzity světla, které vznikají při odrazu tohoto světla. Výhoda této metody spočívá v komfortu pro uživatele, jelikož je prst osvětlován a snímán z jedné strany, může být tento skener minimalizován na poloviční velikost oproti skenerům, které využívají transmisivní metodu. Nevýhodou je ovšem jistá nečitelnost snímaného obrazu (viz Obrázek č. 22), a to z toho důvodu, že je výsledný obraz málo kontrastní a je tak zapříčiněna složitá extrakce žil.[13,14]

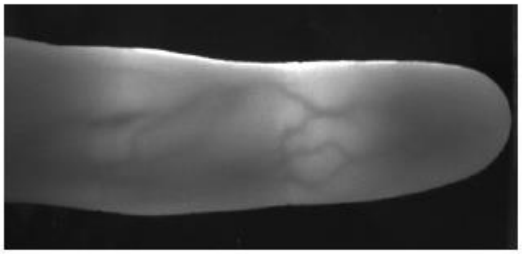


Obrázek 24 Obraz prstu pořízený reflexivní metodou [15]

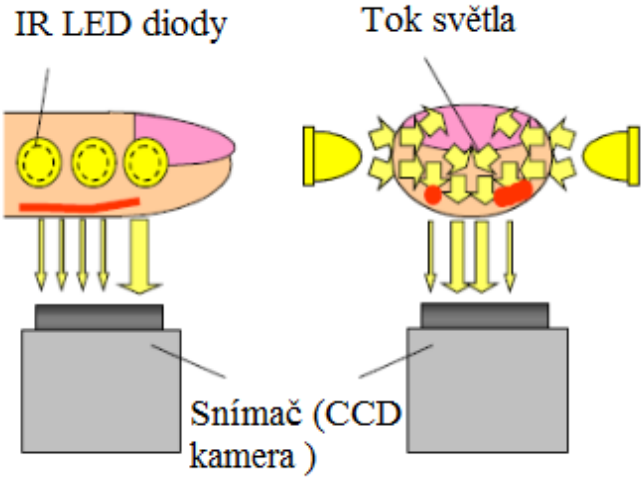


Obrázek 25 Transmisivní metoda[15]

Druhou metodou je metoda **transmisivní,** neboli **metoda s prostupujícím světlem**, při které je prst ozařován svrchu. Jelikož IR světlo prostupuje skrz prst, je výsledný obraz velice kontrastní a lze z něj lépe vyčíst struktura žil (viz Obrázek č. 26). [13,14,15]

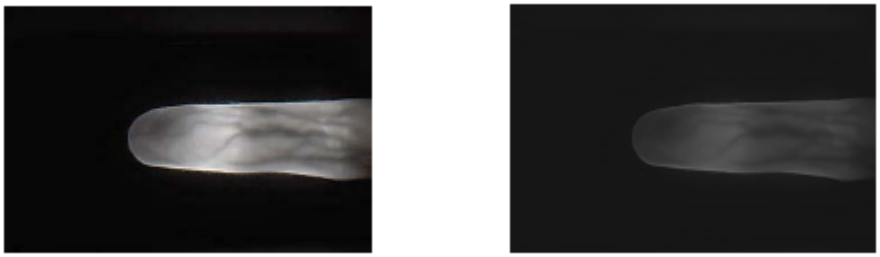


Obrázek 26 Obraz prstu pořízený tansmisivní metodou [15]



Obrázek 27 Metoda bočního světla[15]

U třetí metody se využívá **bočního světla**. Tato metoda je kompromisem dvou zmíněných metod. Je u ní zachován kvalitní kontrast a kompaktnost snímače. [13,14,15]



Obrázek 28 Originální obraz (vlevo), normalizovaný obraz (vpravo) [16]

Originální obraz je třeba normalizovat, abychom získali obraz, jehož střední hodnota a rozptyl intenzity budou odpovídat požadavkům. Dále pak dochází k extrakci struktury žil a jejich následné zpracování.

4.2 Využití v praxi

V současné době se využití skeneru žilního řečiště neustále zvyšuje. Jako první se na trhu s bezpečnostními prvky objevily skenery sloužící pro identifikaci u vstupních dveří. S postupem času se tato technologie začala vyvíjet a skenery se začaly minimalizovat, proto se dnes můžeme setkat se skenery sloužící k ověření identity při přihlašování k osobním účtům v počítači. Skenery žilního řečiště našly hlavní uplatnění v Japonsku, kde tamní banka Bank of Tokio-Mitshubishi zavedla ATM bankomaty, které tuto technologii využívají. Dalším příkladem je nahrazení čipových karet ve finančním institutu v Singapuru nebo kontrola přístupu zaměstnanců banky First Bank Puerto Rico.[3,13,14]

Obrázek 29 ATM bankomat se skenerem žilního řečiště[17]

Díky značné minimalizaci skeneru lze předpokládat, že se tyto skenery začnou využívat v automobilovém průmyslu, kde by mohli nahradit stávající zámky. Nebo v mobilních telefonech, kde by tyto skenery umožnily bezpečné platební transakce.[13]

Obrázek 30 Dveřní systém automobilu[13]

4.3 Porovnání s ostatními biometrickými systémy

V porovnání s ostatními nejpoužívanějšími biometrickými metodami se autentizace za pomoci žilního řečiště umisťuje na špici. To hlavně díky jednotlivým parametrům, které jsou v celkovém shrnutí lepší než u ostatních.

Struktura žilního řečiště je u všech lidí odlišná, jedinečná a neměnná, stejně je tomu tak i u dalších metod jako jsou otisky prstů, DNA, oční duhovky a sítnice. Ostatní využívané metody zmíněné v tabulce č. 2. a 3., jsou na tom o poznání hůře.

Další výhodou, která staví žilního řečiště do popředí je automatické rozpoznání živosti. Díky tomuto rozpoznání je metoda odolná vůči pokusům o padělání reálné vlastnosti, jako tomu často bývá u otisků prstů.

Pokud se zaměříme na přijatelnost ze strany uživatelů, je žilní řečiště jedna z nejlepších voleb. Optimálně by skenery měly být rychlé, přesné, odolné vůči nečistotám a jiným nepříznivým vlivům a zároveň cenově dostupné. Z hlediska hygienického by bylo nejlepší použití bezkontaktních skenerů, které na sobě nezanechávají nečistoty jako je to u kontaktních snímačů.

Tabulka 2 Porovnání základních biometrických metod[18]

Biometrie	jedinečnost	univerzálnost	stálost	dostupnost	přesnost
Žilní řečiště	V	V	V	S	V
DNA	V	V	V	N	V
Otisk prstu	V	V	V	S	S
Geometrie ruky	V	S	S	S	N
Duhovka	V	V	V	S	V
Sítnice	V	V	V	N	V
Obličej	S	V	S	V	S-V*
Podpis	N	N	N	V	N
Stisk kláves	N	N	N	S	N
Hlas	N	S	N	S	N

Tabulka 3 Porovnání základních biometrických metod[18]

Biometrie	přijatelnost	odolnost	rychlost	cena
Žilní řečiště	V	V	V	S
DNA	V	V	N	V
Otisk prstu	V	V	S	S
Geometrie ruky	S	S	S	N
Duhovka	V	V	S	V
Sítnice	V	V	N	V
Obličej	V	S	V	S-V*
Podpis	N	N	V	N
Stisk kláves	N	N	S	N
Hlas	S	N	S	N

Vysvětlivky k tabulce:

V – vysoká (zelená – považováno za kladné), **S – střední** (oranžová – považováno za neutrální), **N – nízká** (červená – považováno za nepříznivé), * – ovlivněno aplikací, pro kterou je určeno a také je důležité přihlédnutí k použité technologii.

4.4 Výhody a nevýhody skeneru žilního řečiště

Výhody:

- Rychlé vyhodnocení identifikace i verifikace.
- Možnost multimodálního provedení.
- Žilní řečiště je neměnné po celý život a je odlišné i u jednovaječných dvojčat.
- Žíly jsou skryty pod pokožkou, tím pádem je jejich padělání obtížnější.
- Hodnoty FAR a FFR u jednotlivých metod jsou přijatelně nízké.
- Velká akceptace u uživatelů biometrických systémů, udává se takřka 100%.
- Možnost provedení v kontaktní i bezkontaktní podobě.
- Rychlost snímání a vyhodnocení je zhruba 1-1,5s.
- Automatické rozpoznání živosti snímaného řečiště.[2,3]

Nevýhody:

- Poměrně vysoká cena.
- Některé skenery jsou náchylné na okolní světlo, které ovlivňuje kvalitu snímku.
- Nízká nabídka skenerů na našem trhu.
- Uživatelé upřednostňují již zaběhnuté identifikační metody. [2,3]

Tato kapitola seznámila čtenáře se základním principem fungování, který je u všech metod snímání žilního řečiště podobný, konkrétně se zaměřila na popis segmentace, vyhlazení a redukci šumu, lokální prahování a postprocessing. Dále byla kapitola zaměřena na porovnání jednotlivých metod s výčtem jednotlivých výhod a nevýhod skeneru žilního řečiště.

II. PRAKTICKÁ ČÁST

5 SKENER ŽILNÍHO ŘEČIŠTĚ

Pro zpracování praktické části byl vybrán skener žilního řečiště od firmy Safran Morpho ze série **MorphoAccess® VP Series**, konkrétně **MorphoAccess® VP-Bio**. Konkrétně tento typ skeneru provádí svou identifikaci za pomocí dvou biometrických vlastností, jedná se tedy o čtečku multimodální. K autentizaci osob tedy využívá struktury žilního řečiště na druhém článku prstu ruky a zároveň ověřuje shodu otisku prstu s referenční šablonou. Tento skener je jeden z mála dostupných skenerů žilního řečiště na českém trhu.

Obrázek 31 MorphoAccess® VP-Bio

Dalo by se říct, že skener je novinkou na trhu, poprvé se tento skener představil v roce 2010 na výstavě Security Essen v Německu, kde také hned získal ocenění Security Essen Innovation Award 2010, toto ocenění získal díky propojení dvou biometrických metod v jednu. MorphoAccess VP je tedy prvním multimodálním skenerem. V roce 2011 byl tento produkt označen jako nejlepší produkt přístupové techniky a odnesl si tak ze Švédska ocenění Detector International Award 2011. O rok později získal tento skener v Las Vegas další ocenění, konkrétně SIA Best New Product Award 2012. Není tedy zapotřebí diskutovat o tom, jestli jsou multimodální skenery budoucností bezpečnostních technologií.

5.1 Výrobce

Výrobcem skeneru je nadnárodní francouzská společnost Safran Morpho. Tato společnost působí na trhu od roku 2007, ovšem pod názvem Sagem Sécurité. V květnu roku 2010 získala firma nový název a to již zmíněný Safran Morpho, to z toho důvodu, že firma vzala pod svá křídla společnost Morpho Systems SA, která se zabývala výrobou skenerů se zaměřením na otisky prstů již od roku 1980.

Tato firma dnešním dnem zaměstnává přes 8400 lidí ve více jak 40 zemích, 85 dceřiných společnostech takřka na celém světě. Příjmy této společnosti se odhadují na 1,5 bilionu euro ročně. Safran Morpho investuje do vývoje a integrace biometrických systémů každým rokem 10% ze svého obratu, díky tomu se tato společnost stala číslem jedna na evropském trhu v oblasti bezpečnostního řešení.

Mimo jiné se tato společnost díky svému snažení a velkým investicím do rozvoje zasloužila o posty:

- Číslo jedna ve světě v oblasti identifikačních karet s integrovanými biometrickými prvky.
- Číslo jedna ve světě v oblasti ABIS (Automated Biometrics Identification System), v překladu automatizované biometrické identifikační systémy se zaměřením na otisky prstů, oční duhovky a rozpoznávání tváře.
- Číslo jedna ve světě v oblasti EDS (Explosive Detection Systems), v překladu systém pro detekci výbušnin, konkrétně pro cestovní zavazadla.
- Číslo dvě ve světě v oblasti herních a sázkových terminálů.
- Číslo tři ve světě v oblasti čipových karet.
- Světový lídr v oblasti pro stopovou detekci výbušnin.

5.2 Využití skeneru žilního řečiště

Skenery žilního řečiště, od firmy Morpho se vyrábí ve třech základních provedeních, jednotlivé provedení můžeme vidět na obrázku č. 32. Tyto typy skenerů mají svá konkrétní využití v určitých oblastech. Jedná se o skenery MorphoSmart™ FINGER VP OEM Series, MorphoSmart™ FINGER VP DESKTOP Series a MorphoAccess®VP Series. V následujících pasážích jsou uvedeny příklady jejich použití.

Obrázek 32 Skenery žilního řečiště [22]

První skener nese označení MorphoSmart™ FINGER VP OEM Series. Tento typ skeneru je určen především pro využití v přístupové oblasti, konkrétněji se nabízí využití u přístupových terminálů, bankomatů, mobilních zařízení pro kontrolu identity a bezpečné platební transakce.

Druhý skener nese označení MorphoSmart™ FINGER VP DESKTOP Series. Tento typ skeneru je více ergonomický, proto nalezne své využití spíše v oblasti desktopových aplikací. Jde tedy o logický přístup do určitých programů a webových aplikací, například by se mohlo jednat o internetové bankovnictví nebo kontrolu identity a také se jedná o přístup k samotnému PC.

Třetí typ skeneru nese označení MorphoAccess®VP Series. Tento skener nalezne využití především v kontrole fyzického přístupu. Tento skener se vyrábí jak ve verzi s označením VP-Bio a VP-Dual. Verze VP-Dual umožňuje uživatelům provádět verifikaci a to díky zabudované čtečce bezkontaktních ID karet, která zároveň navyšuje úroveň zabezpečení. VP-Bio je ochuzen o možnost provádět verifikaci.

5.3 Přesnost skeneru žilního řečiště

V praxi se můžeme setkat s různými technologiemi snímání, odlišují se ovšem ve způsobu vyhodnocování a tedy i v přesnosti. Je tedy důležité se řídit parametry FAR a FRR, neboli pravděpodobností chybného přijetí a pravděpodobností chybného odmítnutí. Jelikož se na trhu vyskytuje spousta skenerů, ať už to jsou kvalitní nebo i nekvalitní snímače, je třeba porovnat tyto hodnoty přesnosti mezi sebou.

Hodnota FAR se u skeneru otisku prstu pohybuje okolo 10^{-4} až 10^{-6}, FRR mezi 10^{-2} až 10^{-3}. Tyto hodnoty jsou u samotného skeneru žilního řečiště až 10x lepší. Ovšem pokud hovoříme o multimodálním skeneru, hodnota díky propojení právě s otisky prstů narůstá a v důsledku hodnota FAR může dosahovat prahové úrovně 10^{-8}.

5.4 Technické parametry skeneru MorphoAccess® VP-Bio

Tabulka 4 Charakteristické vlastnosti skeneru[20]

Charakteristika	
Technologie	Multimodální skenování žilního řečiště a otisku prstu Snímá obě vlastnosti ve stejnou chvíli.
Rozměry	ŠxVxD = 90x160x125mm Váha: 515g
Senzor	Optický senzor
CPU	Dvoujádrový procesor ARM9 s jádry @200MHz a @400MHz
Příslušenství	Barevný LED indikátor aktuálního stavu Zvuková signalizace
Napájení	Externí 9V - 16V SS (1A min @12V) POE (RJ45 nebo kabelové připojení)

Tabulka 5 Vlastnosti skeneru[20]

Vlastnosti	
Metody ověřování	1:N - identifikace
Kapacita uživatelů	Standartně 1 - 5000 uživatelů S licencí 1 - 10 000 uživatelů
Bezpečnost	FAR nastavitelná od 10^{-2} do 10^{-8} Detekce odcizení a narušení (Tamper)
Čas rozpoznání	1s při počtu uživatelů do 1-500 1,5s při počtu uživatelů do 1-5000

Tabulka 6 Možnosti propojení a způsoby komunikace[20]

Rozhraní	
LAN	Ethernet 10/100 Bezdrátové připojení pomocí Wi-Fi™ USB dongle WEP a WPA šifrování SSL certifikace na TCP/IP
Kontrola vstupu – output	Wiegand, Dataclock ISO 2 (pro připojení k přístupovému systému), RS485 (pro sběrnicové zapojení)
Kontrola vstupu – input	LED in

Tabulka 7 Odolnost vůči okolním vlivům[20]

Odolnost vůči okolním vlivům	
Stupeň krytí	IP65 pro venkovní instalaci
Odolnost vůči teplotám	Provozní: -10°C do 50°C Skladová: -20°C to 70°C
Odolnost vůči vlhkosti	Provozní: 0 % - 80 % (bez kondenzace) Skladová: 0 % - 95 %

Tabulka 8 Certifikace[20]

Certifikace	
Kvalita senzoru	FBI PIV IQS
Algoritmus pro otisk prstu	FIPS 201, MINEX
EMC / bezpečnostní standarty	CE, CB, FCC, NF EN 60825-1 2008-01 (Laser Safety)
Standarty pro životní prostředí	RoHS, REACh, WEEE

5.5 Indikace LED diody skeneru

Skener využívá indikace různých stavů pomocí LED diody a zvukové signalizace. Následující tabulky obeznámí čtenáře s jednotlivými indikačními stavy. Zároveň tabulky objasní jejich konkrétní zobrazení pomocí diody a zvukové signalizace. Tato dioda konkrétně zobrazuje barvy zelenou, červenou, žlutou, modrou, azurovou a fialovou. Jedna barevná kulička v tabulce představuje aktuální barvu a dobu svitu 0,5s.

Tabulka 9 Možné indikační stavy[21]

Indikace	Popis
	Blikání – 1s OFF a 0,5s ON
	Rychlé blikání – 0,5s OFF a 0,5s ON
	Pomalé blikání – 1s OFF a 1s ON

Tabulka 10 Přístupové událsti[21]

Událost	LED indikace	Zvuková signalizace
Přístup povolen		Vysoký tón – 1s
Přístup odmítnut		Nízký tón - 1s
Systém čeká na vložení prstu		Není
Prst byl odejmut ze skeneru příliš brzo		Není

Tabulka 11 Ostatní indikační stavy[21]

Událost	LED indikace	Zvuková signalizace
Prázdná databáze		Není
Nesprávná pozice prstu na skeneru		Není
Chybné spuštění skeneru		Není
Proces konfigurace, updatu		Není
Bezpečné odejmutí USB		Dva střední tóny
Anti-tamper nebo anti-pulling alarm		Nízký tón
Změna velikosti vstupních dat		Nízký tón – 1s
Čekání na prst, proces snímání		Není
Dokončení snímání		Vysoký tón - 0.5s
Požadavek na odejmutí prstu, s opětovným vložením		Není
Skenování prstu bylo úspěšné		Není
Registrace byla úspěšná		Není
Registrace biometrických dat je v procesu		Není

5.6 Způsoby propojení skeneru s PC

Skener lze propojit s počítačem několika způsoby:

- Přímým propojením za pomocí Ethernet kabelu.
- Propojením za pomocí dvou Ehthernet kabelů a switche.
- Připojením do sítě LAN s možností využití DHCP.
- Propojení s využitím Wi-Fi USB tokenu.

Ve všech těchto případech je důležité nastavovat hodnoty IP, které definuje výrobce.

Tabulka 12 Nastavení IP[21]

IP adresa	Parametr	Hodnota
Statická (default)	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>

5.7 Software Easy2enroll

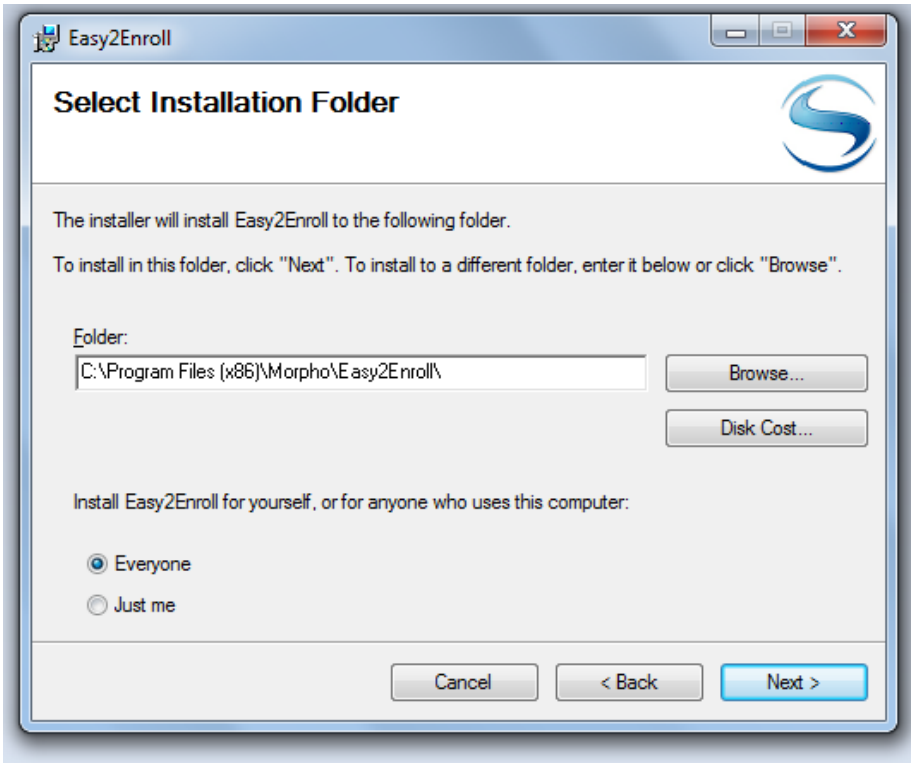
Tento software, je dodávaný společně se skenerem žilního řečiště od firmy Morpho. Hlavním úkolem tohoto softwaru je tvorba přehledné databáze a její následná správa. V podstatě se jedná o evidenci všech uživatelů, kteří tento skener hodlají využívat. Níže si popíšeme jednotlivé kroky, při práci v tomto programu a objasníme tak základní postupy například při registraci nového uživatele.

5.7.1 Instalace

Jako je tomu u každého softwaru, prvním krokem je vždy instalace. Instalace softwaru Easy2Enroll probíhá v několika krocích:

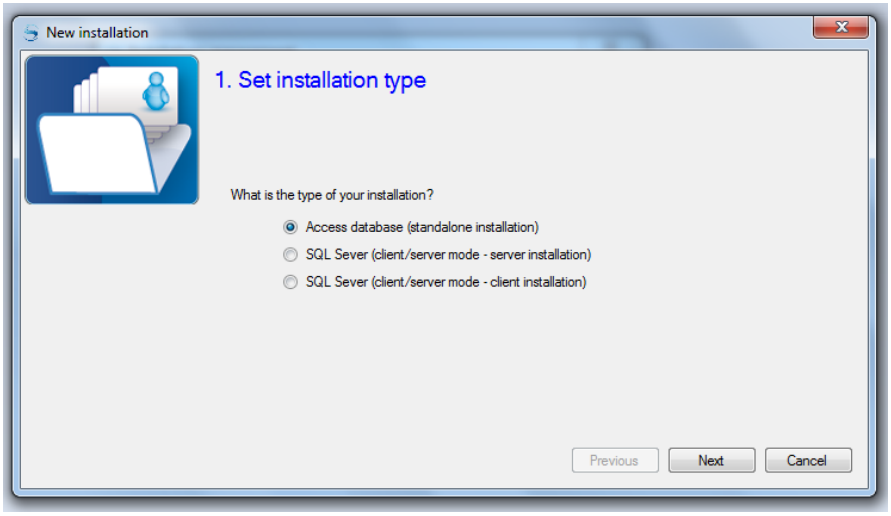
- Instalace databázového enginu, který umožňuje tvorbu databáze a následné zacházení s ní.
- Potvrzení licenčních smluv.

- Umístění programu na pevném disku a nastavení přístupu pro administrátora (správce systému) nebo pro všechny uživatele počítače.



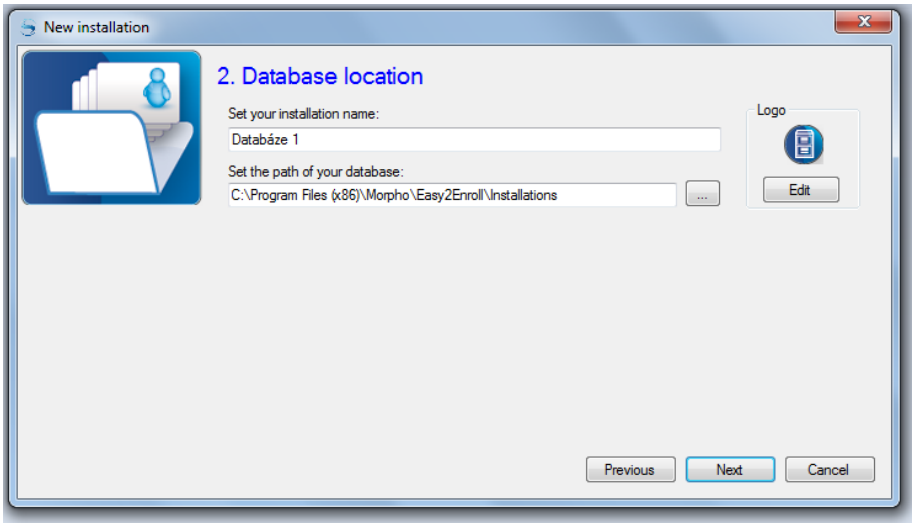
Obrázek 33 Umístění programu

- Instalace softwaru.
- Výběr jazyka programu. Dostupná je angličtina, francouzština a španělština.
- Zvolení typu instalované databáze. Na výběr je ze tří položek a to pro samostatnou instalaci a pro spárování s SQL serverem, kde můžete zvolit serverovou nebo klientskou verzi instalace.



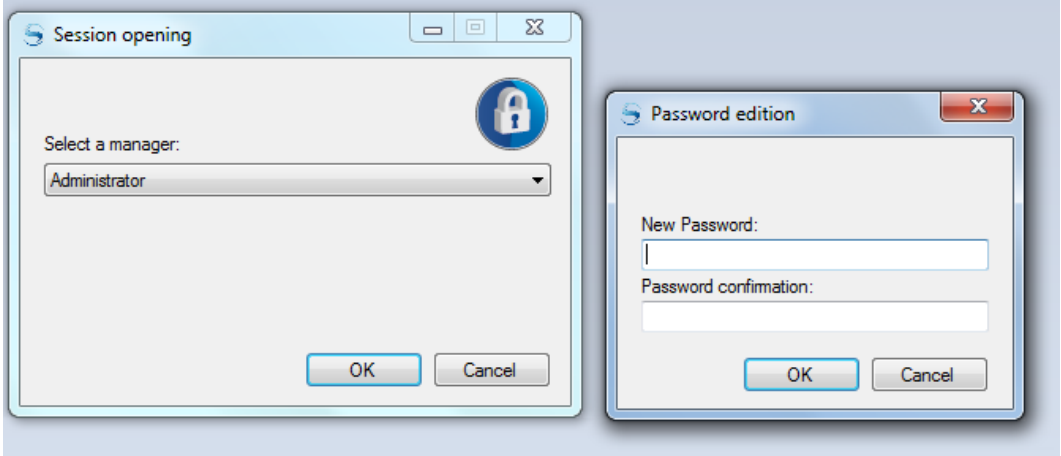
Obrázek 34 Nastavení typu databáze

- Umístění databáze na pevném disku a zvolení názvu.



Obrázek 35 Umístění a název databáze

- Nastavení pracovních dnů pro přehlednější práci s časovými zónami.
- Vytvoření administrátorského účtu. Tento účet má přístup ke všem činnostem, které se v programu nacházejí. Uživatel si zvolí typ účtu a to konkrétně administrátorský a zároveň si vymyslí své heslo k tomuto účtu.



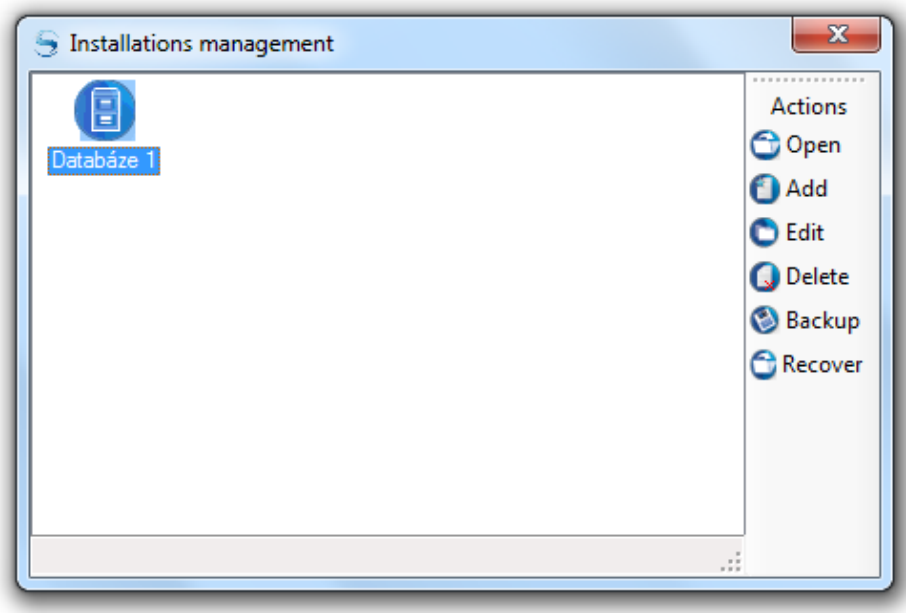
Obrázek 36 Registrace administrátorského účtu

- Po úspěšné instalaci se na ploše vytvoří ikona Easy2Enroll.

5.7.2 Uživatelské prostředí

Po spuštění programu se na obrazovce objeví editační pole databází (viz obrázek 37). Jelikož jsme při instalaci již jednu databázi vytvořili, je možné ji otevřít a pracovat s jejím obsahem. Pokud chceme vytvořit databázi novou, stačí zvolit Add a můžeme si nastavit její umístění a typ jako již ve výše zmíněných krocích. Dále se zde nachází funkce Edit pro

úpravu názvu a umístění, Delete pro odstranění, dále Backup a Recover pro vytvoření zálohy a její opětovné otevření.



Obrázek 37 Editační pole databází

Po otevření databáze po nás bude program požadovat zvolené heslo k administrativnímu účtu. Při úspěšném přihlášení se zobrazí uživatelské menu.

Obrázek 38 Uživatelské menu

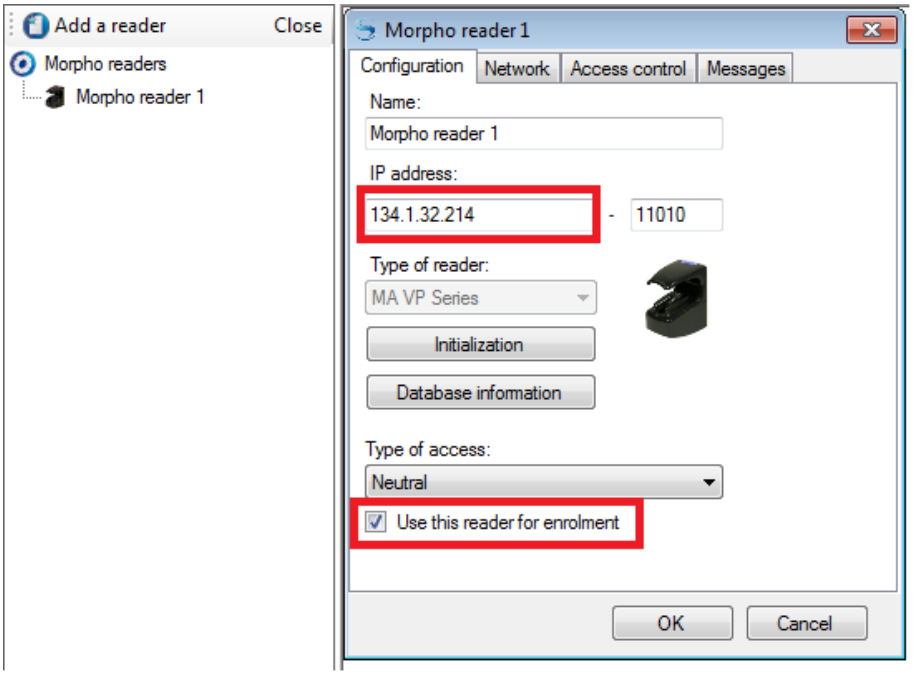
V uživatelském menu můžeme vidět dvě základní lišty, pomocí kterých můžeme upravovat nastavení programu, editovat obsah databáze a měnit nastavení připojeného skeneru. První panel obsahuje záložky File, Viev, Tools, Preferences, Windows a Help. Záložka **File** umožňuje změnu aktuálního hesla, dále odhlášení a vypnutí programu. Pomocí

záložky **Viev** můžeme měnit vzhled programu. Záložka **Tools** umožňuje nastavení událostí, tvorbu a tisk šablon karet a správce licencí, pomocí kterého můžeme tento software updatovat. Pomocí **Preferences** můžeme nastavovat a upravovat základní konfiguraci systému, práh citlivosti, RFID karty, odesílání záznamů na e-maily a synchronizaci. Záložka Windows umožňuje nastavení ikon a aktivních oken. Záložka **Help** obsahuje uživatelský manuál a informace o programu.

Pomocí druhé lišty můžeme ovládat a konfigurovat obsah nastavení databáze a skeneru. Lišta obsahuje záložky Settings, Schedule and Rights, Users, Events, Map a Administration. Záložka **Settings** slouží ke správě skenerů. **Schedule and Rights** umožňuje nastavování přístupových práv skupin a časových zón. Záložka **Users** obsahuje vytvoření nového uživatele, seznamy uživatelů a jejich vyhledávání, obnovení a import seznamů. **Events** obsahuje přehled přístupových událostí. Map umožňuje editaci a otevírání map. Položka **Administration** obsahuje správu a nastavování práv uživatelských profilů.

5.7.3 Propojení skeneru s programem

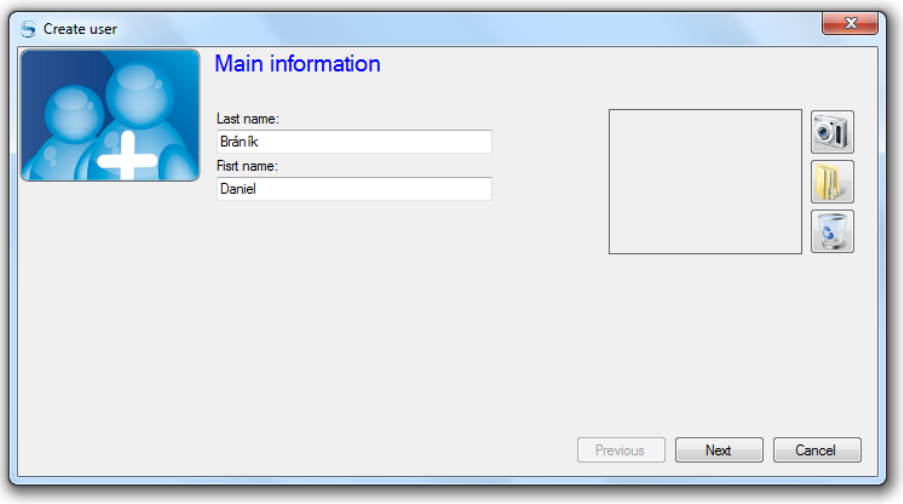
Abychom mohli se skenerem vůbec pracovat, musíme jej propojit s programem. K tomu využijeme položku Add a reader, která se nachází v levé části uživatelského menu (Obrázek 38.). Po kliknutí na tuto položku se zobrazí nastavení skeneru. Ovšem než začneme s nastavováním, ujistíme se, že je skener správně zapojen (napájení, ethernet). Při nastavování skeneru je důležité, abychom nastavili IP adresu 134.1.32.214 a zaškrtli položku Use this reader for entolment (Obrázek 39.). Ostatní záložky není potřeba měnit, následně skener pomocí tlačítka Initialization inicializujeme a potvrdíme tlačítkem OK. Skener by měl začít komunikovat s programem. Pokud jsme úspěšně zvládli tento krok, na pozadí uživatelského menu se zobrazí nápis Active instalation a skener začne indikovat tento stav žlutým problikáváním (indikace prázdné databáze).



Obrázek 39 Konfigurace skeneru

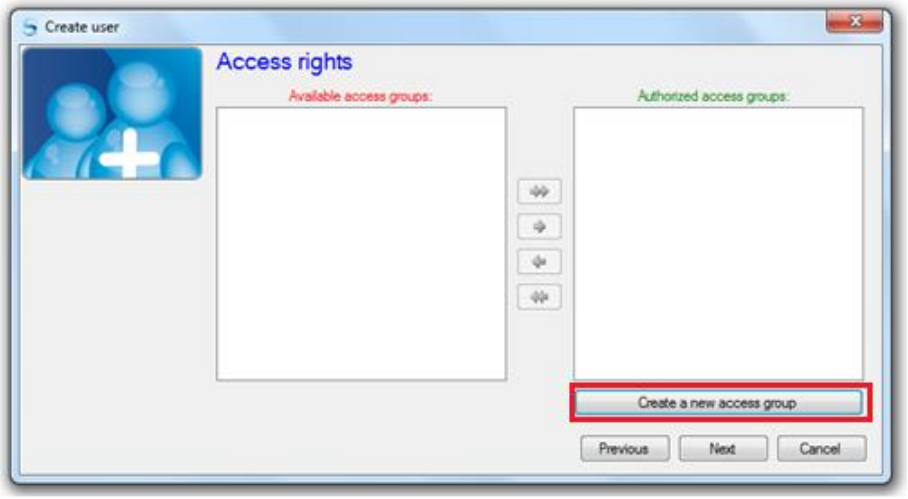
5.7.4 Registrace nového uživatele

Pro registraci nového uživatele zvolíme záložku Users-Create user. Následně se otevře okno Main information, kde zadáme jméno a příjmení uživatele a pokud možno i jeho fotku. Potvrdíme tlačítkem next.

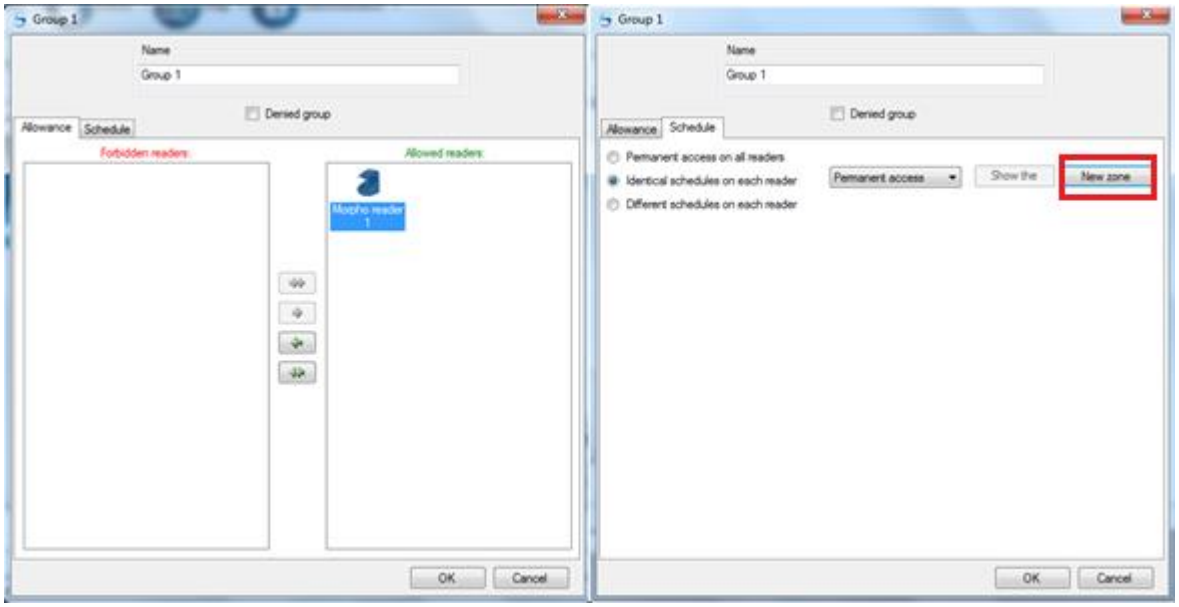


Obrázek 40 Main information

Nyní se zobrazí položka s přístupovými právy. Tato položka je prázdná a proto musíme zvolit volbu Create a new access group, která nám umožní vložit již přidaný skener (Obrázek 41. a 42.).



Obrázek 41 Access rights

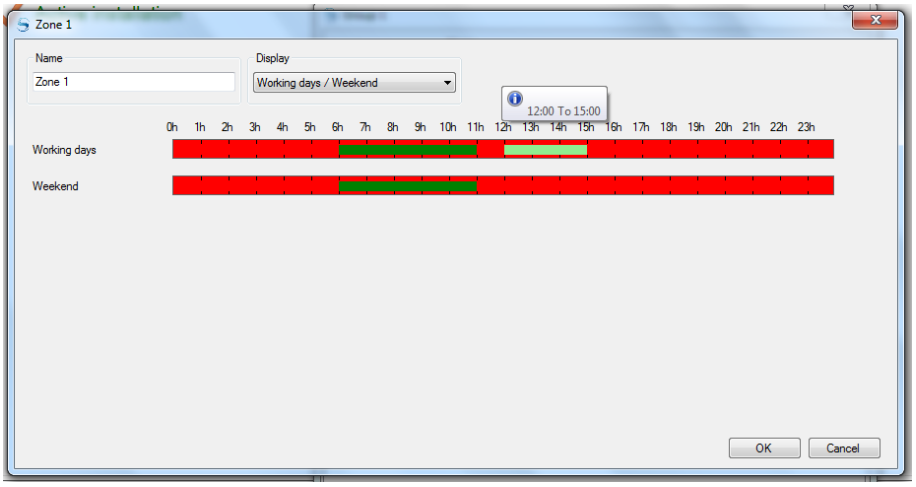


Obrázek 42 Create a new access group

Create a new access group obsahuje dvě záložky, v první Allowance přidáme již spárovaný skener a v záložce Schedule nastavíme požadované časové zóny pro tento skener. Položka Schedule nám dává na výběr ze tří možných nastavení a to konkrétně permanentní přístup bez časového omezení, dále vlastní nastavení časových zón a ostatní nastavení.

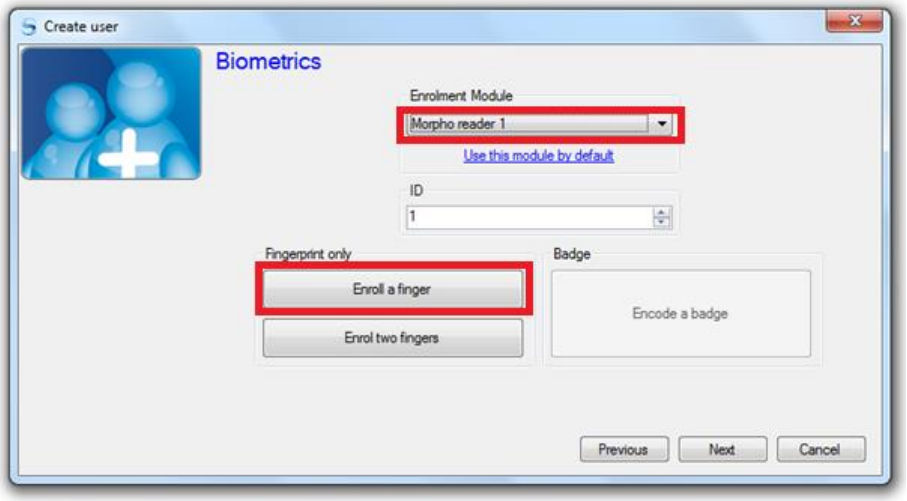
Pokud tedy zvolíme vlastní nastavení časových zón (New zone), zobrazí se pole časových úseků, se kterým můžeme libovolně manipulovat (Obrázek 43.). Položka Display nám usnadňuje práci s časovými zónami, po rozkliknuti této položky máme na výběr ze tří různých zobrazení časových zón. Konkrétně se zobrazují všechny jednotlivé dny (pondělí až neděle), pracovní dny a víkend nebo všechny dny v jedné liště. Pokud jsme nastavili

požadované časové úseky, můžeme tento krok potvrdit tlačítkem OK a pokračovat k dalšímu kroku.



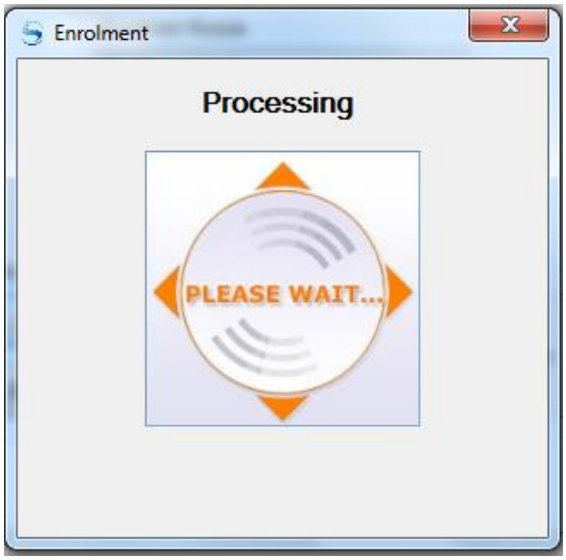
Obrázek 43 Nastavení časových zón

Dalším krokem je načtení biometrických údajů do databáze. V tomto kroku je důležité zvolit připojený skener v políčku Enrolment module, konkrétně Morpho reader 1 a následně stisknout Enroll a Finger.



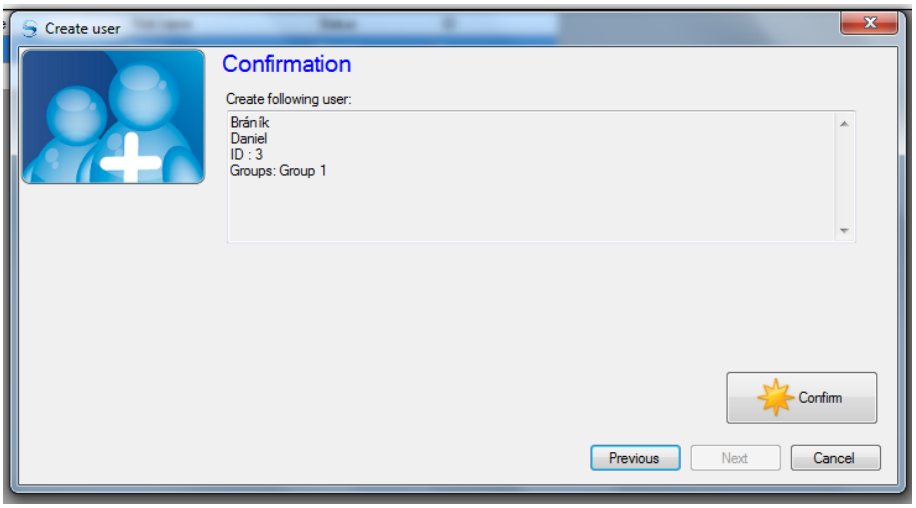
Obrázek 44 Nastavení biometrických údajů

Na obrazovce se zobrazí políčko processing (Obrázek 45.) a skener začne blikat fialově. Tímto nás skener vyzívá k přiložení prstu na snímač. Prst musí být vložen ve správné poloze a to třikrát aby mohl vytvořit co nejlepší referenční šablonu. Při bezchybném sejmutí vzorku se ozve tón a indikační LED dioda zasvítí zeleně.



Obrázek 45 Proces skenování

Posledním krokem je potvrzení všech předchozích kroků a ověření vložených údajů (Obrázek 46.) tlačítkem Confirm.



Obrázek 46 Potvrzení vložených údajů

6 LABORATORNÍ ÚLOHA

Univerzita Tomáše Bati ve Zlíně, Fakulta technologická Ústav bezpečnostního inženýrství			
Jméno a příjmení		Ročník / Skupina	
Předmět	Biometrické systémy	Datum měření	
		Datum odevzdání	
Název úlohy	Skener MorphoAccess VP-Bio	Hodnocení	

Teoretická část:

1. Uveďte základní dělení biometrické autentizace.
2. Uveďte alespoň pět příkladů biometrické autentizace.
3. Vysvětlete pojem identifikace.
4. Vysvětlete pojem verifikace.
5. Vysvětlete pojem multimodální systém.
6. Vysvětlete pojmy FAR a FRR.
7. Vysvětlete, k čemu slouží nastavení prahu citlivosti.
8. Kde konkrétně můžeme snímat strukturu žilního řečiště?
9. Uveďte čtyři základní etapy, prováděné při snímání struktury žilního řečiště.

Praktická část:

1. Seznamte se se skenerem žilního řečiště, s funkcemi indikační LED diody a softwarem Easy2Enroll.
2. V programu Easy2Enroll vytvořte novou databázi.
3. Spárujte skener žilního řečiště s programem Easy2Enroll.
4. Vytvořte nového uživatele a nastavte časové zóny.
5. Vyzkoušejte si další funkce programu a ověřte, zda vás skener opravdu rozpozná.

7 VYPRACOVÁNÍ LABORATORNÍ ÚLOHY

Univerzita Tomáše Bati ve Zlíně, Fakulta technologická Ústav bezpečnostního inženýrství			
Jméno a příjmení	Daniel Bráník	Ročník / Skupina	3b2x
Předmět	Biometrické systémy	Datum měření	15.3.2014
		Datum odevzdání	22.3.2014
Název úlohy	Skener MorphoAccess VP-Bio	Hodnocení	

Teoretická část:

1. Uveďte základní dělení biometrické autentizace.
2. Uveďte alespoň pět příkladů biometrické autentizace.
3. Vysvětlete pojem identifikace.
4. Vysvětlete pojem verifikace.
5. Vysvětlete pojem multimodální systém.
6. Vysvětlete pojmy FAR a FRR.
7. Vysvětlete, k čemu slouží nastavení prahu citlivosti.
8. Kde konkrétně můžeme snímat strukturu žilního řečiště?
9. Uveďte čtyři základní etapy, prováděné při snímání struktury žilního řečiště.

Praktická část:

1. Seznamte se se skenerem žilního řečiště, s funkcemi indikační LED diody a softwarem Easy2Enroll.
2. V programu Easy2Enroll vytvořte novou databázi.
3. Spárujte skener žilního řečiště s programem Easy2Enroll.
4. Vytvořte nového uživatele a nastavte časové zóny.
5. Vyzkoušejte si další funkce programu a ověřte, zda vás skener opravdu rozpozná.

Teoretická část:

1. Biometrická autentizace využívá jedinečných vlastností lidského těla, jde tedy o dělení s využitím anatomických/fyziologických nebo behaviorálních vlastností.
2. Žilní řečiště, otisky prstů, oční duhovka, rozpoznávání tváře, podpis, hlas.
3. Identifikace je určitý proces, který má za úkol zjištění identity osoby na základě jejich shod či rozdílů v daných vlastnostech či chování. Identifikace se také označuje jako porovnání jeden k mnoha (1:N) nebo rekognice.
4. Verifikace je proces, který má za úkol porovnat předložený biometrický vzorek s konkrétní šablonou uloženou v databázi. Taktéž se můžeme setkat s označením jedna k jedné (1:1).
5. Multimodální systém využívá více biometrických vlastností nebo více příznaků jedné biometrické vlastnosti k ověření identity.
6. Pravděpodobnost chybného odmítnutí, neboli FRR (False Rejection Rate) udává, s jakou pravděpodobností bude oprávněný uživatel, který má již v databázi svou biometrickou šablonu chybně odmítnut.

   Pravděpodobnost chybného přijetí neboli FAR (False Acceptance Rate) udává, s jakou pravděpodobností bude neoprávněný uživatel, který nemá v databázi svou biometrickou šablonu chybně přijat.
7. Práh citlivosti umožňuje nastavovat jistou hranici mezi hodnotami FAR a FRR. Jde tedy o upřednostňování komfortu před bezpečností a naopak.
8. Strukturu žilního řečiště lze snímat na dlani, hřbetu a prstech ruky.
9. Segmentace, vyhlazení a redukce šumu, lokální práhování, postprocessing.

Praktická část:

1. Seznámili jsme se skenerem žilního řečiště, dále s funkcemi indikační LED diody a softwarem Easy2Enroll. Všechny důležité informace jsme našli v uživatelském manuálu a v praktické části BP.

2. Spustili jsme program Easy2Enroll, který byl již nainstalovaný. V přehledném menu jsme zvolili *Add*, následně se otevřelo nové okno s typem databáze. Zvolili jsme tedy možnost *Access database* a pokračovali tlačítkem *Next*. Program po nás požadoval zadání názvu databáze a její umístění, zvolili jsme tedy název *Databáze 2* a umístění jsme ponechali na C:\Program Files

(x86)\Morpho\Easy2Enroll\Installations. Pokračovali jsme tlačítkem *Next*. Dalším bodem bylo nastavení pracovních dnů, ty jsme taky nechali tak jak byly přednastavené, tedy pondělí až pátek. Nakonec jsme vše potvrdili tlačítkem *Confirm* a vytvořili tak novou databázi, kterou bylo možno otevřít, ovšem s podmínkou vložení nového hesla pro administrátorské účely.

3. Pro spárování skeneru žilního řečiště s programem jsme zvolili funkci *Add* a *Reader* v levé části uživatelského menu. Následně se objevilo konfigurační okno, kde jsme nejprve zadali IP adresu 134.1.32.214 a pak zaznačili políčko *Use this reader for enrolment*. Potom jsme tento skener inicializovali a potvrdili tyto kroky tlačítkem *OK*. Skener začal komunikovat s programem a indikační LED dioda začala blikat žlutě, což v tu chvíli znamenalo, že má prázdnou databázi.

4. Nového uživatele jsme vytvořili pomocí tlačítka *Users,* kde jsme zvolili *Create user*. V prvním kroku jsme vyplnili údaje o uživateli. V druhém kroku jsme pomocí tlačítka *Create* a *New access group* přiřadili skener a zároveň jsme v záložce *Schedule* vytvořili časovou zónu. Tyto kroky jsme akceptovali tlačítkem *OK* a pokračovali jsme k dalšímu kroku tlačítkem *Next*. Nyní se otevřelo okno s požadavky na biometrický vzorek. Zvolili jsme spárovaný skener ve výberovém políčku *Enrolment Module* a stiskli jsme tlačítko *Enroll* a *Finger*. Nyní začal skener blikat fialově a na obrazovce se objevilo nové okno, kde bylo napsáno *Processing*. Přiložili jsme tedy třikrát prst na skener, aby mohl vytvořit požadovanou šablonu. To se po chvíli podařilo a v posledním kroku po nás program požadoval potvrzení vložených dat tlačítkem *Confirm*. Tyto data jsme tedy potvrdili a vytvořili tak nového uživatele i s časovými zónami.

5. V poslední části úlohy jsme se podívali na ostatní funkce programu a vyzkoušeli jsme si jak je skener spolehlivý. Přiložili jsme registrovaný prst na snímač a během chvilky skener vydal zvukový tón a rozsvítil se zeleně, čímž indikoval příznivé rozpoznání oprávněného uživatele. Vyzkoušeli jsme přiložit i prst, který nebyl v databázi. Skener na to reagoval zamítnutím přístupu, který byl signalizován jak pomocí tónu, tak indikací červené diody.

Závěr laboratorní úlohy: V rámci této laboratorní úlohy jsme nejprve měli odpovědět na několik otázek, které se týkali biometrie. Museli jsme si tedy projít bakalářskou práci, abychom na ně mohli správně odpovědět. V praktické části jsme postupovali dle vypracovaného manuálu, který jsme našli v praktické části bakalářské práce a seznámili jsme se tak s tvorbou databáze, propojením, registrací nových uživatelů, nastavením časových zón a indikačními stavy, které jsou zobrazovány pomocí LED diody a zvukového signálu.

ZÁVĚR

Dle Maslowovy pyramidy lidských potřeb je bezpečnost na druhém místě. Není tedy od věci, zamyslet se nad konkrétním zabezpečením našeho majetku či zdraví. Důležité je, aby byly při pořizování konkrétních bezpečnostních systémů zvoleny ty, které jsou trhem, a především lidmi, prověřeny. Měly by být opravdu kvalitní a bezproblémové.

Cílem této bakalářské práce bylo objasnit problematiku biometriky, s konkrétním zaměřením na skener žilního řečiště. Teoretická část byla zaměřena na terminologii úzce spjatou právě s touto problematikou, funkčním principem biometrických systémů a také jejich uplatnění v praxi. Dále se práce zaměřila na spolehlivost a přesnost systémů, konkrétně šlo o hodnoty FAR a FRR, které jak bylo zmíněno, určují míru chyb, které ovlivňují právě spolehlivost. Třetí kapitola byla věnována minulosti a vývoji biometrie. Toto historické okénko poodkrylo fakt, že biometrie je stará jako lidstvo samo, a právě díky lidským odlišnostem a dnešním vyspělým technologiím je možné tyto dvě položky skloubit a využít je v náš prospěch. Uplatnění krevního řečiště našlo v bezpečnostním průmyslu své místo poměrně nedávno, zhruba před patnácti lety. V porovnání s některými biometrickými metodami je to v této problematice nováček a stále čeká na prosazení ve své oblasti. Ve čtvrté, a tedy i poslední kapitole teoretické části, byly popsány skenery žilního řečiště. Konkrétně byla tato část věnována funkčnímu principu skenování. Právě v této části bylo dosaženo názoru, že jednotlivé metody, jak pro skenování dlaně, hřbetu či prstu ruky, se příliš nemění. Dále byly shrnuty možnosti využití těchto skenerů v praxi a došlo k porovnání s ostatními biometrickými metodami. Závěrem byly shrnuty jednotlivé výhody a nevýhody.

Praktická část se v úvodu zaměřila na použitý skener žilního řečiště, byly zde zmíněny jeho přednosti a také ocenění, která skener získal za velký přínos v oblasti inovace těchto systémů. V další části se práce orientovala na výrobce tohoto skeneru. Bylo zjištěno, že firma Morpho patří mezi jednu z nejlepších v dané oblasti. Jejím největším přínosem pro danou problematiku je, že investuje několik procent ze svého zisku do vývoje biometrických technologií. Dále bylo zmíněno využití všech nabízených typů skenerů od této firmy, a zároveň následovalo zhodnocení jejich přesnosti. Následující část se zaměřila opět na použitý skener, a obeznámila čtenáře s jeho technickými parametry, indikačním systémem a možnostmi propojení s PC. Následně byla práce zaměřena na software, který je dodáván se skenerem, konkrétně se věnovala instalaci programu, uživatelskému prostředí a obecně práci s tímto programem. Poslední dvě kapitoly praktické části byly věnovány tvorbě laboratorní

úlohy. Do této úlohy byla zahrnuta teoretická část, ve které mají studenti za úkol odpovědět na otázky spjaté jak s biometrií, tak i se skenerem žilního řečiště. Praktická část laboratorní úlohy je zaměřena na práci se skenerem. Po nastudování základních pokynu objasněných v této práci by studenti měli dokázat vypracovat jednotlivé body, které jsou obsahem praktické části.

Tato práce byla vytvořena za účelem obeznámení s biometrickými systémy, konkrétně pak se skenerem žilního řečiště, pro který byla vytvořena v praktické části laboratorní úloha. Tato laboratorní úloha, a zároveň i bakalářská práce, může v budoucnu sloužit jako edukační materiál, který by našel využití při práci se skenerem na laboratorních cvičeních, tak i při tvorbě nových bakalářských či diplomových pracích zaměřených na podobné téma.

SEZNAM POUŽITÉ LITERATURY

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

[2] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

[3] KOVÁČ, Petr. *Ezoterická identifikace, druhy, způsob identifikace, přístrojová identifikační technika, vývoj*. Zlín, 2007. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[4] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2014-01-28]. Dostupné z: http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf

[5] JEN-CHUN, Lee. *A novel biometric system based on palm vein image.* Pattern Recognition Letters. 2012, roč. 33, č. 12.

[6] Famous Scientists: Marcello Malpighi. *Marcello Malpighi* [online]. 2013 [cit. 2014-04-22]. Dostupné z: http://www.famousscientists.org/marcello-malpighi/

[7] Osobnosti: Jan Evangelista Purkyně. *Jan Evangelista Purkyně* [online]. © 1996-2014 [cit. 2014-04-22]. Dostupné z: http://www.osobnosti.cz/jan-evangelista-purkyne.php

[8] Slough history online: Prints of hands and fingers made by W. J. Herschel. *Prints of hands and fingers made by W. J. Herschel* [online]. 2005 [cit. 2014-04-22]. Dostupné z: http://www.sloughhistoryonline.org.uk/ixbin/hixclient.exe?a=query&p=slough&f=generic_objectrecord.htm&_IXFIRST_=1&_IXMAXHITS_=1&t=sl-sl-williamjamesherschel&%3dcms_con_core_identifier=sl-sl-1526_herschelfprint-i-01-000.tif&t=sl-sl-williamjamesherschel&

[9] Galton: fingerprints. *Henry Faulds: the Invention of a Fingerprinter* [online]. 2003 [cit. 2014-04-22]. Dostupné z: http://galton.org/fingerprints/faulds.htm

[10] Famous Psychologists: Francis Galton. *Francis Galton* [online]. © 2014 [cit. 2014-04-22]. Dostupné z: http://www.famouspsychologists.org/francis-galton/

[11] British Broadcasting Corporation: BBC Mundo. *BBC Mundo - Ciencia y Tecnología - Argentina, pionera de la dactiloscopia* [online]. © 2014 [cit. 2014-04-22]. Dostupné z: http://www.bbc.co.uk/mundo/ciencia_tecnologia/2009/11/091027_especial_aportes_al_vucetich_mr.shtml

[12] Encyclopædia Britannica: comptons. *Bertillon, Alphonse* [online]. © 2014 [cit. 2014-04-22]. Dostupné z: http://kids.britannica.com/comptons/art-137305/Alphonse-Bertillon

[13] STAN, Z.Li. *Encyclopedia of biometrics* [online]. Editor S Li, Anil K Jain. New York: Springer, c2009, xxxi s., s. 1-713[cit. 2014-04-22]. ISBN 978-0-387-73002-8. Dostupné z: databáze Springer

[14] DOBIÁŠ, Richard. *Biometrické systémy* [online]. 2006 [cit. 2014-04-22]. Dostupné z: http://www.biometricke-systemy.cz

[15] HASHIMOTO, Junichi. INFORMATION & TELECOMMUNICATION SYSTEMS GROUP, Hitachi, Ltd. *Finger Vein Authentication Technology and its Future*. Kawasaki, Kanagawa, Japan, 2006.

[16] WANG, Kejun. COLLAGE OF AUTOMATION HARBIN ENGINEERING UNIVERSITY. *A novel Finger Vein Pattern Extraction Method Using Oriented Filtering Technology*. Harbin, China, 2010.

[17] *Discovering São Paulo: Bradesco's biometric blood vessel recognition* [online]. 2011 [cit. 2014-04-22]. Dostupné z: http://www.discoveringsaopaulo.com/2011/05/bradescos-biometric-blood-vessel.html

[18] Posterus. SULOVSKÁ, Kateřina. ÚSTAV BEZPEČNOSTNÍHO INŽENÝRSTVÍ, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně. *Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu* [online]. 2011 [cit. 2014-04-22]. Dostupné z: http://www.posterus.sk/?p=11511

[19] *On-line Bible: Kniha Soudců* [online]. 2010 [cit. 2014-04-22]. Dostupné z: http://onlineb21.bible21.cz/bible.php?kniha=soudcu

[20] *MorphoAccess® VP Series: MorphoAccess VP Series Product Technical Datasheet*. Francie, 2012 [cit. 2014-04-22]. Dostupné z:

http://emssa.net/source/content/Safran/MorphoAccess_VP_Series_Product_Technical_Datasheet_Rev01_3.pdf

[21] *MorphoAccess® VP Series: User Guide*. Francie, 2012 [cit. 2014-04-22].

[22] *MorphoAccess® VP Series: About Multimodality* [online]. Francie, 2012 [cit. 2014-04-22]. Dostupné z: http://www.morpho.com/IMG/pdf/Multimodality_EN-5.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

°C	Stupeň celsia
A	Ampér
ABIS	Automated Biometrics Identification Systém
ATM	Automated teller machine
CE	Communauté Européenne
CPU	Central Processing Unit
DNA	Deoxyribonucleic Acid
EDS	Explosive Detection Systems
ERR	Equal Error Rate
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FIPS 201	Personal Identity Verification for Federal Employees and Contractors
FRR	False Rejection Rate
ID	Identification
IP	Internet Protocol
IQS	Image Quality Specifications
IR	Infra Red
LAN	Local Area Network
LED	Light-Emitting Diode
MHz	Megahertz
MINEX	The Minutiae Interoperability Exchange Test
mm	Milimetr

PC	Personal Computer
PIN	Personal Identification Number
PIV	Personal Identity Verification
POE	Power Over Ethernet
REACh	Registrace, evaluace (hodnocení), autorizace (povolování) a omezování chemických látek
RFID	Radio Frequency Identification
RJ45	Registered Jack 45
RoHS	Restriction of the use of certain Hazardous Substances
RS485	Recommended Standard 485
s	Sekunda
SS	Stejnosměrné napětí
SSL	Secure Sockets Layer
SQL	Structured Query Language
TCP	Transmission Control Protocol
Th	Threshold
USA	United States of America
USB	Universal Seriál Bus
V	Volt
WEEE	Waste Electrical and Electronic Equipment
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK