Biometrické identifikační metody

Biometric identification methods

Bc. Libor Staník

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Libor STANÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Biometrické identifikační metody**

Zásady pro vypracování:

1. **Práci zpracujte jako výukový materiál do předmětu Kriminalistické technol a systémy.**
2. **Zpracujte vývoj počítačových technologií s ohledem na možnosti realizace biometrických identifikačních metod.**
3. **Objasněte vztah verifikace versus identifikace.**
4. **Zpracujte kritéria hodnocení a oblast využití biometrických identifikačních systémů.**
5. **Práci doplňte grafickou a obrazovou dokumentací.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Čandík Marek. Objektová bezpečnost II, Univerzita Tomáše Bati ve Zlíně 2004 ISBN 80-7318-217-3.**
2. **Laucký Vladimír. Technologie v komerční bezpečnosti I, Univerzita Tomáše Bat Zlíně 2004, ISBN 80-7318-194-0**
3. **Porada, V. a kol. Kriminalistika, Akademické nakladatelství CERM 2001**
4. **Musil, J. a kol. Kriminalistika, Praha C.H.BECK 2001**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **22. května 2009**

Ve Zlíně dne 20. února 2009

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek,
ředitel ústavu

ABSTRAKT

V této diplomové práci se budu zabývat biometrií, což se jedná o metody jednoznačné identifikace osob na základě fyziologických a behaviorálních vlastností člověka. První část práce objasňuje základní pojmy týkající se biometrie, dále v práci popisuji problematiku elektronického biometrického systému jako celek. Praktická část vytváří přehled jednotlivých metod a principů funkcí biometrické identifikace a také vhodné aplikace do praxe. V praktické části také rozpracovávám nově zavedené biometrické pasy, respektive získávání biometrických informací a zpracování prostřednictvím počítačového programu, který se používá na městských úřadech v oddělení cestovních dokladů.

Klíčová slova: biometrie, identifikace, verifikace, behaviometrika, token, etalon, e-pass

ABSTRACT

In my thesis work I deal with biometrics, whith are methods unique identification of people in terms of physiological and unique properties of human body. In the first part of my work I describe basic conceptions of biometrics, next part I describe problems of electronic biometric systems entire. There is practical part about table of individual methods and tenet of function biometric identification and facility to real life too. The practical part also detail the recently introduced biometric passports or biometric information acquisition and processing through a computer program that is used for municipal authorities in the department of travel documents.

Keywords: biometrics, identification, verification, behavioral, etalon, token, e-pass

Mé poděkování patří zejména panu JUDr. Vladislavu Štefkovi za odborné vedení, poskytnutí odborné literatury, materiálů a ochotné konzultace při zpracovávání práce. Dále děkuji Městskému úřadu ve Valašských Kloboukách, oddělení cestovních dokladů za poskytnuté informace, věnovaný drahocenný čas a poskytnuté materiály.

Dále bych rád poděkoval své rodině za podporu, kterou mi poskytovali během svého studia na Univerzitě Tomáše Bati ve Zlíně.

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.

Ve Zlíně

…….

Podpis diplomanta

OBSAH

ÚVOD

Už v dávné historii si člověk uvědomuje svoje biometrické unikátní vlastnosti. Důkazem toho jsou například otisky dlaní v jeskyních u nástěnných maleb, které měly zpečetit a „podepsat" dílo autora.

Až s rozvojem počítačových technologií se biometrické rozpoznávání stává automatizovaným procesem. Identifikační technologie, podporované výpočetní technikou se velice rychle rozvíjejí a v praxi se setkáváme stále ve větší míře s jejich aplikačním nasazením. Tyto systémy nejsou nijak jednoduché a vznikají občas obavy vyplývající z nepochopení nebo možnosti zneužití citlivých osobních údajů uživatele. V této problematice se setkáváme s nedůvěrou a odpůrci, s různými problémy politického, společenského, právního nebo náboženského charakteru. K nepochopení a obavám dochází velmi zbytečně a je to hlavně důsledkem neznalostí podstaty jednotlivých identifikačních postupů a základů daných informační technologií. Nedůvěru je třeba překonávat a tvrdě šířit a dokazovat, že i takový systém dokáže ochránit nás samotné před dnešní nebezpečnou dobou plné kriminality. Naší snahou je rozvíjet tyto jedinečné identifikační technologie kupředu a více přesvědčovat laickou veřejnost o tom, že právě tyto technologie se snaží zajistit větší bezpečí právě pro ně. Na vývoji nových technologií v tomto oboru je, aby se přicházelo se stále novými a osvědčenými metodami zabezpečení samotných identifikačních systémů. Takový systém se pak stane nezranitelný a neprolomitelný z hlediska pokusů pachatele prolomit a obelstít tento systém a získá tak i větší důvěru u veřejnosti. Následující studijní text shrnuje biometrické identifikační metody od samého počátku a pokusí se objasnit podstatu celé problematiky.

Vývoj počítačových technologií jde stále kupředu a to co se zdálo před několika lety nemožné se stává skutečností a otevírají se nové brány pro rozvoj různých technologií, v našem případě i pro biometrické systémy identifikace člověka. Díky zvýšení rychlosti běžných počítačů a zlepšení srovnávacích algoritmů dochází k rozšíření biometrických systémů a tím se drahé a náročné biometrické metody identifikace stávají levnější a dostupnější i pro komerční sféru. V nedávné době se zavedlo vydávání biometrických pasů.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY BIOMETRIE A TEORIE

Vědní obor zkoumající živé organismy (bio), v našich potřebách zejména člověka a zaměřující se na měření (metric) jeho biometrických vlastností a behaviorálních charakteristik se nazývá biometrie. Tento vědní obor je základem pro celou moji práci, proto si nejprve ujasníme všechny pojmy, které souvisí s touto problematikou a které se budou často vyskytovat v následujícím studijním textu. Slovo biometrika se skládá ze dvou řeckých slov a to konkrétně ze slova *bios=život* a *metron=měření*. Biometrika se zabývá metodami, které vedou k rozpoznání člověka na základě jeho proporcí nebo vlastností. Tyto proporce/vlastnosti jsou unikátní pro každého jedince, tedy každý člověk je v těchto znacích originálem a neexistuje možnost dvou stejných proporcí u dvou jedinců.

Základní názvy pojmů, používané v oblasti biometrie, jsou odvozeny z anglického jazyka a jejich překlad do češtiny bývá občas špatně pochopen. Proto uvádím některé z nich:

- recognition – rozpoznávání člověka použitím vhodné tělesné vlastnosti. Nejde tedy o přímou identifikaci ani verifikaci
- verification – jedná se o pokus biometrického systému potvrdit totožnost jedince, na základě porovnání sejmutého vzorku se vzorkem již uloženým v databázi systému. Uvádí se princip one-to-one.
- identification – jedná se o proces, kdy se biometrický sytém pokouší identifikovat neznámého člověka. Sejmutý vzorek je porovnáván se všemi vzorky uloženými v databázi systému. Uvádí se jako princip one-to-many.
- Authentication – tento pojem lze sloučit s termínem rozpoznávání. Uživatel na konci tohoto procesu zjistí status oprávněný/neoprávněný.

1.1 Verifikace versus identifikace

Jak jsem již zmiňoval výše, význam pojmu verifikace a pojmu identifikace má odlišný význam a z toho plyne, že ověřování identity může probíhat dvojím způsobem. Tyto dva termíny musíme od sebe ve svém významu patřičně rozlišovat a nelze si je plést.

1.1.1 Pojem verifikace

Slovo verifikace je odvozeno z latinského výrazu *verum facere,* nebo-li činit pravdivým. Identita jedince je známá (lépe řečeno se předpokládá, že osoba udá svou identitu) a úkolem biometrického identifikačního zkoumání je tuto identitu potvrdit. Verifikovaná osoba sama, nebo za pomocí obsluhy biometrického snímacího zařízení, zadá identifikátor a poté se sejme vzorek biometrické charakteristiky požadované systémem. Ten následně vyhledá v archivu šablonu pro dotyčného jedince a porovná oba vzorky (aktuálně sejmutý vzorek osoby, která se pokouší verifikovat se vzorkem uloženým v archivu). Jakmile se dosáhne vzájemné shodnosti obou vzorků, je proces verifikace ukončen, v opačném případě systém ohlásí stav zamítnutí. Někdy se také používá označení one-to-one, tedy systém porovnává jeden neznámý vzorek s jednou šablonou v archivu.

1.1.2 Pojem identifikace

Identifikace se od verifikace odlišuje hlavně tím, že identita jedince není známa. To provedeme sejmutím vzorku požadované biometrické charakteristiky, ale protože není předem zadán identifikátor osoby pokoušející se o identifikaci, systém musí porovnávat tento sejmutý vzorek s každou šablonou uloženou v archivu systému. Tento proces porovnávání se děje tak dlouho, až systém dojde ke shodě údajů. Zde se občas uvádí označení one-to-many (tedy sejmutý vzorek se porovnává s více šablonami). Proces identifikace je tedy náročnější na výkon celého systému než u verifikace.

1.2 Uplatnění biometrických systémů

Biometrické rozpoznávání člověka lze uplatnit na mnoha místech, kde se požaduje moderní a efektní zajištění bezpečnosti a to například:

Přístupové systémy:

- budovy
- sklady
- elektrárny
- letiště
- výpočetní střediska

- trezory
- vydávání e-pasů

Identifikace osob:

- náhrada průkazů
- náhrada podpisů
- věrnostní systémy
- půjčovny
- turistické zóny a kasína
- stravovací systémy

Docházkové systémy:

- státní instituce
- komerční organizace

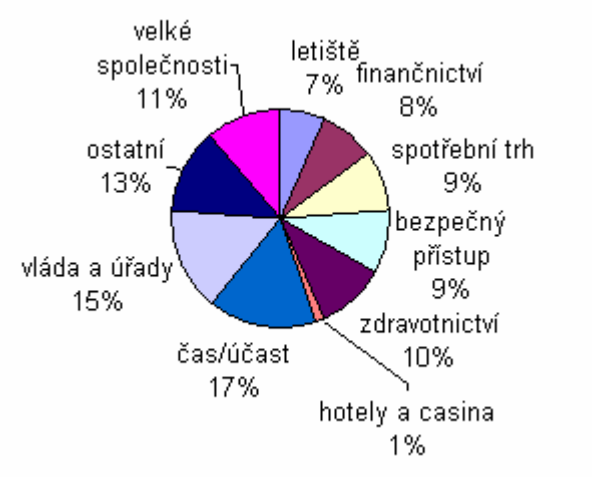
Ochrana počítačů:

- přístupy k souborům a adresářům
- přístupy do serverů
- přístupy do sítí
- aplikační software
- komerční využití internetu

1.2.1 Využívání biometriky pro přístupové systémy

Příznivější cena biometrických systémů je již nyní přijatelnější i pro komerční sféru, nikoli jen pro forenzní. Například firma s 50 zaměstnanci a dvěma vchody do budovy standardně zaplatí 5 až 10 tisíc dolarů za vstupní bezpečnostní systém na základě identifikace člověka pomocí PIN. Dnes je však za stejný finanční výměr možné pořídit bezpečnější biometrický systém, založený na rozpoznávání otisků prstů nebo oční duhovky. Biometrická data by mohla v podnicích nahradit hesla nebo PIN, která se obtížně pamatují. Ještě kvalitnějšího zabezpečení je možné docílit kombinací všech metod autentizace,

protože tak se využijí všechny tři pilíře bezpečnosti: co máme (kartu), co známe (PIN) a co jsme (např. otisk prstu). O tom, že biometrika se uplatňuje v nejrůznějších oblastech, vypovídá následující graf. Nejčastěji se biometrické systémy používají pro fyzický nebo logický přístup (do budovy, resp. do sítě, k informacím), pro kontrolu totožnosti osob či ochranu dat.



graf 1: Uplatnění biometriky v různých oblastech (zdroj: ABI)

1.3 Kriminalistická identifikace osob podle vnějších znaků

Antropologické metody jsou základem zkoumání a popisu lidského těla, významného především při pátrání po osobách, pro individuální identifikaci živých osob, ale částečně i pro identifikaci mrtvol neznámé totožnosti. Tyto antropologické metody jsou dělené na dvě části:

- antropometrické – které zjišťují kvantitativní charakteristiky antropometrických znaků (například oblouků v jistých partiích obličeje)
- somatoskopické – zjišťují kvalitativní charakteristiky lidského těla, jeho stavbu a to například chybějící část některé z končetin

Při popisu osob využíváme tyto vnější znaky a rozlišujeme je na:

- anatomické – (statické), což jsou znaky charakterizující například tvar hlavy nebo obličeje, výšku nebo hmotnost postavy a nebo vývin končetin

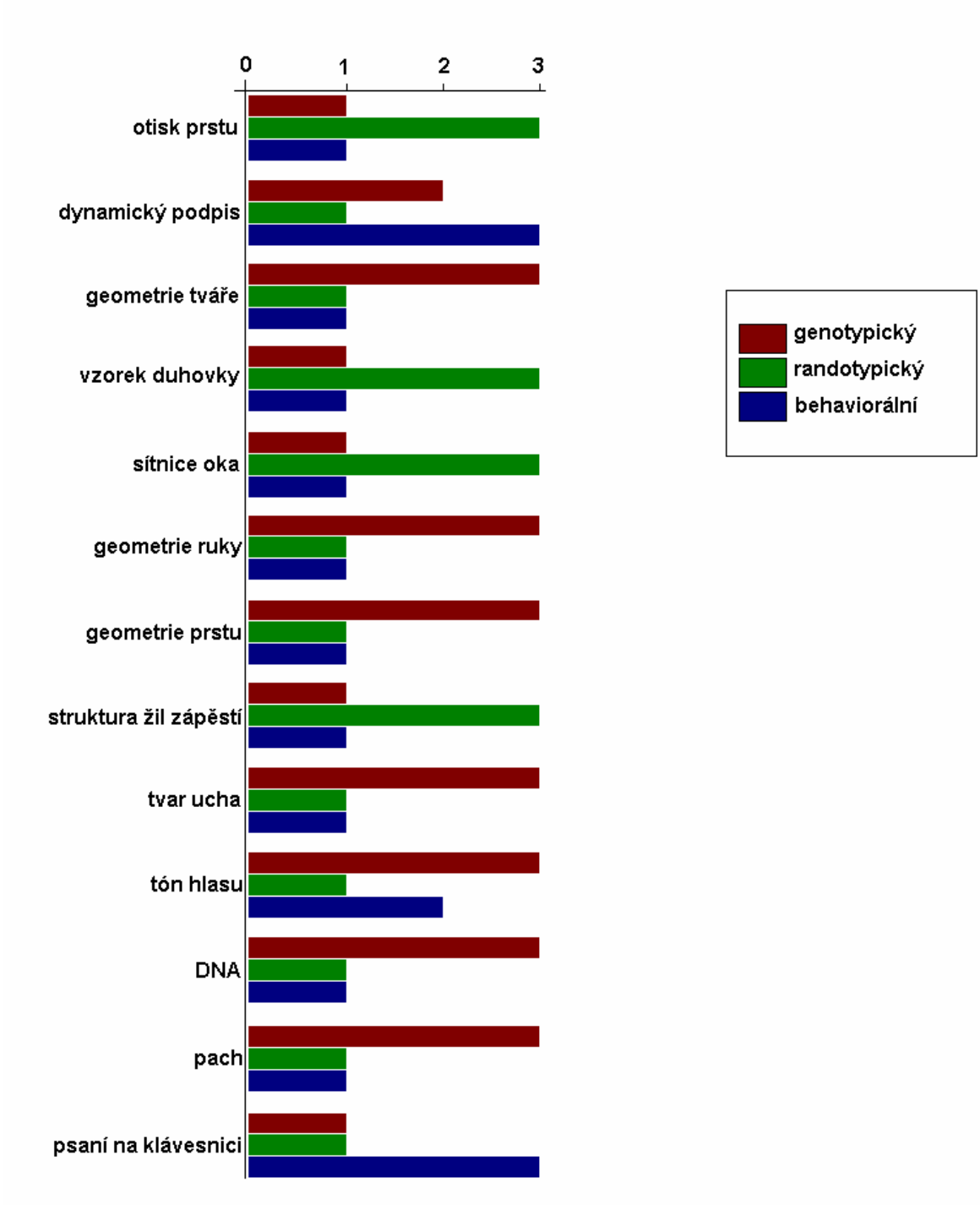
lidského těla. Jedná se tedy o znaky člověka, které lze hodnotit i na základě fotografie

- fyziologické – (dynamické) znaky, které charakterizují například držení těla, chůzi, slovní projev

Tyto anatomické a fyziologické znaky jsou základem pro biometrickou identifikaci osob, které jsou užívány v jednotlivých metodách jako svůj základ pro identifikaci člověka.

1.4 Vznik biometrických vlastností člověka

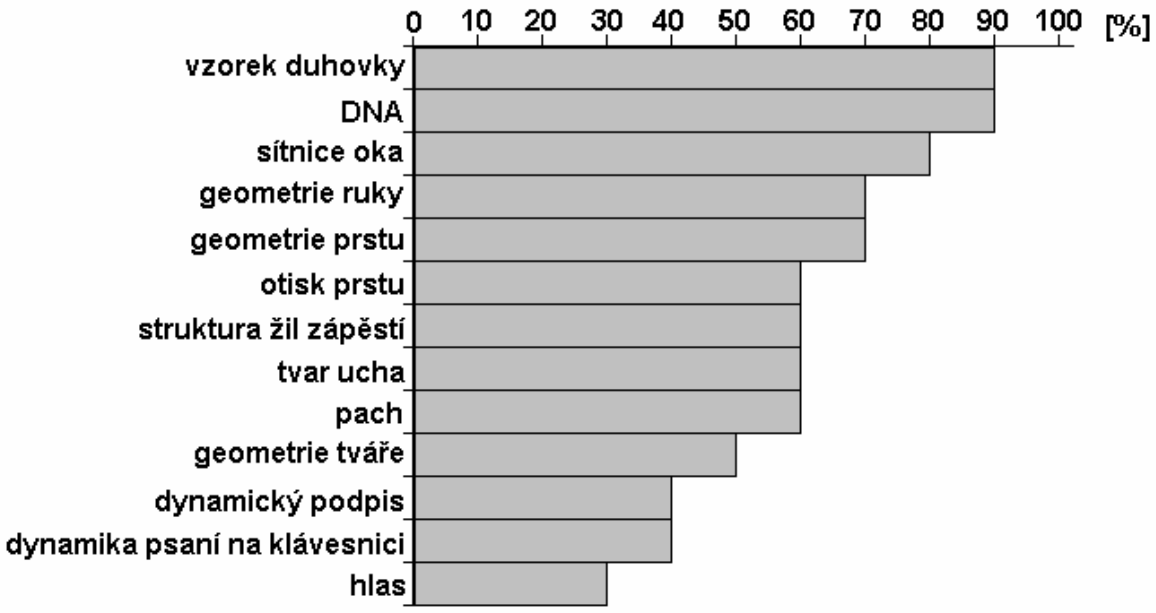
Biometrické vlastnosti člověka vznikají v základě třemi způsoby, jsou to genotypické (skrze genetický vývoj a uplatňuje se vliv dědičnosti DNA), randotypické (náhodné varianty vzniku při vývoji embrya) a behaviorální (získává jedinec skrze učení a výchovu). Všechny tři způsoby přispívají (každý v jiné míře) k biometrické vlastnosti člověka. Následující graf hodnotí relativní vliv vývojových vlastností na jednotlivé biometrické znaky a jejich důležitost jednotlivých faktorů. Stupeň 1 znamená zanedbatelný vliv, stupeň 3 významný vliv vývojových vlastností na biometrické znaky člověka.



graf 2: relativní vliv vývojových vlastností na jednotlivé biometrické znaky a jejich důležitost (zdroj: VŠB TU Ostrava)

1.5 Stálost biometrické vlastnosti v čase

V potřebách biometrických systémů potřebujeme také, aby sejmuté a uložené vzorky do databáze byly co nejdéle (nejlépe stále) co nejvíce aktuální. Mluvíme tedy o stálosti biometrických vlastností. Důvodů, proč se může tato vlastnost změnit je několik a to například opotřebení tkáně, vliv růstu živé tkáně, biologické stárnutí, popřípadě špína a nečistoty, zranění nebo následující hojící se rány. Nejméně ovlivnitelné biometrické vlastnosti jsou znázorněné v následujícím grafu, z kterého lze vyčíst, že největší stálost v čase mají bimetrické vlastnosti u člověka DNA a vzorek duhovky, dosahují 90% stálosti v čase.



graf 3: Stálost biometrické vlastnosti v čase (zdroj: VŠB TU Ostrava)

Optimální biometrická metoda se špatně definuje. Uživatel se musí rozhodnout, ke kterému řešení se přikloní a které mu bude nejvíce vyhovovat z hlediska uživatelského komfortu, ceny a také v přesnosti snímání. Snímání vzorku duhovky je ideální, pokud nezáleží na ceně. Při použití DNA si musíme uvědomit, že jednovaječná dvojčata mají shodné DNA. Jako nejvíce přijatelná možnost v poměru cena, komfort a přesnost nám vychází snímání otisku prstu.

1.6 Zabezpečení přístupu

U systémů s automatizovaným přístupem je nutné zajistit zabezpečení tohoto přístupu. U těchto systémů existují tři mechanismy, které se používají pro tyto účely. Jedná se o mechanismus, kdy využíváme heslo, předmět nebo biometrický prvek.

Rozdělení autentizačních přístupů je založeno na tom :

· co člověk zná (přístupové heslo)

· co člověk vlastní (identifikační karta)

· čím je člověk tvořen (obrazec papilárních linií)

1.6.1 Přístup heslem

Autentizace (neboli rozpoznání, jak jsme si vysvětlili dříve) heslem je založena na principu posloupnosti určitých znaků, které si uchovává v paměti nejlépe jen jeden uživatel a prostřednictvím tohoto hesla se dostane do chráněné oblasti. V praxi je nejpoužívanějším systémem, jelikož se jedná o jednoduchou a levnou záležitost. Setkáváme se s ním denně u zabezpečení počítačů, počítačových sítí, e-mailových účtech, bankovních účtech, mobilních telefonů atd. Přístup do chráněné oblasti za použití hesla se však využívá pouze pro systémy s nízkým stupněm zabezpečení, jelikož jej doprovází velká řada nevýhod jako jsou především vyzrazení hesla nebo dekódování hesla speciálními programy Heslo může být také vysledováno jinou osobou při zadávání znaků na vstupní klávesnici nebo v jiném případně může dojít k zapomenutí hesla uživatelem. Bezpečnost hesla se dá zvýšit, pokud budou jednotlivé znaky obsahovat velká a malá písmena, mezi jednotlivá písmena vložit i jiné znaky, například lomítko, číslice apod. Délka hesla je zpravidla minimálně 8 znaků. Význam těchto znaků by neměl mít přímou spojitost s uživatelem (například jméno, rodné číslo, číslo popisné), vhodné jsou slova či slovní spojení a znaky pro uživatele neobvyklá. Tyto hesla se nesmí nikde poznamenávat, musí se obměňovat v pravidelných časových intervalech a pokud jej musíme sdělit druhé osobě, tak jedině zabezpečeným způsobem.

1.6.2 Přístup za pomocí předmětu

Rozpoznávání člověka na základě specifického předmětu, který uživatel musí nosit u sebe má své výhody i nevýhody. Tento předmět, nazývaný TOKEN je přenositelný, to s sebou nese určitou již zmíněnou výhodu, ale také velkou nevýhodu (může dojít ke zcizení a zneužití). Dobře vyrobený token je co možná nejhůře kopírovatelný a je nositelem

informace pro autentizační protokol, tím dojde k rozpoznání uživatele (přístup do systému povolen/nepovolen). Tento způsob autentizace pro vyšší stupeň zabezpečení se využívá v kombinaci s biometrickým rozpoznáním člověka na základě sejmutého vzorku uživatele. Tokeny se využívají v mnoha systémech identifikace a to například stravovací systém nebo docházkový systém, v tomto případě není nutná kombinace s biometrickými systémy. V praxi se využívají tyto typy tokenů:

- tokeny s heslem – ty zároveň vyžadují zadání hesla (platební karty)
- logické tokeny – zpracovávají jednoduché podněty
- tokeny pouze s pamětí – magnetické, elektronické nebo optické karty
- inteligentní tokeny – mohou obsahovat vlastní vstupní zařízení a umět šifrovat a generovat náhodná čísla

1.6.3 Přístup pomocí biometrické charakteristiky

Výhodou těchto systémů je snadná identifikace uživatele a to bez použití přenositelných tokenů či hesel, které je nutné si pamatovat, což je pro člověka využívající biometrický systém velmi pohodlné, nedají se tedy vymazat z paměti (zapomnětlivost) nebo jej ponechat doma (jako klíče nebo token). Tyto systémy jsou navíc levnou záležitostí vzhledem ke svým neexistujícím budoucím nákladům. Biometrická informace je nezcizitelná, po celý život člověka neměnná a stálá. Vyznačují se vysokým stupněm zabezpečení a osvědčené systémy se dají jen těžko oklamat, jsou rychlé, praktické, výsledek je jednoznačný, jsou efektivní (dají se propojit přímo s databází počítače) a jsou cenově dostupné v poměru cena/výkon.

U biometrických systémů je hlavní podstatou snímání biometrické charakteristiky člověka a jeho následné porovnávání se vzorky uloženými v paměti systému. Při měření více biometrických charakteristik se mnohonásobně zvyšuje bezpečnost systému. Současné biometrické systémy využívají charakteristické znaky člověka, jako jsou otisk prstu, geometrie tváře, duhovka oka, sítnice oka, geometrie ruky nebo prstů, struktura žil na zápěstí, tvar ucha, lidský hlas, dynamika psaní na klávesnici, dynamika podpisu, DNA, lidský pach atd.

Při konstatování všech tří autentizačních metod lze říci, že při použití hesla je stupeň zabezpečení nízký, avšak v kombinaci s tokeny se stupeň zabezpečení mnohonásobně zvyšuje, je zde ale pravděpodobnost selhání lidského činitele (vyzrazení hesla a zapůjčení tokenu). Biometrické metody autentizace se jeví jako systémy pro vysoký stupeň zabezpečení (nelze je ztratit, ani předat). Každý z těchto typů zabezpečení je možno podrobit útokům. Tyto hrozby lze snížit použitím kombinace jednotlivých metod a dosáhnout tak vysokého stupně zabezpečení.

2 BIOMETRICKÉ SYSTÉMY

Elektronické biometrické identifikační systémy mají široké uplatnění v komerční i forenzní sféře. Pokud se jedná o forenzní sféru (soudní, kriminalistické a vyšetřovací) je nejznámější a nejvíce používaný systém AFIS (Automated Fingerprint Identification System – v překladu: Automatický systém pro identifikaci dle otisku prstu), byl vyvinutý vládou USA v úzké spolupráci s FBI (Federal Burelu Of Investigation – v překladu do češtiny: Národní úřad pro vyšetřování). Tento systém vlastní i Česká Republika, je instalován v Praze a byl pořízen za více jak 100mil Kč, nese název AFIS200. V mnoha státech světa se nevyužívá jen systémů na základě otisku prstu, ale velký rozmach nastává s automatickou identifikací, využívající charakteristik DNA systémů, které průběžně vyhodnocují geometrii tváře osob v davu například na letištích, nádražích v centru města a na všech místech s větší koncentrací osob. Stále více se rozvíjí biometrická identifikace i u cestovních pasů. Pro komerční sféru je podstatné, aby takový systém byl cenově přijatelný, není nutné například ukládat vzorky otisků všech deseti prstů (jako tomu je v kriminalistické sféře), ale stačí pouze otisk jednoho prstu, tím se sníží paměťová kapacita pro ukládání vzorků do systému.

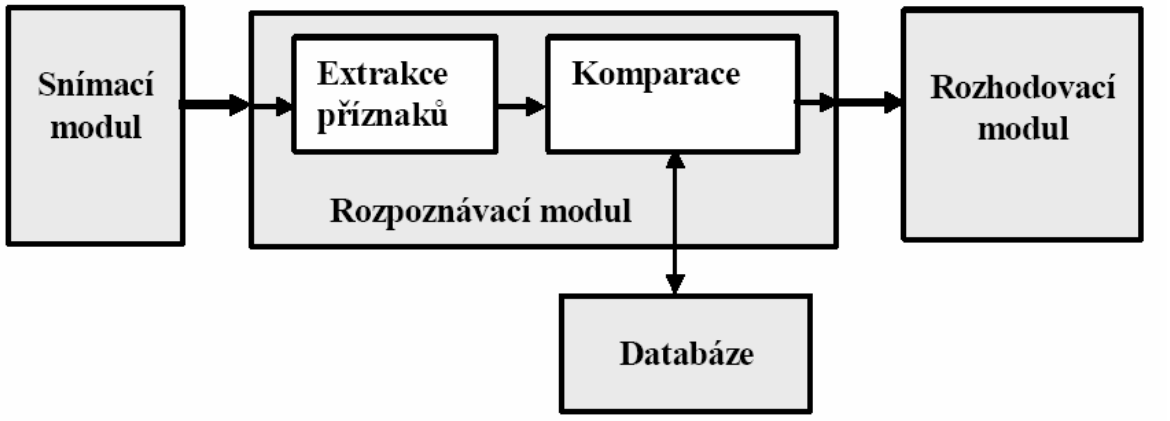
Ještě nedávno se biometrické identifikační zařízení využívaly jen z malé části pro bezpečnostní aplikace (jednalo se hlavně o bezpečnostní aplikace pro zvláštní účely), ale zhruba kolem roku 1999 se ceny těchto zařízení výrazně snížily a jejich použití se rozšířilo a stále více se rozšiřuje i do komerční sféry.

V průmyslu komerční bezpečnosti se využívá těchto systémů především v systémech kontroly vstupů ACS (Access Control Systems), které hlídají vstup do chráněných objektů a umožňuje průchod jenom osobám k tomu určeným. Počet povolených nepovedených pokusů je nutné omezit, abychom případnému narušiteli nedávali potřebný čas na prolomení systému a tím zvýšili úroveň zabezpečení systému. Na druhou stranu, když zvolíme malý počet povolených nepovedených přístupů, zvyšujeme tak pravděpodobnost výskytu falešných poplachů způsobené neoprávněnou identifikací oprávněného uživatele. ACS systémy spadají pod normu ČSN EN 50133 poplachové systémy – systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Výsledky všech přístupů by měly být pro vyšší stupně zabezpečení ukládány pro pozdější zpracování. Možnosti ukládání těchto informací jsou různé, buď přímo do hlavní jednotky snímače, což je ale nevýhodné z hlediska menší kapacity paměti a snadnějšího přístupu pro narušitele nebo ukládat

informace do vzdálenějšího počítače, tato možnost by nebyla omezena kapacitou paměti, ale je zde možnost narušení komunikační trasy. Pokud by pro identifikaci uživatele bylo použito tokenu, je zde možnost ukládat tyto informace přímo do tohoto zařízení, ale nevýhodou je nutnost složitější elektroniky při výrobě tokenu, což je samozřejmě dražší záležitost.

2.1 Funkční schéma biometrického systému

Biometrické identifikační systémy se skládají z několika logických modulů. Snímací modul zajišťuje snímání biometrických informací, další rozpoznávací logický modul se skládá z modulu pro extrakce příznaků a modulu komparačního (porovnávacího). Porovnávací modul porovnává získané biometrické informace (vzorky) s uloženými šablonami v databázi a rozhodovací modul zobrazí informaci o shodě (popřípadě neshodě) dvou vzorků. Následující blokové schéma znázorňuje základní princip elektronického biometrického identifikačního systému.



Obrázek 1: Funkční schéma biometrického systému (zdroj: Ščurek, R., Biometrické metody identifikace v bezpečnostní praxi)

2.2 Proces zápisu uživatele do databáze biometrického systému

Základem bezchybné autentizace osob je správně sejmutý biometrický vzorek uživatele, který je dále uložen centrálně do datové paměti systému nebo aplikace (nebo decentralizovaně na čip ID karty) jako osobní referenční šablona. Snímání a zápis vzorku musí být prováděn v důvěryhodném prostředí a hlavně opatrně s co nejvyšší možnou

kvalitou, jelikož kvalita má zásadní vliv na proces autentifikace. Při pořizování nového záznamu o uživateli se nejdříve pořídí vhodným snímačem datový soubor (obraz, zvuk, atd.), který obsahuje biometrickou vlastnost a následně se provede ověření kvality dat (pokud nevyhovuje kvalita, systém odmítne nebo uživateli poskytne radu jak zvýšit kvalitu sejmutí vzorku – například směr snímání). Dále dojde k vyextrahování požadované biometrické veličiny z datového souboru a vytvoří se šablona vzorku. Následuje zápis šablony jako referenční šablona do archivu a systém vyžaduje ověření (spočívá v porovnání aktuálního vzorku s referenční šablonou, provádí se algoritmem pro určení shody a dojde k vygenerování skóre, pokud skóre překročí předdefinovanou hodnotu, tak je přístup umožněn, jinak dojde k odmítnutí).

2.2.1 Zápis a možnosti ukládání etalonu

Dříve než lze pomocí biometriky ověřit identitu uživatele, je nutné získat referenční vzorek zvolené biometrické charakteristiky. Vzorek je označován jako biometrický etalon[1] (předloha) a představuje údaje, vůči nimž jsou následující vzorky porovnávány. Bývá sejmuto větší množství vzorků (obvykle tři), aby bylo možno vytvořit reprezentativní vzorek například jejich zprůměrováním. Následně je referenčnímu vzorku přiřazen identifikátor (obvykle PIN nebo číslo karty). Identifikátor slouží k vyvolání referenčního vzorku v etapě verifikace. Etapa zápisu a kvalita výsledného reprezentativního vzorku jsou kritické faktory ovlivňující úspěšnost biometrického systému.

Existují 4 možná řešení jak získaný vzorek uložit do systému:

1) V biometrickým čtecím zařízení – výhodou je nezávislost na externích procesech a rychlá reakce
2) Ve vzdálené centrální databázi - jakmile je síť mimo provoz, biometrický systém je vyřazen z činnosti a je třeba mít pro tento případ v záloze nějaké náhradní řešení.
3) V přenosných totenech - nevyžaduje žádné lokální nebo centrální ukládání etalonů, nevýhodou je vyšší cena a složitost biometrického systému

[1] Etalon – nebo-li předloha, je označení používané pro biometrické údaje vzorku. Tento vzorek je pak porovnáván s následujícími sejmutými vzorky

4) Kombinace předešlých způsobů

2.3 Kritéria pro výběr biometrické informace

Výběr biologické nebo behaviorální vlastnosti člověka pro následnou identifikaci je citlivý z hlediska následného způsobu užití. Musí být co nejefektivnější a musí splňovat řadu vlastností jako jsou: jedinečnost, univerzálnost, trvalost, měřitelnost a uživatelská přijatelnost. Z těchto požadavků vyplývá, že vlastnost se nesmí objevit u dvou lidí zároveň, musí být měřitelná shodnými technickými prostředky, neměnná v čase a přijatelná pro uživatele z hlediska snadné a pohodlné měřitelnosti.

Na celém světě jsou pro identifikační účely nejvíce prozkoumané a nejvíce užívané tyto biometrické vlastnosti:

- otisk prstu – měří se struktura papilárních linií včetně jejich detailů
- duhovka oka – obrazový vzorec duhovky
- geometrie tváře – vzdálenosti očí, nosu a úst
- sítnice oka – struktura žil
- dynamika podpisu – měří se rozdíly v tlaku a rychlost psaní
- geometrie ruky – rozměry dlaně a prstů
- tvar ucha – rozměry části ucha
- struktura žil na zápěstí
- hlas – především tón a zabarvení hlasu
- pach – jeho chemické složení
- DNA – řetězec deoxyribonukleové kyseliny
- psaní na klávesnici – měří se rytmus úderů na klávesy počítače

2.4 Výkonnost biometrických systémů

Výkonnost těchto systémů měříme z důvodu efektivního využívání v praxi, z hlediska bezpečnosti a uživatelského komfortu (pro uživatele je nepříjemné, pokud ho systém chybně odmítne). Měří se zpravidla koeficient nesprávného přijetí, koeficient nesprávného

odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu a doba ověření. Pro získání spolehlivých statických údajů je nutno provést velké množství pokusů. Čím více pokusů provedeme, tím přesnější hodnoty vycházejí.

2.4.1 Koeficient nesprávného přijetí

Koeficient FAR (FAR – False Acceptance Rate) se měří z hlediska bezpečnosti systému neboť koeficient udává pravděpodobnost, že nesprávná osoba je označena jako oprávněná. Takové nesprávné přijetí může vest ke vzniku škody, jedná se o chybu závažnou jak z hlediska bezpečnosti tak i z marketingového hlediska. Tento koeficient bývá označován jako chyba II. druhu.Vypočítá se následujícím vzorcem a udává se v procentech nebo se může vyjádřit poměrem například FAR = 0,001% což odpovídá poměru 1:100000 a znamená, že jeden ze 100 tisíc pokusů může být nesprávně přijatý.

$$FAR = (N_{FA} / N_{IIA}) \,.\, 100 \quad [\%]$$

N_{FA} - počet chybných přijetí

N_{IIA} – počet všech pokusů neoprávněných osob

2.4.2 Koeficient nesprávného odmítnutí

Koeficient FRR (False Rejection Rate) se především měří z hlediska komfortu uživatele, protože nesprávné odmítnutí je pro oprávněnou osobu nepříjemné. Udává pravděpodobnost toho, že oprávněný uživatel je systémem odmítnutý. Bývá označován jako chyba I. druhu. Z bezpečnostního hlediska se nejedná o závažnou chybu, ale z marketingového hlediska se jeví pro uživatele nevýhodně, protože jej nutí o opakování pokusu. Vypočítá se následujícím vzorcem a výsledek se udává v procentech nebo se může vyjádřit poměrem například FRR = 0,001% což odpovídá poměru 1:100000 a znamená, že jeden ze 100 tisíc pokusů může být nesprávně odmítnut.

$$FRR = (N_{FR} / N_{EIA}) \,.\, 100 \quad [\%]$$

N_{FR} - počet chybných odmítnutí

N_{EIA} – počet všech pokusů oprávněných osob

2.4.3 Koeficient FTE a FER

Failure To Enroll Rate. Vyjadřuje poměr osob, u kterých selhal proces sejmutí biometrické vlastnosti. Jedná se o poměr velmi pohyblivý, protože nemá vztah k samotnému systému, ale ke konkrétní osobě resp. ke konkrétní snímané biometrické vlastnosti člověka. FER je konkrétní koeficient k určité osobě udávající vztah biometrické vlastnosti k procesu snímání. V praxi to znamená, že uživateli byla správně sejmuta biometrická vlastnost, ale systém ho nesprávně odmítl i po mnoha pokusech verifikace, jedná se tedy o koeficient selhání přístupu FTA (Failure To Acquire).

Mezi další koeficienty řadíme koeficient FIR (False Identification Rate), který udává pravděpodobnost, že biometrická veličina je nesprávně přiřazena k některému referenčnímu vzorku. Dále koeficient FMR (False Match Rate), jedná se o podobný koeficient jako je FAR, liší se tím, že se do koeficientu FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu.

2.4.4 Přehled FFR, FAR a čas verifikace jednotlivých metod

V tabulce jsou znázorněny pravděpodobnosti chybného zamítnutí (FRR), pravděpodobnosti chybné akceptace (FAR) a čas verifikace ve srovnání s jednotlivými metodami identifikace.

	FRR [%]	FAR [%]	Čas verifikace [s]
Geometrie ruky	0,1	0,1	1-2
Otisk prstu	<1,0	0,0001-0,00001	0,2-1
Sítnice	0,4	0,001	1,5-4
Duhovka	0,0006	0,00078	2
Geometrie tváře	<1,0	0,1	3

Tabulka 1: Srovnání jednotlivých metod na základě pravděpodobnosti chyb FFR, FAR a v porovnání s časem verifikace

2.4.5 Nastavování citlivosti systému

Křížový koeficient EER nám udává pravděpodobnost při jakém nastavení hranice rozhodování nastane současně jev FAR a FFR. Udává ideální rozložení chyb FAR a FFR. Pokud jsou tyto dva koeficienty v rovnováze, znamaná to, že je v rovnováze celý systém ve smyslu bezpečnosti a komfortu. Následující graf nám znázorňuje tuto rovnováhu mezi oběma koeficienty a z grafu je také patrné, že pokud posouváme hranice jednoho z koeficientů jedním či druhým směrem, stává se systém buď bezpečnější nebo na druhou stranu více komfortnějším.

2.5 Bezpečnost biometrických systémů

Biometrické identifikační systémy se stávají častým terčem pokusů o prolomení systému, obelhání senzorů a mnoho dalších útoků protiprávního jednání (ať už za účelem se dostat do chráněného prostoru nebo do chráněných a cenných souborů v počítači). Spolehlivý systém si dnes už dokáže poradit s častými falešnými pokusy o identifikaci neoprávněné osoby, ale zkušený pachatel stále hledá nové a nové metody, jak prolomit a obelstít systém.

2.5.1 Ověřování živosti osoby

Důležitým faktorem pro bezpečný chod celého systému je ověřování živosti osoby, která se pokouší o identifikaci. Musíme počítat i s možností, že nepovolaná osoba se bude pokoušet obelstít proces identifikace. Objevují se pokusy o odlívání otisků prstů za pomocí

silikonu nebo i pokusy plastických operací za účelem změny charakteristických znaků pro identifikaci člověka podle tváře. Z hlediska bezpečnosti musí identifikovaná osoba prokázat, že v době pokusu o identifikaci je živá. Zkoumá se tedy živost osoby, jeho části nebo určité biometrické charakteristiky, na které je zařízení založeno. Pro systémy založené na identifikaci osob z hlediska otisků prstů se navíc může zkoumat pohyb krve v kapilárách pokožky prstu. Zařízení identifikující uživatele na základě podoby tváře vyžaduje navíc, aby osoba například mrkla, jelikož tyto systémy lze v opačném případě velice snadno oklamat fotografií. Aby nebylo možné identifikovat osobu prostřednictvím nahrávky (systémy pro rozpoznání uživatele podle hlasu), požaduje se při pokusu o identifikaci i odpověď na jednoduchou otázku. Tento systém pak identifikuje osobu na základě analýzy hlasu, ale i podle logiky odpovědi na danou otázku. Je tedy zřejmé, že doplňková ověřování jsou nutná pro zvýšení bezpečnosti celého systému a je zde jisté, že se o identifikaci pokouší živá osoba a ne třeba jen uříznuté části těla (například prstu).

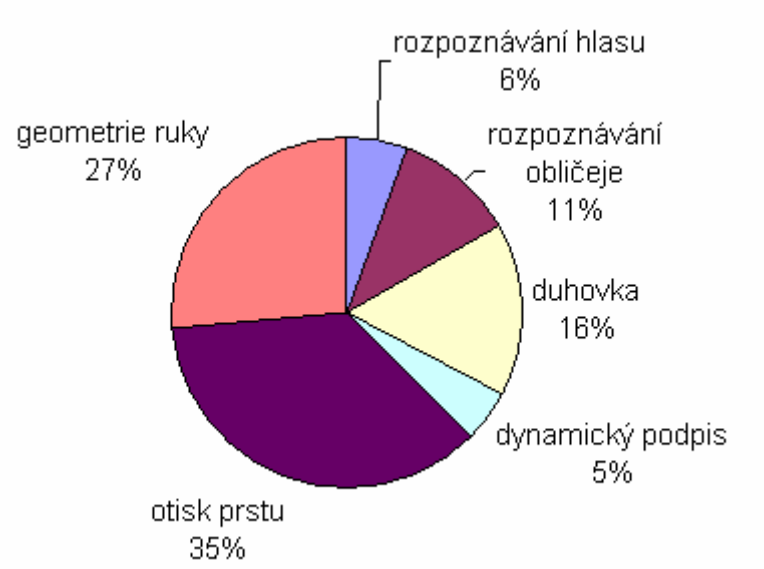
2.5.2 Způsoby zabezpečení

Další způsoby jak zvýšit bezpečnost je využití aplikace ezoterické identifikace, která pracuje na základě skrytých znaků a tím pádem je o mnoho obtížnější změnit tyto charakteristiky (například topografie žilního řečiště ruky, termovizní obraz tváře, otisk ušního boltce, otisky rtů a pórů, pach lidského těla, pleťová spektroskopie, obsah solí v lidském těle, rýhování nehtů na ruce atd.). Ke zvýšení bezpečnosti nám dopomůže i tzv. Multiple Biometric, jedná se o vícenásobnou identifikaci charakteristických znaků (obvykle dvou) použité pro jeden systém. Nejčastěji se využívá kombinace otisku prstu s geometrií tváře a kombinace geometrie oční sítnice či duhovky s analýzou hlasu. Mezi další způsob zabezpečení řadíme i tzv. behaviometriku, ta se zabývá sledováním vlastností člověka jako je například styl psaní na klávesnici počítače nebo monitorování pohybu počítačové myši (tyto pohyby je nemožné se naučit nebo odkoukat od uživatele). V tomto případě nestačí jen se správně přihlásit za pomocí hesla, ale jsou zde vyhodnocovány i tyto skryté vlastnosti a počítač pozná, kdy pracuje se systémem jiná osoba.

II. PRAKTICKÁ ČÁST

3 METODY K INDIVIDUÁLNÍ IDENTIFIKACI

V praxi se využívá mnoho metod pro individuální identifikaci osob. Každá z nich má své určité výhody, pro které se využívají, ale bohužel se objevují i nevýhody. Proto je nutné zvážit, jakou metodu je vhodné použít pro konkrétní praktické využití ať už z hlediska komfortu pro uživatele, ale hlavně i bezpečnosti a efektivnosti systému. Podíl jednotlivých technologií biometrických systémů na trhu naznačuje následující graf.



graf 4: Podíl jednotlivých technologií biometrických systémů na trhu (Zdroj: ABI)

3.1 Otisk prstu

Už na konci 19. století Sir Francis Galon objevil skutečnost, že obrazce papilárních linií na vnější straně prstů rukou, nohou a dlaní lze použít pro identifikaci člověka, charakterizoval taky některé charakteristické body, použitelné pro identifikaci. Tyto body (tzv. Galtonovi body) se staly základem pro další rozvíjení celého vědního oboru zabývající se otisky prstů. Jedná se o metodu, která se stala jednou z nejznámější a nejpoužívanější pro svou stálost v čase, jedinečnost a jednoduchost.

3.1.1 Základní zákonitosti

„Daktyloskopie umožňuje jednoznačně individuální identifikaci osob, řídí se vědecky odůvodněnými zákonitostmi a vychází z těchto poznatků:

- na světě neexistují dva lidé s naprosto shodnými obrazci papilárních linií. Kromě faktu, že toto tvrzení dosavadní kriminalistické praxe potvrdila, i výsledky matematických poznání vyvracejí pouhou pravděpodobnost existence dvou jedinců se shodnými obrazci papilárních linií, kteří na zemi v minulosti žili či v současné době žijí
- obrazce papilárních linií zůstávají po celý život člověka relativně neměnné. Od počátku jejich tvorby, tj. od 4. měsíce vývoje lidského plodu, je dán základ kresby papilárních linií, jenž zůstává nezměněn po celý život člověka. Z pohledu potřeb individuální identifikace osob lze zaznamenat pouze nevýznamné změny v obrazcích papilárních linií během života jedince, kdy poranění (jizvy), zhrubnutí či jiné zvýraznění obrazců papilárních linií jsou sice změněny, ale bez vlivu na jejich celkovou kresbu, která zůstává stálá.
- papilární linie jsou neodstranitelné, pokud není odstraněna i zárodečná vrstva kůže. Mechanické působení (odříznutí či obroušení), vliv chemikálií (poleptání) změní obrazec papilárních linií v místě kontaktu s nástrojem či chemickou látkou v rozsahu intenzity kontaktu, ale výsledná změna je dočasná pouze do zhojení vzniklého poranění papilárních linií. Trvalá změna může nastat, když je přímý kontakt na papilární linie veden způsobem, že dojde ke zničení zárodečné vrstvy kůže. Výsledkem bude deformace v obrazci papilárních linií, např. jizva, která v podobě stálé změny vytvoří nový individuální znak, využitelný pro dané individuální identifikační zkoumání.“[2]

3.1.2 Stavba kůže a základní dělení vzorů papilárních linií

Na obrázku vidíme průřez kůže prstu.

1 – pokožka (epidermis)

2 – škára (cutis)

a – vrstva rohová (stratum corneum)

---

[2] RYBÁŘ, M – Základy kriminalistiky, 1. vydání, vydavatelství a nakladatelství Aleš Čeněk, 2001

b – vrstva zárodečná (stratum geminatium)

c – póry

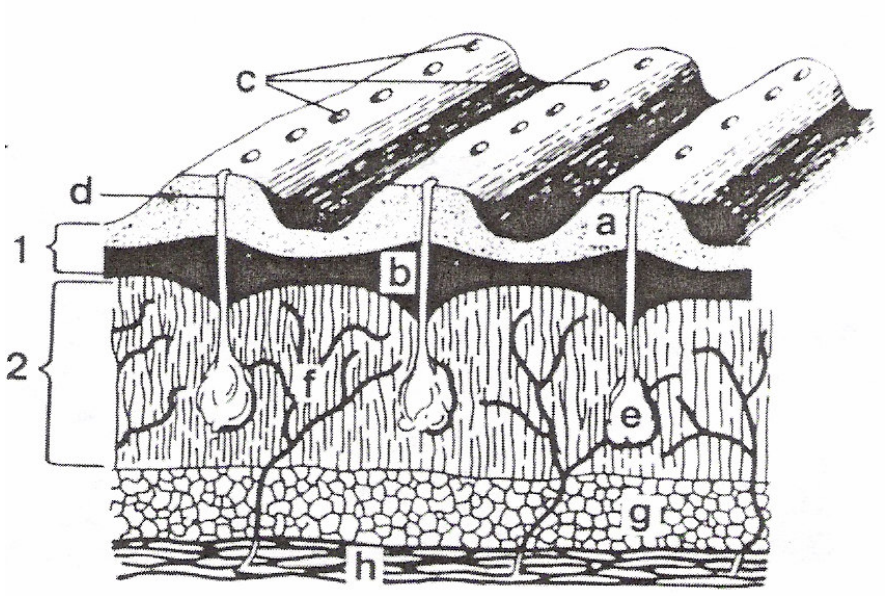
d – vývody potních žláz

e – potní žlázy

f – cévy

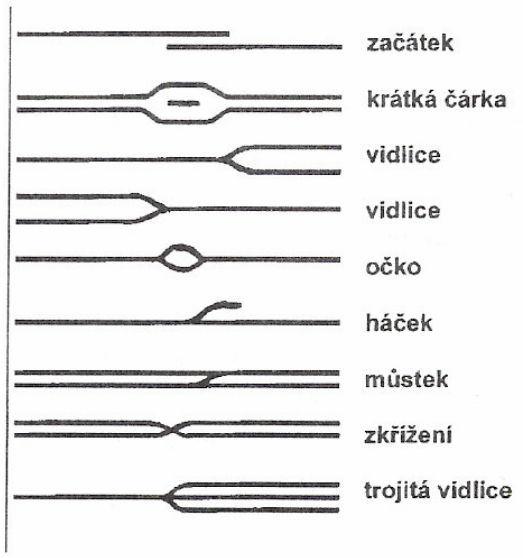
g – podkožní tuk

h – svalstvo



Obrázek 2: Schéma stavby kůže s papilárními liniemi (zdroj: Porada, V., Kriminalistika)

Vlastní identifikace se provádí na základě daktyloskopických markantů. Jednoznačně vyjádřená individualita papilárních linií se projevuje v tom, že obsahují velký počet těchto markantů umožňujících poměrně snadno jednotlivé obrazce navzájem odlišit. Tyto markanty se liší nejenom geometrickým tvarem, ale i četností výskytu, rozmístění markantů je v jednotlivých obrazcích papilárních linií nepravidelné a i konkrétní tvary markantů mohou vykazovat rozdíly. Na obrázku znázorňuji základní tvary identifikačních znaků:



Obrázek 3: Daktyloskopické markanty (Zdroj: Porada, V., Kriminalistika)

Na dalším obrázku jsou vidět detaily třech hlavních vzorů seskupení papilárních linií. Jedná se o smyčky(loop), víry (whorl) a oblouky (arch).

Obrázek 4: Hlavní vzory seskupení papilárních linií

3.1.3 Výpočetní technika využívaná pro daktyloskopii

Rozvoj počítačové techniky dopomohl k její plné automatizaci a tato metoda získala díky tomu i své uplatnění v dnešní době. Pro vysoké procento populace je velmi jednoduchá z hlediska sejmutí vzorku papilárních linií, problém nastává jen u osob, kteří přišli o končetiny a nemají ani jednu ruku a zároveň ani jednu nohu (tato situace je ale málo pravděpodobná). Biometrická identifikace se stala zavedenou a osvědčenou metodou v právní sféře a u policie, která obsahuje velkou databázi. Již v šedesátých letech se objevily

první návrhy na počítačovou podporu a v 80. a 90. letech se za rozvoje informatiky podstatně zvětšila oblast využití daktyloskopie za pomocí počítačových programů.

Využití výpočetní techniky má zásadní význam pro podstatné zvětšení produktivity a kvality práce v tomto oboru, jelikož manuální vyhodnocování obrazců otisků prstů je velice náročné jak časově tak i odborně a fyziologicky. Dalším faktorem je i doba vyhodnocení, která je mnohem kratší za využití počítačové techniky. Sejmuté otisky prstů na místě činu se musejí co nejdříve laboratorně prozkoumat, aby pachatel byl co nejdříve usvědčen a nemohl páchat další trestné činy. To by byl dnes bez plné automatizace velký problém.

3.1.3.1 Vyhodnocování otisků prstů za pomocí počítačové technologie

Je opravdu mnoho firem, které nabízejí programy pro zpracování otisků prstů, mezi nejznámější patří Printrak, Morpho, Cogent System International. Mnoho dalších firem nabízí programy a systémy i pro komerční využití a to hlavně ve spojení s různými přístupovými systémy do chráněných objektů nebo systémů. Objektem daktyloskopie je tedy stopa (sejmutá například na místě činu nebo kdekoliv jinde za účelem následného použití pro identifikaci) a srovnávací materiály, které jsou uloženy ve sbírkách a nebo v archivu počítače. Pro identifikaci jsou vzájemně srovnávány a cílem celého procesu je zjistit zda se shoduje nebo neshoduje tento sejmutý vzorek s některým s uloženým v archivu a dojít tak k závěru shoda / neshoda (a nejlépe i určit přímou identitu osoby). Problémem je, že oba porovnávané objekty jsou snímány za různých podmínek a poloh, tedy ne vždy může dojít k absolutní shodě. Tyto programy vyhledávají v archivu šablonu nejvíce vyhovující sejmutému vzorku a pověřená osoba pak nadále přezkoumá tyto dva vzorky. Tedy zkoumá už jen jeden sejmutý vzorek s jednou šablonou v archivu a to po náročném a složitém srovnávacím procesu počítače. Porovnávání za pomocí programu počítače není zrcadlové (překrývání dvou folií). Otisky nikdy nejsou sejmuty ve stejné poloze, mohou mít různá zakřivení. Počítač považuje jednotlivé papilární linie a identifikační znaky za samostatné objekty a určuje mezi nimi charakteristické, markantní body, definuje geometrické závislosti, vzdálenosti a vektory. Vytváří vlastně unikátní vzorec, matice číselných hodnot. Porovnávání otisků pak probíhá na základě podobnosti nebo shody takto uměle vytvořených šablon.

3.1.3.2 Průběh zpracování sejmutého vzorku

Sejmutý otisk se nejprve musí digitalizovat a předzpracuje se, to představuje filtraci, segmentaci, vyhlazení a vytvoření kostry otisku, tomuto postupu se říká skeletizace, která je znázorněna na obrázku. Takový materiál je pak vhodný pro následné zpracování počítačem, neboť jsou omezeny chyby vzniklé špatnou kvalitou obrázku. Charakteristickými body, které jsou významné pro proces identifikace se nazývají markanty. Na obrazu a vzorku se vyskytují body, které si vzájemně odpovídají a těmto bodům pak říkáme identické body. Vyhledáváním dvojic identických bodů realitujeme ztotožňování vzoru a obrazu, zpravidla se jedná o vrchol otisku a delta bod, okolo těchto dvou bodů je otisk plošně orientován. Transformace se realizují pomocí násobení a sčítání transformačních matic.

3.1.3.3 Počet identifikačních znaků v otisku pro počítačové zpracování

Počet identifikačních znaků je velmi důležitý pro vyhodnocování otisků prstů z hlediska počítačového zpracování. Udávají nám míru pravděpodobnosti, že sejmutý vzorek a uložený otisk v archivu jsou od stejné osoby. Taková míra pravděpodobnosti se musí blížit jistotě a ta roste s rostoucím počtem identifikačních znaků v otisku prstu. Počet těchto identifikačních znaků je stanoven pro českou republiku na deset znaků. Policejní služby různých zemí však pracují s odlišným počtem těchto identifikačních znaků (zpravidla 8 – 12). Používaný počet identifikačních znaků je taky omezen podle toho, zda se daktyloskopická technika využívá pro komerční účely nebo pro soudní. Při využívání biometrického identifikačního systému pro komerční účely, se může počet identifikačních znaků snížit a zpravidla nemusí být uváděn výrobcem, musí však splňovat technické charakteristiky, uváděné zákazníkovi. Systémy pro policejní aplikace pracují s daktyloskopické údaje milionů lidí, kdežto technické biometrické vybavení pro identifikaci člověka v soukromé sféře (firma, která využívá biometrický identifikační systém pro přístup do objektu) má ve své databázi podstatně nižší počet těchto údajů ke zpracování. Systémy s menším počtem identifikačních znaků jsou i levnější, menší cena se ale odráží i na menším počtu funkcí systému.

3.1.4 Metody používané pro zachycení otisku prstu

Metod pro zachycení otisků prstu existuje celá řada, v průběhu rozvoje daktyloskopie se vynalézaly různé metody. Cílem je získat přesný, nerozmazaný, co možná nejvěrohodnější obrazec, bez posunutí a zakřivení.

3.1.4.1 Inkoust a papír

V angličtině Rolled Finger. Tento druh metody se využívá jen policií při vyšetřování. Základem je získat otisk prstu v co největším rozsahu, aby se na papír přeneslo co nejvíce informací a identifikačních znaků. Na prst je nanesen inkoust a ten se otiskne rolováním (od nehtu po nehet) na papír. Snažíme se otisknou co největší plochu prstu, abychom získaly větší počet markat, tím se zvýší rychlost rozpoznání otisku.

3.1.4.2 Statické snímání

Tato metoda s sebou nese spoustu výhod a nevýhod. Jedná se v podstatě o pouhé přiložení prstu na plochu snímače (pracujících na různých fyzikálních principech), což je pro uživatele velice jednoduchá a pohodlná metoda. Plocha snímače je ale zatěžována a při větším tlaku může dojít k prolomení čočky, navíc je plocha snímače vystavena prachu a po přiložení prstu se můžou objevit nečistoty nebo latentní otisky, které pak zkreslují následné otisky. Prst se na plochu musí jen přiložit, nesmí dojít k žádnému pootočení (to vede k deformaci pokožky).

3.1.4.3 Šablonování

„Uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů, které jsou znázorněny na obrázku. Používá se křemíkový snímač, pohybuje se i cena v oblasti křemíkových součástek. Redukovat cenu lze právě využitím šablonového snímání, tím že snímač bude mít tvar úzkého pruhu. Celková cena pro pořízení otisku prstu je poté výrazně nižší. Výhody šablonového snímání jsou: snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor, na snímači nezůstávají skryté (latentní) staré otisky, uživatel

nemá pocit zanechaného otisku prstu a snímání je rychlé. Nevýhodou je, že obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup.“[3]

3.1.5 Snímače používané pro otisk prstu

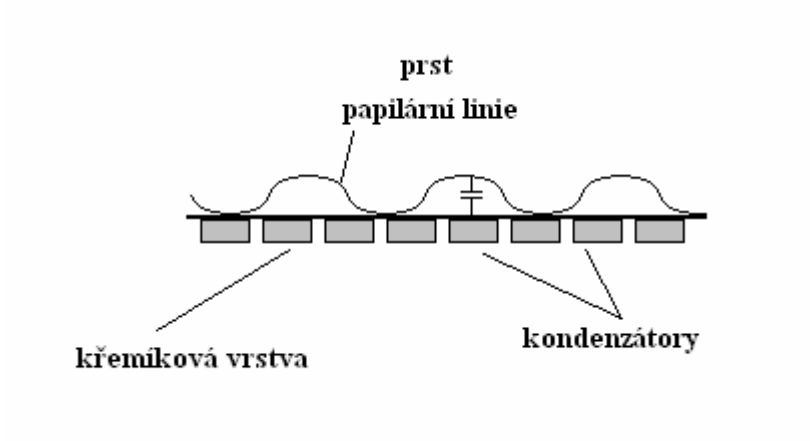
Sejmutí obrazu otisku prstů se může provést mnoha způsoby a existuje pro tyto účely hodně technologií, které se v praxi používají. Stále se rozvíjejí a vylepšují principy a metody snímání otisků prstů a cílem je zajistit pro identifikační systém snímače, které podají nejlepší výsledky, jsou efektivní, pohodlné a za rozumnou cenu.

U senzorů pro otisk prstu jsou vyhodnocovány kritéria jako jsou celkové rozměry s dostatečnou snímací plochou, dostatečné rozlišení a ochrana vůči napodobeninám. Dále se hodnotí uživatelská přívětivost, odolnost proti mechanickému poškození, jejich životnost a spolehlivost

3.1.5.1 Kapacitní snímače

Tato metoda snímání otisků prstů je založena na principu, že prst tvoří jednu desku kondenzátoru a aktivní pixely druhou desku. Velikost elektrického pole se mění na závislosti dielektrika, tedy pokud se jedná o vzduch (rýha mezi liniemi) nebo o kůži. Tato metoda je jednou z nejrozšířenější. Senzor je zpravidla malý a rozměry se pohybují kolem 4 cm^2. Plocha senzoru je tvořena velkým počtem kondenzátorů strukturovaných do sítě (řádu 10 tisíc). Snímací zařízení je CMOS kamera, TFT displej nebo progresivní metoda silikonových čipů.

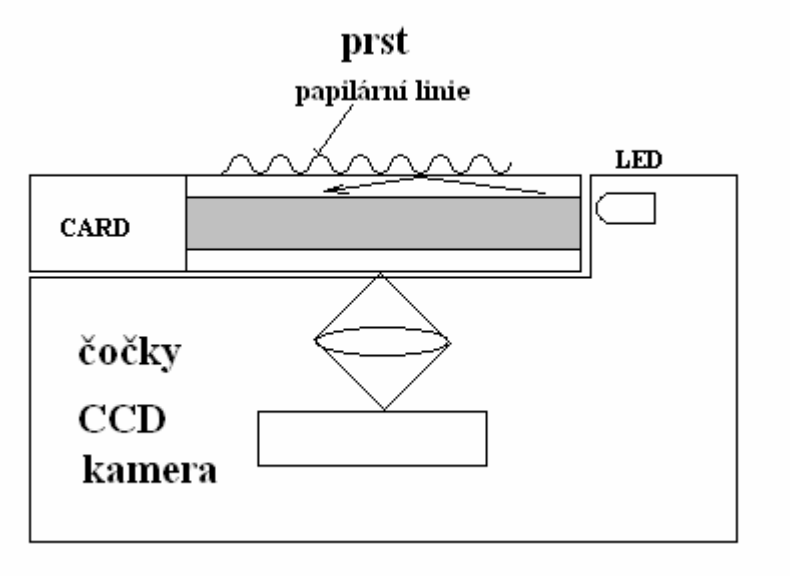
[3] Ščurek, R. – Biometrické metody identifikace v bezpečnostní praxi, červen 2008



Obrázek 5 Kapacitní princip snímání otisku prstu

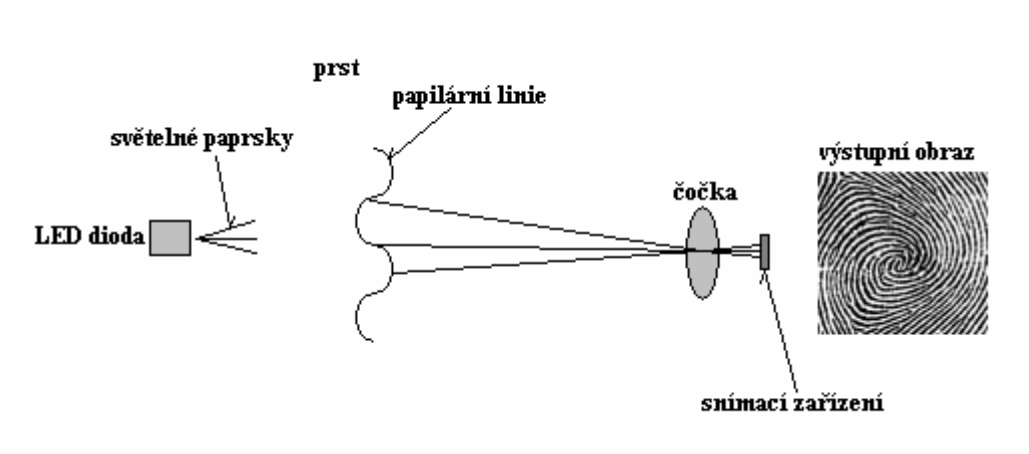
3.1.5.2 Optické senzory

- Reflexní – prst se přidrží nad skleněnou ploškou, která je podsvětlena , světlo se odráží od prstu a prochází do CCD snímače a ten zachycuje obraz otisku. Nevýhodou této metody je, že skleněná plocha je náchylná na znečištění, která vede ke zhoršení obrazu. Obraz otisku prstu se získává staticky. Používají se i reflexní rolovací senzory, po které prst klouže a výsledný obraz se skládá z jednotlivých pásů, jedná se o tzv. šablonování.



Obrázek 6 Princip snímání reflexními optickými senzory

- Transmisní – prst ruky je z vrchní části prosvětlen všesměrovým zdrojem světla (LED dioda). Obraz otisku prstu je zachycen systémem čoček a snímacím zařízením, jako je CCD, CMOS kamery nebo polymerický organický fotodetektor.



Obrázek 7 Princip transmisních snímačů otisku prstu

- Bezkontaktní – Touchless Technology – Základem principu jsou LED diody pod různým úhlem, které vysílají proti prstu světelné paprsky, ty se odrážejí od papilárních linií zpět do čočky a signál zpracovává CMOS čip.
- Elektro-optické – u těchto snímačů je použitý polymerní materiál, který je schopný emitovat světelné záření a to v případě, že je nabuzen vhodným napětím. Otisk prstu získáme tak, že tento polymerní materiál propojíme se snímacím zařízením (CMOS kamerou) a materiál emituje světlo jen v místech dotyku s papilárními liniemi
- TFT optické snímače – běžné snímací zařízení, jako je CMOS nebo CCD, je nahrazeno TFT displejem

3.1.5.3 Teplotní snímače otisku prstu

Jedná se o čip vyrobený z křemíku, pokrytý pyroelektrickým materiálem v podobě přiléhajících pixelů, citlivý na změny teploty. Vyhodnocují se nepatrné rozdíly teplot mezi pokožkou prstu a vzduchu (papilární linie – vzduch mezi papilárními liniemi), neměří se tedy absolutní hodnota teploty, ale tepelný rozdíl pokožky v místě dotyku snímače. Teplotní

diference se převede na elektrický náboj, který je zesílen a předán na spodní křemíkový čip. Výsledný obraz se zobrazuje ve formě několika stupních šedi.

3.1.5.4 Tlakové snímače

Využívají piezoelektrických materiálů, které využívají změnu tlaku. Aby mohly tyto materiály být použity i pro snímače otisků prstů, kdy se snažíme zachytit i nepatrné tlakové rozdíly (papilární linie), musí se použít v kombinaci s vodivostní membránou (tvořenou maticí piezoelektrických tlakových senzorů) na CMOS kameru se silikonovým čipem nebo je zde taky možnost umístit membránu na TFT podložku. Další z metod využívá maticového systému mikro mechanických spínačů, které reagují na tlak v místě dotyku s papilárními liniemi.

3.1.5.5 Ultrazvukové senzory

Jejich výhodou je, že ultrazvuk pronikne i nečistotami a tím se redukují chyby vzniklé na otisku prstu. Jedná se o podobný princip jako u optických snímačů, s tím rozdílem, že místo světelných paprsků je zde použitý ultrazvuk, který se odráží od prstu. Odražená zvuková vlna (od papilárních linií a prohlubní prstu) se pak vrací zpět na senzor a tento signál je pak dále zpracován a vyhodnocen ve formě obrazu otisku prstu.

3.1.5.6 Aktivní kapacitní snímače

Styčnou plochu s prstem u těchto senzorů tvoří síť miniaturních antén, které vyhodnocují nízký RF signál vyslaný a následně odražený zpět na snímač. Měří se síla radiového signálu a ta se mění v závislosti na odporu či vodivosti spojení (vzdálenost mezi kůží a anténní soustavou). Odlišnost těchto signálů bude v místech dotyku papilárních linií a v místě prohlubní mezi papilárními liniemi.

3.1.6 Praktické využití metody otisků prstů

V praxi se například tato metoda využívá pro hlavní a přídavné zámky určené pro dveře do prostor, do kterých je nutné zajistit jedinečnou a nepřenositelnou identifikaci osob oprávněných ke vstupu, jsou vhodné na dveře do kanceláří a skladů, odemykání otiskem prstu nebo PIN kódem, paměť zámku až na 130 uživatelů, automatické zamykání,

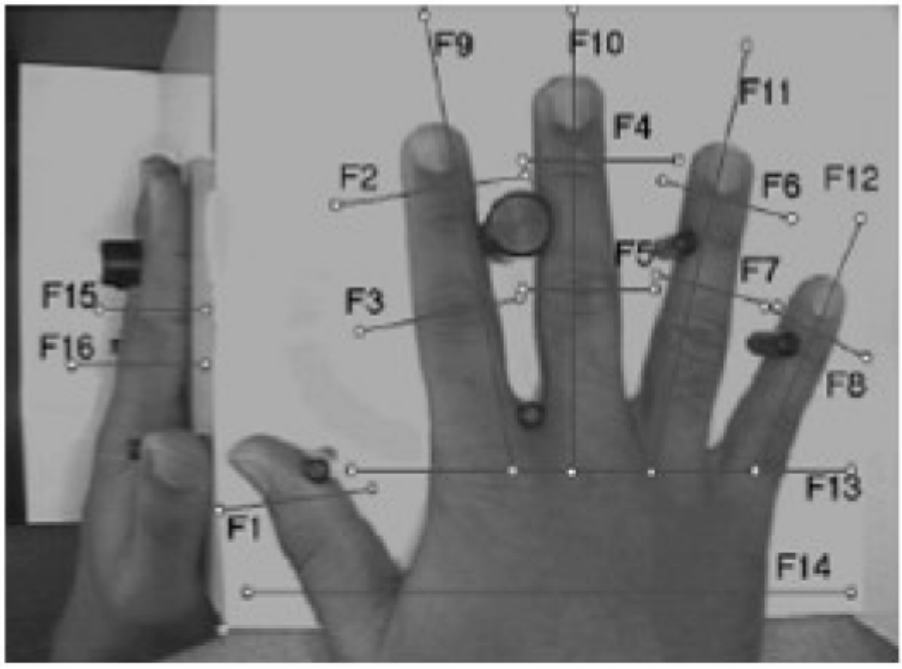
jednoduché ovládání, žádné klíče, karty, hesla, rychlý přístup do místnosti (do 1 sekundy), rychlé přidávání či odebírání oprávnění ke vstupu.

Obrázek 8: Čtečka otisku prstu jako přídavný zámek (zdroj: Ekey)

3.2 Geometrie ruky

Tento systém vyvinul David Sidlauskas v roce 1985 a v brzké době se začal využívat i komerčně. Je jedním z nejstarších implementovaných biometrických principů. Její aplikace v bezpečnostní sféře je však omezena stupněm bezpečnosti, protože geometrie ruky není příliš unikátní. Obvykle se využívají v docházkových a přístupových systémech Systém pracuje na principu podložky, na které jsou umístěny polohové kolíky a CCD kamera. Snímá se 3 dimensionální délka, šířka ruky, která se umisťuje na podložku s pěti kolíky. Sytém není náročný na paměť, vybrané měřené informace se ukládají jako 9 bitový soubor. Na obrázku je znázorněna čtečka pro geometrii ruky od firmy Granus.

Obrázek 9 Čtečka pro geometrii ruky (Zdroj: Granus)



Obrázek 10: Rozpoznávání geometrie ruky – hodnoty rysů (zdroj: , J., Význam a charakteristika identifikačních biometrických systémů v průmyslu komerční bezpečnosti)

F1 – šířka palce ve druhém článku

F2 – šířka ukazováčku ve třetím článku

F3 - šířka ukazováčku ve druhém článku

F4 – šířka prostředníčku ve třetím článku

F5 - šířka prostředníčku ve druhém článku

F6 – šířka prsteníčku ve třetím článku

F7 - šířka prsteníčku ve druhém článku

F8 – šířka malíčku ve třetím článku

F9 – délka ukazováčku

F10 – délka prostředníčku

F11 – délka prsteníčku

F12 – délka malíčku

F13 – šířka dlaně u prstů

F14 – šířka dlaně u palce

F15 – tloušťka ruky u druhého článku

F16 - tloušťka ruky u třetího článku

3.3 Geometrie tváře

Rozpoznávání je založeno na obrazu sejmutého kamerou a obrazem, který je uložen v databázi. K identifikaci slouží tvar obličeje a poloha významných míst na obličeji jako je nos, oči, ústa, obočí. Uchovává se především vzdálenost očí, vzdálenost rtů a nosu a úhel mezi špičkou nosu a jedním okem. Identifikace osob podle geometri tváře se rozvíjí velice rychle a dochází k jejímu nasazování do prostor s velkým pohybem lidí (s předpokladem, kde by se mohly vyskytovat hledané nebo pohřešované osoby) místa jako jsou letiště, náměstí, rušné ulice, nádraží. Je známo několik technik rozpoznávání tváří a jedná se o obor, který je dnes nejvíce zkoumán a to z hlediska praktického využití. K těm nejznámějším patří metoda měření geometrických vlastností a metoda porovnávání šablon. Vznikají však i nepřesnosti identifikace, zvláště při různých sklonech vyfotografování, osvětlení, fotografie obličeje musí být celá, záběr snímku musí obsahovat celou tvář. Tři nejlépe prozkoumané algoritmy rozpoznání tváře jsou:

- analýza hlavních částí – PCA (Principal Components Analysis)
- lineární diskriminační analýza – LDA (Linear Discriminant Analysis)
- elastický srovnávací diagram – EBGM (Elastic Bunch Graph Matching)

3.3.1 Analýza hlavních částí

Metoda PCA využívá vektorů tváře odvozených s kovariační matice pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání. Jednotlivé tváře člověka lze rozdělit na tzv. vzory tváří – matice jasových úrovní, a poté je opět složit. Těmto vzorům tváří se také říká eigenfaces a přiřazují se k nim jen čísla, neukládá se tedy obrázek, ale číslo.

3.3.2 Lineární diskriminační analýza

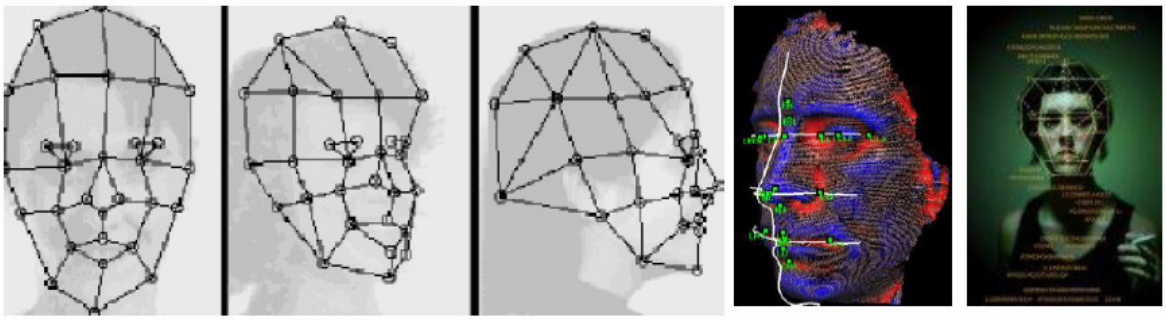
Pořízené obrazy tváří se v této metodě třídí do určitých skupin a to za účelem maximalizace rozdílů mezi jednotlivými skupinami a minimalizace rozdílů v každé skupině. Každý blok obrázků reprezentuje jednu třídu. Na obrázku vidíme seskupení podle specifických tříd, systém provedl seskupení například starších osob nebo osob určité národnosti s jinými rysy tváře.

Obrázek 11 Seskupení tváří podle specifických tříd (Zdroj: VŠB TU Ostrava)

3.3.3 Elastický srovnávací diagram

Tato metoda byla vyvinuta z důvodů, že metody PCA a LDA nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, výraz ve tváři nebo poloha hlavy. „Na obličeji se definují uzlové body, které se propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje viz. následující obrázek. Samotné rozpoznání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou. FRR <1%; FAR 0,1%; čas verifikace 3 sekundy; míra spolehlivosti střední.“[4]

[4] Ščurek, R. – Biometrické metody identifikace v bezpečnostní praxi, červen 2008



Obrázek 12: Síť vytvořená elastickým mapováním a obraz zpracovaný počítačem

3.3.4 Příklad využití

Nizozemský fotbalový klub PSV, který sídlí v Eindhovenu si objednal bezpečnostní systém, kterým chce předcházet výtržnostem na stadionu, jinými slovy zabránit výtržníkům ve vstupu na stadion.

Cituji z tiskové zprávy dodavatele: "Řešení funguje tak, že obraz z bezpečnostních kamer je předáván do počítačové aplikace, která záběry porovnává s fotografiemi osob, jimž byl na základě předchozího nevhodného chování zakázán vstup na stadion. V případě, že je takový návštěvník odhalen, je upozorněna bezpečnostní služba a policie."

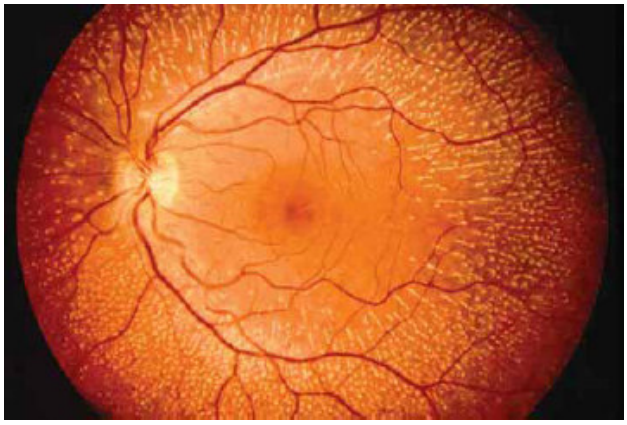
Vše spočívá ve využití biometriky, kdy dojde k porovnání charakteristik lidského těla. Tyto elektronické hlídače nelze oklamat tmavými brýlemi nebo falešným plnovousem, měří totiž vzdálenost mezi očima, tvar hlavy a proporce obličeje. Cílem je jak již bylo řečeno, nevpustit „chuligány“ na stadion. Ostatní návštěvníci nebudou ani nic vědět. Tento systém lze, použít k identifikaci obličeje i třeba na náměstí, v metru, v nákupním centru, prostě kdekoliv.

3.4 Sítnice oka

Použití této metody se zahrnuje do oblasti s největším stupněm zabezpečení. Jejím základem se stává světlo-citlivý povrch sítnice lidského oka, která obsahuje strukturu cév a to v okolí slepé skvrny. Sítnice se nachází na zadní straně oka a je složena z velkého množství nervových buněk. Pro neskenování obrazu se využívá zdroj světla s nízkou intenzitou záření a opto-elektronický systém. Využívá se LED dioda, která snižuje riziko ozáření oka. Takový obraz je poté převeden do 40 bitové číselné podoby. Uživatel se musí

dívat do přesně vyznačeného prostoru, což může způsobit problémy hlavně pro osoby používající brýle, z tohoto důvodu se tato metoda nestala příliš rozšířenou.

Obrázek 13: Zařízení pro snímání struktury cév sítnice oka

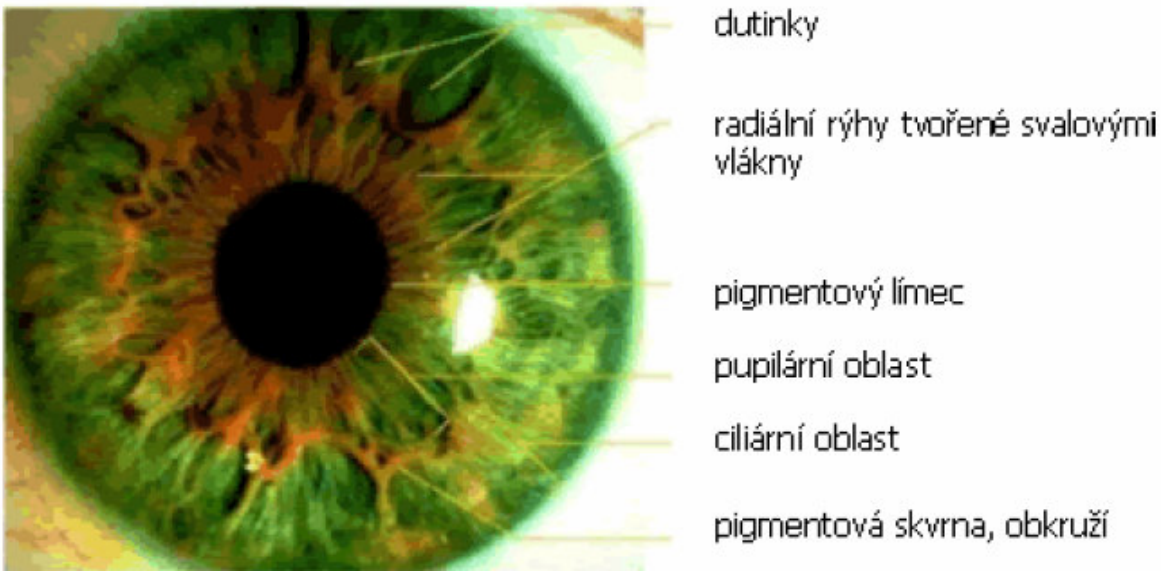


Obrázek 14: Struktura cév sítnice oka

3.5 Duhovka oka

Duhovka je sval uvnitř oka, která se vyvíjí během prenatálního růstu plodu. Reaguje na dopadající světlo a podle toho se reguluje zaostření čočky. Její zabarvení i struktura duhovky je geneticky závislá, ale vzorkování je náhodné a tudíž i jedinečné. Dokonce i jeden člověk má u každého oka jiné vzorkování. Jedná se o mladou metodu, první patent je evidován k roku 1994 a byl vyvinut americkým Úřadem pro jadernou bezpečnost. Snímání duhovky se provádí kvalitní digitální kamerou a infračerveným osvětlením. Během snímání

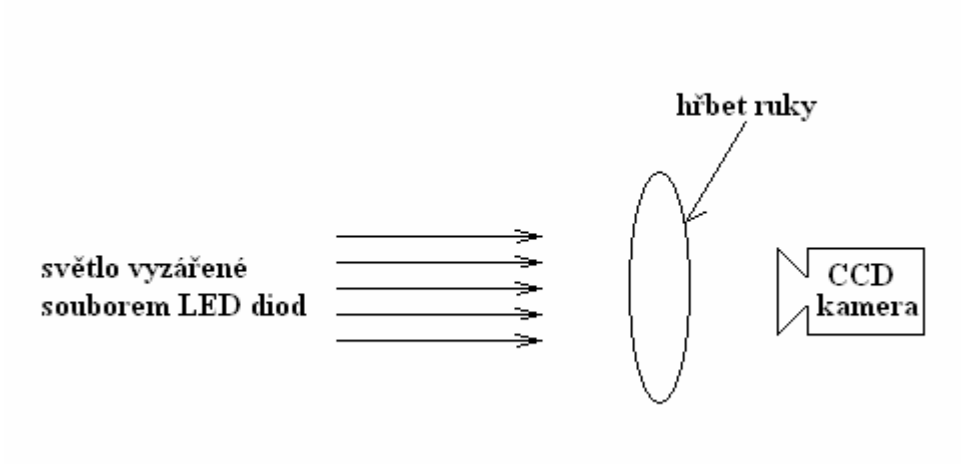
se duhovka mapuje do názorových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Podle těchto informací se vytvoří šablona vhodná pro identifikaci.



Obrázek 15: Struktura duhovky (zdroj: Kazderová, J., - Význam a charakteristika identifikačních biometrických systémů v průmyslu komerční bezpečnosti)

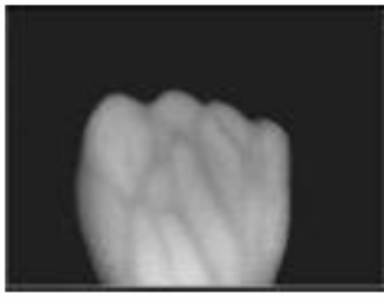
3.6 Struktura žil na zápěstí

Metoda rozpoznání člověka za pomocí struktury žil na zápěstí je jedna z nejnovějších, teprve roku 2000 se dostaly na trh komerčně dostupné systémy založené na této technologii. Jedná se o metodu, kdy se snímá hřbet ruky speciální kamerou v infračerveném světle. Struktura krevního řečiště se v dospělosti téměř nemění. Metoda je výrazná a jedinečná, vědecké studie prokázaly jedinečnost i mezi jednovaječnými dvojčaty. Ruka je prosvícena světelným zdrojem LED diod a vytvoří se obraz cév na základě odrazu tohoto světla. Obraz se snímá pomocí CCD kamery, dále se digitalizuje a zpracuje do podoby sítě cév. Hlavními identifikačními znaky jsou body, úhly, větvení cév a jejich tloušťka.



Obrázek 16: Princip snímání

„Použitím v zobrazení ve spektru blízkému infračervenému světlu (IR záření) se zvýrazní kontrast mezi cévním řečištěm hřbetu ruky a okolní kůží. Odkysličený hemoglobin v žilách pohlcuje světlo o vlnové délce přibližně $7{,}6.10^{-4}$mm, což je hodnota blízká infračervenému světlu. Hloubka absorpce IR záření živou tkání je přibližně 3 mm, tzn. že termální IR záření proniká do hřbetu ruky jen povrchově a v nasnímaném obrazu je pak nejvíce rozeznatelné právě celé cévní řečiště. Díky tomu jsou žíly na IR snímku vytaženy tmavou barvou, jak je patrné z obrázku.“[5]



Obrázek 17: IR zobrazení hřbetu ruky

[5] Ščurek, R. – Biometrické metody identifikace v bezpečnostní praxi, červen 2008

Dalšími potřebnými procesy pro úpravu získaného obrázku je segmentizace (rozdělit obraz na dvě části a to ruku a pozadí), vyhlazení a redukce šumu (vyhlazení obrazu cévního řečiště a potlačení případného vlivu tvaru hřbetu ruky), prahování (oddělení struktury žil od zbytku obrazu) a postprocessing (na obrázku zůstává jen struktura žil). Cílem těchto finálních úprav je získat obrázek pouze se strukturou žil hřbetu ruky ve stavu, který lze již označit jako šablonu, znázorněnou na následujícím obrázku.

Obrázek 18: Postprocessing hřbetu ruky (Zdroj: VŠB TU Ostrava)

3.7 Identifikace podle pachu

„[6]Kriminalistická odorologie je odvětvím kriminalistické techniky, která zkoumá vznik, význam a vlastnosti tělesného pachu člověka, rozvoj metod zajišťování pachových stop a jejich zkoumání pomocí analytických přístrojů. Jejím cílem je individuální identifikace osob nebo věcí.“

Identifikace člověka podle pachových stop využívá policie už mnoho let. I přes to, že lidský pach může být přesným měřením spolehlivým identifikačním znakem, v civilní sféře se neuplatnil. Lidský pach e skládá asi ze 30 chemických sloučenin, jejichž různá intenzita vytváří jedinečný pachový profil člověka. V civilní sféře je potřeba porovnávat a správně identifikovat více než jednu pachovou konzervu zároveň a právě proto neexistují dostatečně

[6] VIKTOR P. a kol., Kriminalistika, CERM, 2001

přesné senzory. Další nevýhodou jsou i změny ve skladbě pachových stop (způsobené emocionálně nebo hormonálně). Výhodou je, že lidský pach je vylučován nepřetržitě a bez ohledu na vůli člověka.

3.7.1 Individuální a přidružené pachy lidského těla

„Individuální pach vzniká při fyziologických procesech v organismu člověka. Pach vychází z těla s potem, kožním mazem, při odlupování zrohovatělé kůže - epidermis.

Přidružené pachy dělíme na:

- pachy obydlí
- pachy povolání či zaměstnání
- pachy kosmetických přípravků
- pachy dalších předmětů, které má člověk u sebe (léky, cigarety)
- pach šatů, obuvi

Ve volném terénu je lidský pach doplněn ještě dalšími přidruženými pachy:

- o pach rozrušené půdy
- o pach rozšlápnutých mikroorganismů
- o pach rostlin
- o pach prostředí, kde se pachová stopa nachází

Na pachovou stopu mají vliv vnější podmínky:

- a) teplota
- b) vlhkost vzduch
- c) tlak vzduchu a jeho pohyb
- d) struktura půdy a její porost

Za negativní podmínky jsou považovány vysoké teploty, přímé slunce, mráz, silný vítr, hustý či vytrvalý déšť nebo sněžení. Za kladné podmínky považujeme mlhu, mrholení, teplotu okolo 10° C, bezvětří. Důležitým faktorem pro vypracování či zajištění pachové

stopy je její stáří. Za čerstvé stopy jsou považovány stopy do jedné hodiny stáří, za normální stopy od jedné do tří hodin stáří, za vychladlé považujeme stopy starší více jak tři hodiny. Toto platí u pachových stop v terénu. Zpracovávání pachových stop pomocí přístrojů vyžaduje nákladně vybavené laboratoře. Na srovnávání pachu a na vypracování pachových stop jsou v dnešní době využíváni především speciálně cvičení psi.“[7]

3.8 DNA

Metoda identifikace člověka podle DNA (deoxyribonukleová kyselina) je používána asi od poloviny 80. let minulého století. Jedná se o velmi přesnou metodu, avšak nelze použít pro jednovaječná dvojčata, která mají shodné DNA. Získání otisku DNA je velmi náročný proces, který zahrnuje asi pět kroků k získání řetězce využitelné velikosti. Získaný otisk připomíná čárový kód, který se snadno převádí do elektronické podoby. Po odebrání vzorku tkáně je vypreparována spirála DNA, která se dále štěpí enzymem EcoR1. Získané fragmenty jsou po štěpení prosévány až se získá vhodný řetězec využitelné velikosti. Rentgenový snímek, neboli otisk DNA získáme z fragmentů, přenesených na nylonovou membránu, kde se přidají radioaktivní nebo obarvené genové sondy.

Tato metoda v komerční sféře není použitelná. Je často využívána pro identifikaci otce dítěte (přiznání otcovství) nebo k identifikaci mrtvol. Objevují se i databáze DNA zaměstnanců pro armády nebo záchranářské sbory.

3.8.1 Genetický kód

Genetický kód tvoří pouze 4 nukleové kyseliny:

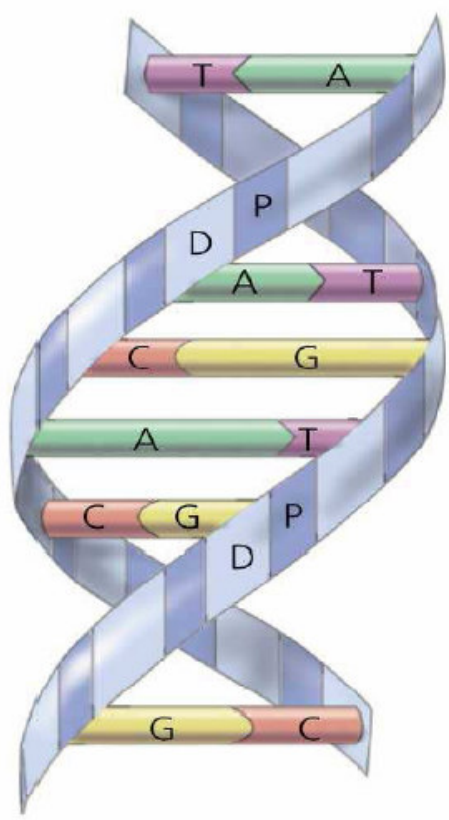
A – adenin

T – thymin

G – guanin

C - cytosin

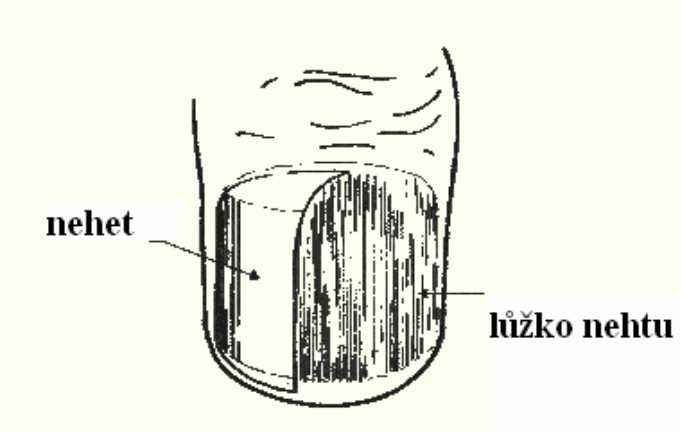
[7] Internetový portál www.cz-pes.cz, Lidský pach, nauka o pachu



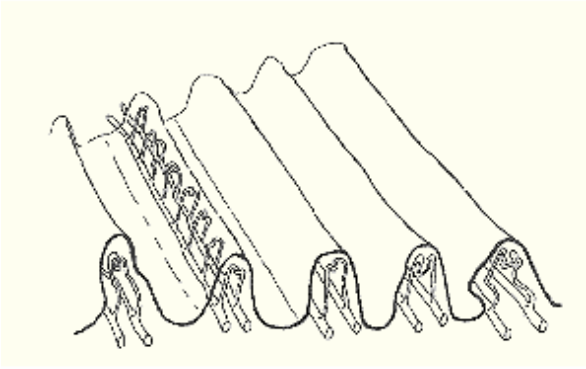
Obrázek 19: Struktura DNA (zdroj: Academy Artworks)

3.9 Podélné rýhování nehtů

Metoda identifikace člověka pomocí podélného rýhování nehtů se nezaměřuje přímo na nehet, ale na strukturu nehtového lůžka, která se nachází pod nehtem. K identifikaci se využívá přírodního polymeru (keratin), který mění orientaci dopadajícího světla. Zdroj polarizovaného světla pod určitým úhlem ozařuje nehet a tím zachytíme a analyzujeme fázové změny paprsku po odrazu z nehtu na přijímači. Signál se dále zpracuje na číselnou sekvenci čárového kódu, který lze porovnávat s databází. Na obrázku uvádím strukturu nehtu a řez nehtovým lůžkem.



Obrázek 20: Struktura nehtu (Zdroj: VŠB TU Ostrava)



Obrázek 21 Řez lůžkem nehtu (Zdroj: VŠB TU Ostrava)

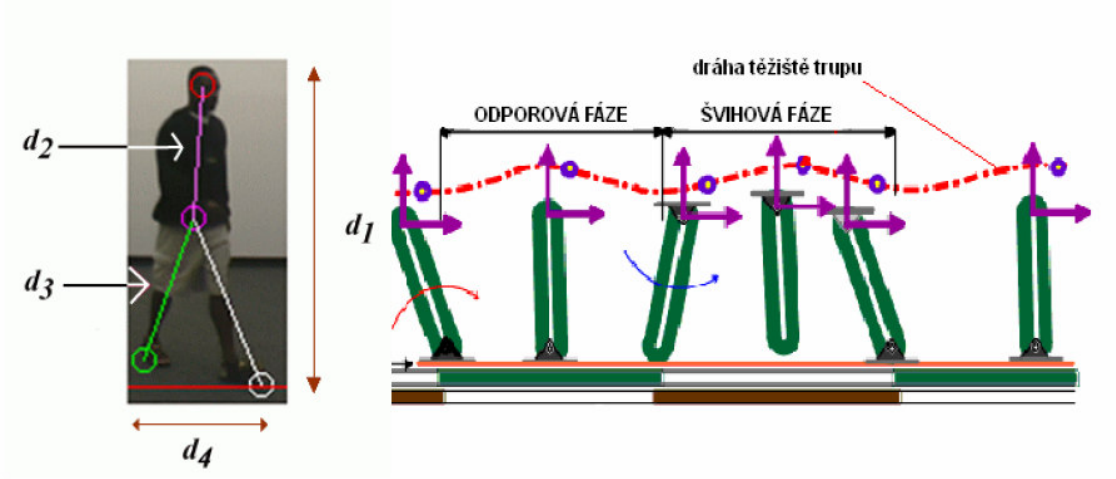
4 BEHAVIOMETRIKA

Behaviometrika je speciální kapitolou biometriky, kdy nedochází ke sledování fyzických vlastností člověka, ale vlastností, které člověk získává během svého života (naučené vlastnosti). Tyto identifikační znaky nelze odkoukat ani se je přesně naučit od ostatních lidí, tedy je kopírovat a popřípadě zneužít. Problémem je, že se tyto vlastnosti mění v čase, tedy nejsou po celý život člověka stálé. Typickým příkladem může být třeba styl psaní na klávesnici (četnost úderů, jejich rytmika), což jsou znaky pro každého člověka jedinečné. Tyto systémy umožňují například průběžně kontrolovat identitu člověka při práci na počítači, tedy nestačí se jen správně přihlásit do systému, protože systém pozná kdy na klávesnici pracuje jiná osoba (nebo s počítačovou myší). Mezi další metody behaviometriky patří například rozpoznání člověka podle stylu chůze, jeho typických znaků či gest. Do budoucna se uvažuje s využitím těchto metod při vyhledávání osob na velké vzdálenosti (pomocí družic na oběžné dráze).

4.1 Dynamika chůze

Metoda identifikace dle chůze se zaměřuje na pohyb po dvou nohách, nebo-li bipedální lokomoce. Chůze člověka je jedinečným charakteristickým znakem, stejně jako otisk prstu a je časově neměnná v relativně širokém věkovém období. S rozmachem záznamové a snímací techniky roste i rozvoj této metody. Je založena na různém dynamickém stereotypu chůze a celého pohybu těla člověka. Uplatnění však nachází jen ve forenzní sféře, dochází k prudkému nasazování průmyslových kamer na místa s velkým pohybem osob, tedy tam, kde se mohou vyskytovat pohřešovaní pachatelé (jako jsou letiště, nádraží, rušné ulice a náměstí atd.). Metoda nachází uplatnění i při vyšetřování loupežných přepadení, kdy je pachateli úplně zbytečné maskování obličeje či jakékoliv převleky.

Systém rozpoznává identitu člověka na základě porovnávání křivek drah, které opisují těžiště na lidském těle. Každý člověk má jedinečné svalově kosterní systém a jedinečný dynamický stereotyp, tudíž jsou křivky drah unikátní a můžou se použít pro identifikaci osoby. Na následujícím obrázku jsou vidět způsoby vytváření těchto křivek.



Obrázek 22: Postup vytváření dráhy těžiště trupu při bipedální lokomoci[8]

4.2 Dynamika podpisu

Jedinečnost identity člověka spočívající v písemném projevu a to z grafického hlediska je prokázanou záležitostí na základě dlouhodobých zkušeností, avšak doposud nebyla doložena staticky. „Soudobá filozofie a psychologie vysvětluje relativní stálost rukopisu učením o pohybových návycích a o dynamickém stereotypu, jímž se rozumí ustálený, automatizovaný systém reakcí organismu na opakující se podmínky. Při psacím pohybu nejedná se o „rukopis“, ale o „mozkopis“, přičemž ruka s celým svým svalově-kosterním ústrojím je jakýmsi seismografem zaznamenávajícím impulzy, které přicházejí z mozkového centra. Písmo je produktem centrální nervové soustavy a nezáleží na tom, zda je psáno rukou, nohou, či ústy, pokud pisatel dosáhl těmito orgány plné písařské zralosti.“[9]

Metoda je využívána od roku 1977. Zařízení využívané pro identifikaci člověka podle dynamického podpisu se často a mylně zaměňuje s elektronickým podpisem nebo se zařízením, které snímá samotný podpis jako obraz. Základem je ale zjištění tahu, tvaru a tlaku při psaní. Jednotlivé zařízení využívané pro tuto metodu mají společnou vlastnost použití technologií citlivých na dotek, jako jsou PDA záznamníky nebo digitalizační tabule.

[8] ŠČUREK R., Biometrické metody identifikace v bezpečnostní praxi, červen 2008

[9] PORADA V., Kriminalistika, akademické nakladatelství CERM, 2001

Zařízení mohou využívat jenom dynamických vlastností podpisu, ale některé snímají i statické a geometrické vlastnosti.

Základem pro sejmutí dynamických vlastností podpisu jsou:

- rychlost
- akcelerace
- časování
- tlak
- směr tahu

Tyto vlastnosti jsou zaznamenávány do trojrozměrného souřadnicového systému, kde osa „x" a „y" slouží pro určení rychlosti a směru tahu a osa „z" pak určuje tlak, který je při psaní podpisu vyvíjen na podložku.

Rukopis osoby se dělí na dvě stránky a to na grafickou a jazykovou. Z hlediska identifikace je význačná grafická stránka. Pisatele mohou ovlivňovat různé faktory, dělíme je na:

- vnitřní – tyto vnitřní faktory ovlivňují jak grafickou tak i vyjadřovací formu projevu. Jedná se především o stav svalově-kosterního aparátu, ovlivnění pisatele alkoholem nebo drogami. Pisatel může i úmyslně měnit své písmo za cílem anonymu a taky rychlost a kvalita úkonu psaní
- vnější – pisatele ovlivňují i vnější faktory, jako je prostředí, ve kterém se nachází (světlo, tma, zima), dále poloha, ve které psal (ve stoje, v sedě) nebo podle podložení paží, v jedoucím vozidle. Mezi vnější faktory řadíme i prostředky použité pro psaní (druh pera, podložky).

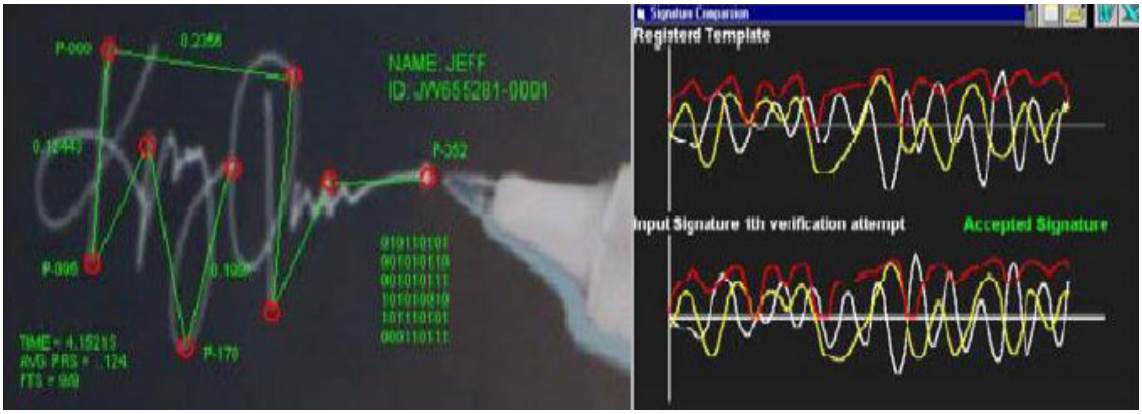
Grafická stránka projevu písma zkoumáme ve více rovinách:

- obecná rovina – grafická úprava – sklon, velikost, poměrové rozložení písmen, tvar a velikost odstavců, umístění nadpisů
- zvláštní rovina – ta zkoumá psané projevy na úrovni dílčích komponentů (náběhové tahy, spodní a horní kličky, koncové tahy), na úrovni základních

komponentů (celých písmen nebo označení) nebo na úrovni multikomponent (spojení dvou a nebo více písmen či označení)

4.2.1 Systémy využívané pro identifikaci podle dynamiky podpisu

Tyto systémy mají výhodu v tom, že se dynamické vlastnosti nedají odkoukat nebo nějak naučit (za statického obrazu podpisu jsou nečitelné). Dále se mohou prostřednictvím vhodného SW a PDA integrovat do již exitujících systémů. Jedinou nevýhodou je, že dokáží zvládat jedině verifikační proces, tedy porovnávání sejmutého vzorku s jednou šablonou (one-to-one). Na obrázku je znázorněno měření a SW rovnání dynamického podpisu.



Obrázek 23 Princip dynamického podpisu (Zdroj: VŠB TU Ostrava)

4.3 Psaní na klávesnici

Technologie identifikace uživatele na základě dynamiky psaní na klávesnici je velmi zajímavou formou zjišťování identity osoby. Jelikož je poměrně velká pravděpodobnost zranitelnosti charakteristik psaní na klávesnici u více uživatelů, doporučuje se používat jako sekundární autentizace přístupu. Dynamika psaní se může s časem měnit a sejmutí tzv. „otisku psaní na klávesnici“ vyžaduje i delší dobu, než například sejmutí otisku prstu.

Princip metody je založen tedy na sledování doby, po kterou jsou klávesy drženy a taky prodleva mezi jednotlivými stisky kláves. Nasazení metody se hodí nejenom pro ochranu nežádoucích přístupů k osobním počítačům, ale taky i ke vzdáleným informačním systémům pracujících v režimu on-line. Rozpoznávání identity uživatele může probíhat na

pozadí (během práce na počítači) a při zjištění odchylky od uloženého vzorku („otisku psaní na klávesnici“) může systém vyžadovat žádost o primární identifikaci. Systém tedy hlídá, kdy k počítači usedne jiná osoba a průběžně zajišťuje ochranu počítače před zneužitím dat jinou osobou.

4.4 Akustická charakteristika hlasu

Z hlediska kriminalistiky je fonoskopie specifickou metodou kriminalistické praktické činnosti, která se zabývá zkoumáním lidského hlasu. Zkoumání hlasových projevů zařazujeme mezi metody identifikace osob.

Fonoskopická zkoumání lze rozdělit do tří oblastí:

- zkoumání hlasových projevů
- zkoumání záznamových prostředků
- zkoumání dalších stop, které jsou v souvislosti s danou událostí (určení velikosti prostoru, místa)

4.4.1 Vývoj lidského hlasu

Hlas člověka prochází během života několika charakteristickými vývojovými stádii. Pro identifikační systémy je nejlepší hlas člověka ve stáří od 20-60 let, kdy je hlas poměrně dlouhou dobu relativně stálý. Změny hlasu se projevují po prodělání různých nemocí nebo pozměňováním návyků. Vlivem nemoci se může změnit hlas trvale nebo dočasně. Dočasné změny vylučují provedení identifikace člověka. Kdežto trvalé změny hlasu jsou významnější, protože se vytváří jiné významné identifikační znaky hlasu (markanty).

4.4.2 Složení hlasového traktu a mluvních orgánů

Aktivní mluvní orgány

· A – mandibula (dolní čelist)

· B – labia (rty)

· C – Lingea (jazyk)

· D – velum (měkké patro)

· E – chordae vocales (hlasivky)

Vokální (hlasový) trakt

· Dutina ústní – orální

· Dutina nosní – nasální

· Dutina hrdelní – laryngální

· Velum, měkké patro

Generování řeci se skládá z:

· Plíce (zdroj stejnosměrného proudu)

· Hlasivky (impulsní generátor)

· Hrany, štěrbiny (šumový generátor)

· Artikulační trakt (lineární přenosový systém)

4.4.3 Identifikační systémy pracující na principu ověření hlasu

Tyto identifikační systémy pracují na principu srovnávání hlasového záznamu a vzorku hlasu. Pro ověření člověka, který se pokouší o identifikaci slouží předem namluvené klíčové věty. Výhodou je, že i ten nejlepší imitátor hlasu nedokáže přelstít tento systém, protože nezná potřebný klíčový význam věty. Některé identifikační systémy ověřují dodatečně osobu tím, že zadá jednoduchou otázku. Není tedy vyhodnocována jenom shoda hlasového záznamu se vzorkem, ale i logika odpovědi. Problém nastává v praktickém využití (v reálných místech), kdy se identifikovaná osoba pohybuje v rušném prostředí a vznikají tak rušivé vlivy pro proces identifikace.

5 BIOMETRICKÉ PASY

Někteří ochránci občanských práv zavádění biometrických pasů kritizují a tvrdí, že pasy zcela bezpečné nejsou. Vidí riziko především v tom, že údaje budou uloženy v databázích a mohou se dostat do rukou například komerčních firem. V médiích se objevila také zpráva, že jistý počítačový expert prokázal, že je možno údaje v dokumentu zkopírovat z jednoho čipu na druhý. Nemluvilo se však vůbec o tom, že údaje nedokázal přečíst. České pasy však navíc podle ministerstva vnitra využívají zcela jinou technologii, než doklady vydávané v Německu či USA a jsou naprosto bezpečné.

Podle nařízení Rady EU č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy, jsou všechny státy EU povinny vydávat pasy, které obsahují biometrické prvky (otisky prstů) od konce února 2008. Tyto biometrické charakteristiky jsou používány pro ověřování autenticity pasů a víz a také pro ověřování identity držitele pasu.

„V cestovním dokladu jsou čipy takzvaně radiofrekvenční. Ve stránce cestovního dokladu tedy je zataven čip s anténou. Údaje je pak samozřejmě možné číst distančně, to znamená bez kontaktu s nějakým čtecím zařízením. Expertní studie, které byly provedeny ve Spojených státech, říkají, že je možné číst tento čip až na vzdálenost dvacet metrů. Čtecí vzdálenost pro biometrické pasy je však jenom 10-20cm. Kdekoli se budete pohybovat, tajné čtecí zařízení může snímat údaje z biometrického pasu. V čipu budou zapsány všechny údaje, které jsou i ve viditelné zóně cestovního dokladu. Je tam, kromě digitálního foto a otisku prstu, vaše jméno, příjmení, rodné číslo, národnost, datum vydání, atd.“[10]

5.1 Pracoviště Městského úřadu - oddělení cestovních dokladů

Ve spolupráci s Městským úřadem ve Valašských Kloboukách jsem zpracoval základní informace o procesu tvorby biometrického pasu žadatele. Jde v podstatě o celou řadu administrativních úkonů, které v přesné posloupnosti vedou k získání žádosti o nový biometrický pas. Jedná se o tyto kroky:

[10] http://www.radio.cz/cz/clanek/73041

- přihlášení žadatele o žádost k vydání nového biometrického pasu
- zkontrolování údajů o žadateli
- sejmutí fotografie obličeje
- sejmutí otisků prstů
- ztotožnění otisků
- sejmutí biodynamického podpisu
- automatické odeslání údajů k dalšímu zpracování

5.1.1 Bezpečnost pracoviště

Bezpečnost provozu pracoviště je zajištěno elektronickým systémem přístupu, mechanickým zábranným systémem a elektronickým zabezpečovacím systémem. Každý pracovník tohoto oddělení vlastní token a čipovou kartu k přihlášení do systému. Před vstupem do místnosti pracoviště se pracovník přihlásí pomocí tokenu a odemkne místnost viz obrázek 24.

Obrázek 24: přístupový režim pracovníka pomocí tokenu

Další přihlášení se provádí pomocí čipové karty do počítačového systému přímo na pracovišti. Karta se zasune do čtečky zařízení, které je propojeno s počítačovým systémem a následně pracovník zadá svůj osobní PIN kód. Karta je zasunuta ve čtečce po celou dobu práce se systémem. Pokud není zaznamenána delší činnost se zařízením, systém se automaticky odpojí. Tak je zajištěna bezpečnost při případném zapomenutí spuštění programu (například při odchodu z místnosti) a zabráněna tak neoprávněná manipulace. Čtečka čipové přihlašovací karty pracovníka je znázorněna na následujícím obrázku.

Obrázek 25: Čtečka čipové karty pracovníka

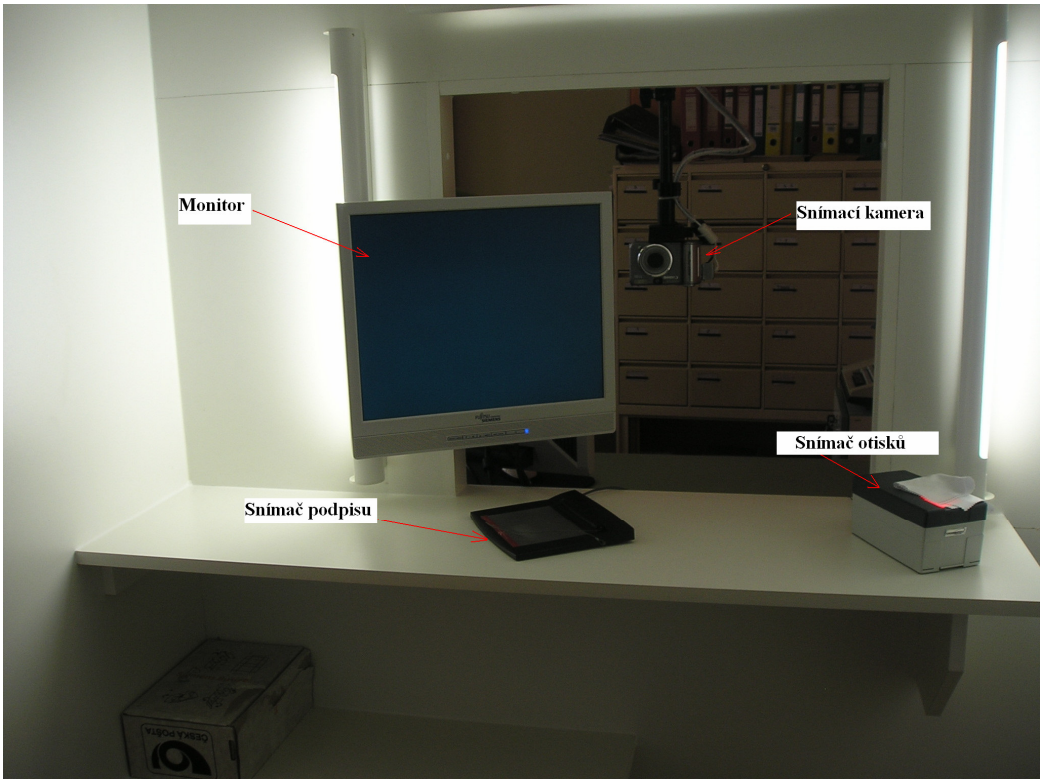
Úvodní obrazovka programu obsahuje pracovní prostředí s celou řadou potřebných úkonů, které pracovník může vykonávat, jedná se o tyto operace:

- Řízení o žádosti
- Pokračování v řízení
- Kontrola a reklamace e-pasu
- Řešení nevyrobeného e-pasu
- Kontrola e-pasu pro držitele
- Předání e-pasu

- Zneplatnění e-pasu
- Sestava žádostí
- Zpracování žádostí ze ZÚ (zastupitelský úřad)
- Řešení reklamace ze ZÚ
- Změna PIN na kartě
- Ukončení aplikace
- Nápověda

5.1.2 Řízení o žádosti

Řízení o žádosti je proces, kdy od žadatele získáváme potřebné administrativní a biometrické informace potřebné pro vyrobení cestovního dokladu. Spočívá v přesné posloupnosti na sebe navazujících kroků, které určuje počítačový program. Komunikace mezi pracovníkem a žadatelem je v oddělené místnosti. Žadatel sedí ve vyhrazeném prostoru, kde se nachází příslušná technická zařízení jako je kamera pro pořízení fotografie, snímač otisků prstů, zařízení pro sejmutí biodynamického podpisu žadatele a monitor propojený se systémem sloužící pro kontrolu prováděných jednotlivých kroků. Místnost určená pro žadatele je znázorněná níže na obrázku.



Obrázek 26: Místnost určená pro žadatele

Nejprve žadatel předloží platný občanský průkaz a pomocí čtečky dokladů se sejmou data o žadateli jako je například rodné číslo, číslo dokladu, jméno, příjmení atd. Tyto informace je nutné překontrolovat, protože systém tyto informace může načíst chybně. V případě chyby se informace buď načtou znovu nebo se ručně opraví. Na obrázku můžeme vidět čtečku dokladů se strojově čitelnými údaji.

Obrázek 27: Čtečka dokladů se strojově čitelnými údaji

Po načtení a zkontrolování všech údajů o žadateli se dále vloží další potřebné úřední záznamy, které není možné načíst z občanského průkazu.

5.1.3 Pořízení obrazu obličeje

Žadatel sedí ve své místnosti a před sebou má umístěnou kameru, která snímá jeho obličej tak jak je to znázorněno na obrázku 28. Pořízenou fotografii obličeje vidí i žadatel na monitoru, který je umístěn v jeho blízkosti. Fotografie obličeje žadatele je ukládána na radiofrekvenční čip v barevném formátu a přímo na stránku pasu je tištěna černobíle.

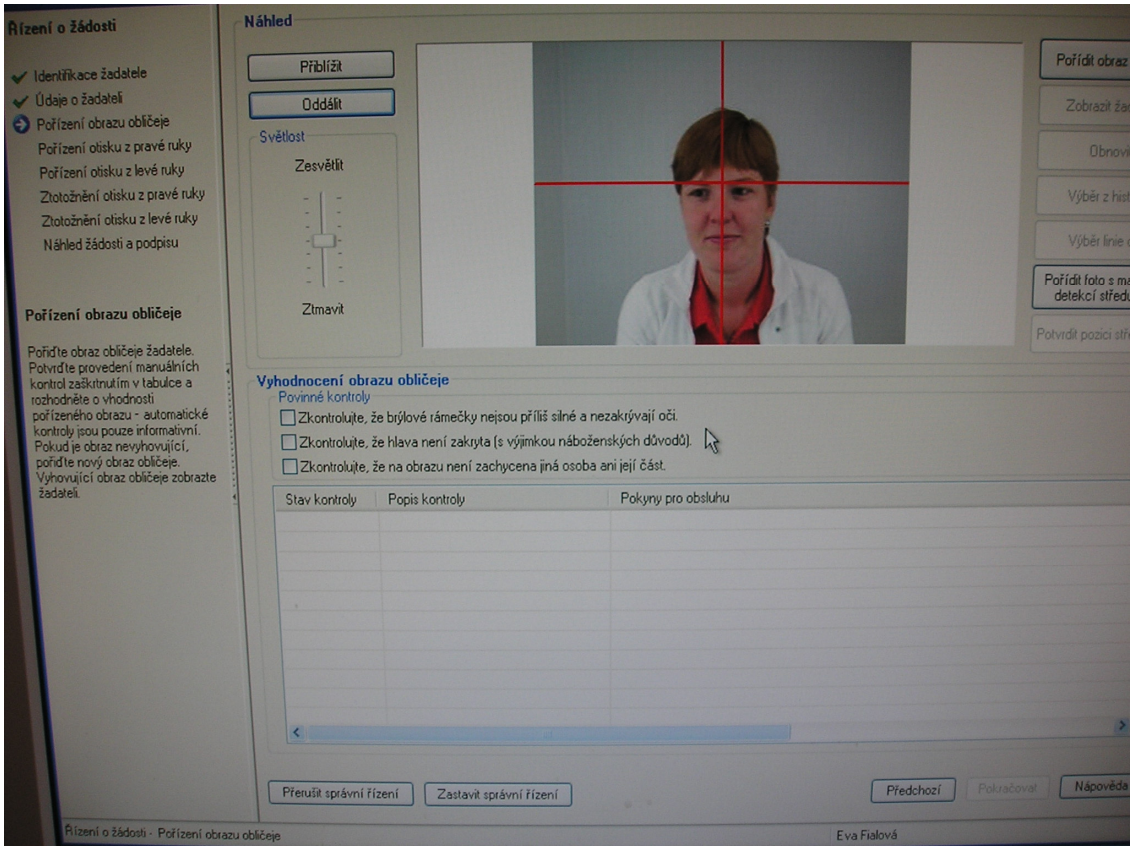
Obrázek 28: Pořízení obrazu obličeje

Úředník vydá pokyn systému k pořízení snímku a ten se zobrazí na monitoru počítače. Na této obrazovce se provádí tyto operace:

- přiblíží (zvětší), nebo
- oddálí (zmenší) obraz obličeje;
- může změnit světlost snímku;
- zobrazí obraz žadatelova obličeje;
- pořídí obraz obličeje automaticky nebo s manuálním určením středu očí
- zobrazí výsledky kontrol ICAO;
- potvrdí provedení povinných kontrol;
- zobrazí výsledné snímky žadateli;
- dále může volitelně: a) opakovat pořízení obrazu obličeje
  b) vybrat jiný, dříve pořízený snímek
  c) vybrat pro další použití snímek s posunutou linií očí

- zastavit / přerušit správní řízení

Pořízený obraz obličeje se zobrazuje v pracovním oknu programu znázorněném níže na obrázku 29.



Obrázek 29: Pracovní okno pořízení obrazu obličeje

Kontrola pořízeného snímku obličeje:

Úředník zkontroluje všechny parametry pořízeného snímku obličeje a při zjištěných nedostatcích se snímek musí zaktualizovat novým snímkem. Kontrola se provádí podle těchto parametrů:

- Barevnost pozadí – zkontroluje, zda nejsou rušivé prvky na pozadí (stíny, poškození barvy, nežádoucí předměty), a tyto prvky eliminuje
- Barevnost fotografie a odstíny šedi – obraz obličeje nesplňuje podmínky na škálu odstínů šedi (kontrast). Změní se osvětlení, tím se změní kontrast, jinak se kontaktuje technická podpora

- Čelní pozice hlavy žadatele – zkontroluje se, zda hlava žadatele je v čelní pozici, tj. přímá pozice vůči fotoaparátu s hlavou namířenou přímo do fotoaparátu
- Čirosti skel brýlí – pokud má žadatel brýle, pak tyto brýle mají čirá a čistá skla
- Efekt červených očí – pokud byl detekován efekt červených očí – kontaktovat technickou podporu (v kabinách totiž tento jev nemůže nastat, nepoužívá se blesku)
- Kontrola zakrytí tváře – obličej žadatele nesmí být zakryt nějakým předmětem (šátek, ruka)
- Míra (doba) expozice – změnit nastavení clony na fotoaparátu, obrázek je buď příliš tmavý, nebo příliš světlý
- Obroučky brýlí zakrývají oči
- Odlesky na brýlích
- Otevřená ústa
- Přímý pohled do fotoaparátu – žadatel se musí dívat přímo do fotoaparátu
- Správnost osvětlení a přirozené barvy – musí svítit všechna světla
- Stíny a přesvětlená místa na tváři – kontrola, zda obličej není zastíněn nebo nevykazuje tmavé, případně přesvětlené místo
- Zaostření
- Zavřené či zakryté oči

5.1.4 Pořízení otisků prstů

Po pořízení obrazu obličeje následuje druhý krok a to sejmutí otisků prstů. Požaduje se sejmutí ukazováčku pravé i levé ruky. Otisky prstů se pořizují u osob ve věkovém rozmezí 12 – 75 let. Snímání otisku prstu je znázorněn na dalším obrázku:

Obrázek 30: Snímání otisku prstu žadatele

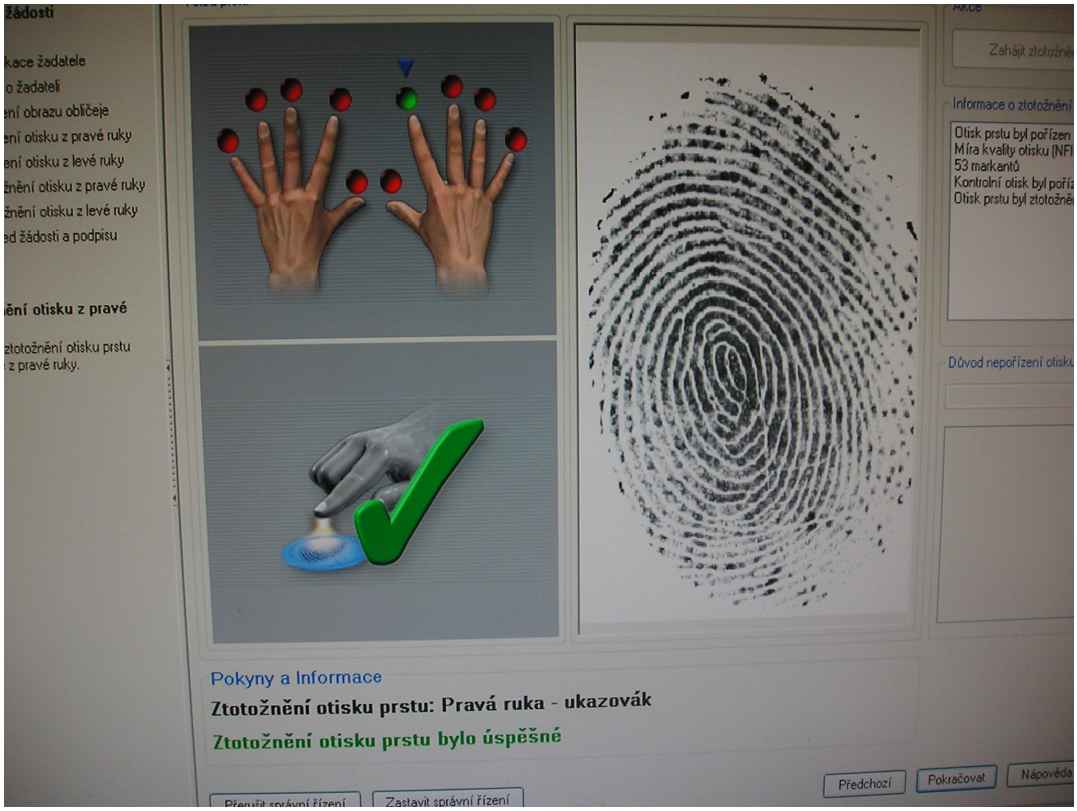
Proces pořízení otisků lze rozdělit na dvě části:

- V první části procesu jsou **pořízeny otisky prstů** – nejprve jsou z přiloženého prstu pravé ruky sejmuty 3 pracovní otisky prstu a z nich je pak aplikací automaticky vybrán otisk s nejlepšími parametry (nejkvalitnějšími) pro použití v e-pasu. Pořízení otisku lze opakovat libovolněkrát. První část procesu se pak opakuje pro získání otisku prstu levé ruky.
- V druhé části procesu je provedena kontrola kvality otisků pořízených v první části procesu, tzv. **ztotožnění** – opět nejprve pro pravou ruku, potom pro levou. Je sejmut jeden otisk prstu, tzv. kontrolní, který je porovnán s otiskem

pořízeným v první části procesu – pokud jsou kontrolní otisk a pořízený otisk vyhodnoceny jako shodné (byly ztotožněny), pak pořízený otisk může být v e-pasu použit. V případě neúspěchu lze pokus ztotožnění otisku opakovat 2x. Pokud není úspěšný ani jeden pokus o ztotožnění, otisk je odstraněn a je nutno pořídit otisk dalšího prstu dané ruky, nebo zadat důvod nepořízení otisku.

Pokud nelze otisk prstu pořídit (např. pro fyzickou indispozici žadatele), nebo nelze pořídit kvalitní otisk (otisk nelze ztotožnit), je nutno uvést důvod, pro který nebyl otisk prstu pořízen.

Proces snímání otisků prstů a následné ztotožnění je graficky znázorněno v okně programu. Pracovník se pomocí těchto grafických informací lépe orientuje při zadávání pokynů žadateli. Na následujícím obrázku vidíme takové okno pro ztotožnění prstu pravé ruky.



Obrázek 31: Grafické okno programu určené pro ztotožnění otisku

5.1.5 Pořízení podpisového vzoru

Dříve než se dostaneme k podpisovému vzoru na podpisovém tabletu dojde k vygenerování náhledu žádosti. Na této obrazovce se:

- zobrazí se první nebo druhá strana vygenerované žádosti
- určuje se, zda: a) bude pořízen digitální podpis, nebo
  b) existují důvody, pro které podpis nemůže být pořízen
- tiskne se vygenerovaná žádost
- případně zahájí a ukončí proces digitalizace podpisu a zkontroluje výsledný digitalizovaný podpis (v případě potřeby postup opakovat od kroku 3) – tisk vygenerované žádosti
- dokončí proces pořízené žádosti
- zastavit / přerušit správní řízení

Na dalším obrázku vidíme technické zařízení pro sejmutí podpisového vzoru, který se taky nazývá tablet.

Obrázek 32: Tablet pro digitalizaci podpisu

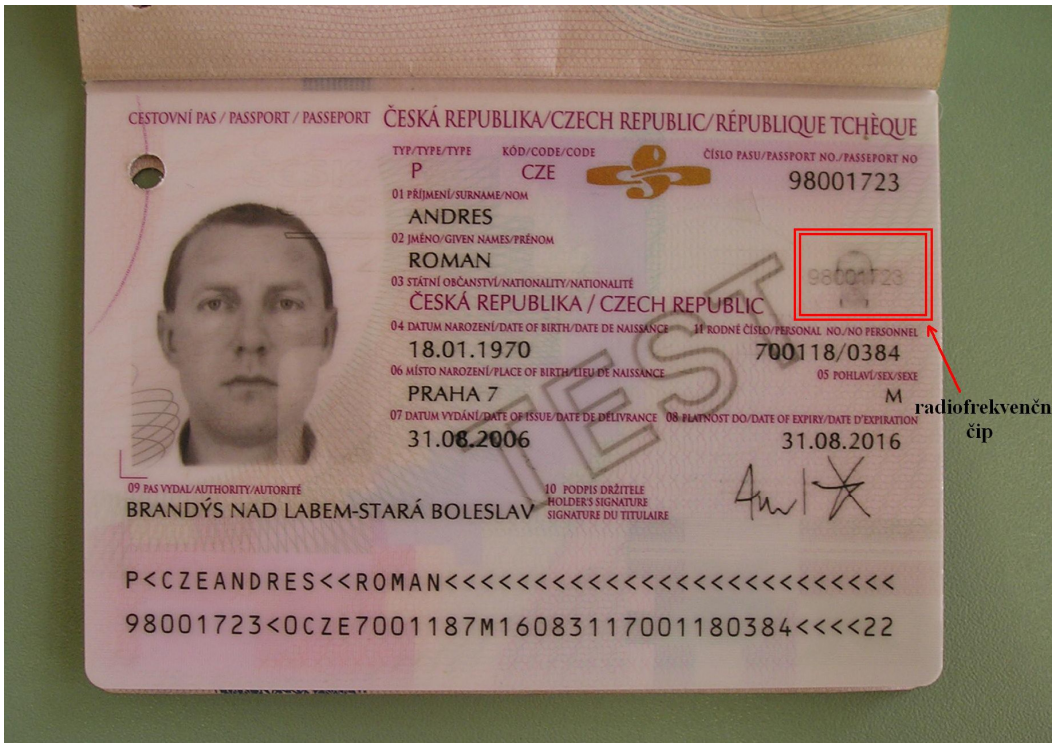
5.1.6 Vyhotovení a vydání biometrického e-pasu

Pokud se pořídí všechny potřebné informace o žadateli (jak biometrické tak administrativní), dochází k automatickému odeslání těchto záznamů do Státní tiskárny cenin, kde se e-pas ještě ten den vyrobí. Následuje však 60ti denní lhůta, kdy se informace ještě ponechávají v systému. Tato lhůta je stanovena pro reklamační řízení e-pasu.

Pokud žadatel požaduje připsání dětí do svého pasu, může tak udělat prostřednictvím speciální žádosti, která se po vyrobení e-pasu vlepí na stránku cestovního dokumentu. Děti se připisují maximálně tři a do věku 10 let. Dokument pro připsání dětí je na obrázku níže.

Obrázek 33: formulář pro připsání dětí do e-pasu rodičů

Na dalším obrázku můžeme vidět vzor biometrického e-pasu. V červeném rámečku je znázorněno místo, kde se nachází radiofrekvenční čip, na kterém jsou umístěna biometrická data jako je otisk prstu pravé i levé ruky, podpis žadatele v digitální formě a barevná fotografie s údaji o poloze očí, nosu atd. Taková biometrická fotografie s geometrií tváře je znázorněna na obrázku 12 v kapitole 3.3.



Obrázek 34: Vzor biometrického pasu

Po obdržení e-pasu si žadatel na úřadě cestovní dokladů překontroluje správnost všech viditelných informací a funkčnost e-pasu, co se týká radiofrekvenčního čipu se otestuje na přístroji, tzv. kiosek. Ten je znázorněn na fotografii 35.

Obrázek 35: Kiosek – ověření funkčnosti e-pasu

5.1.7 Bezpečnost dat

Technické řešení zvolené v České republice splňuje požadavek na bezpečnost čipu a na ochranu dat v čipu dle doporučení EU, tzv. Basic Access Control, což chrání data před rozkódováním bez příslušného elektronického klíče. Všechny osobní údaje žadatelů jsou po celou dobu existence v informačním systému chráněny před zneužitím nebo jiným neoprávněným zpracováním (jednotlivé kroky nakládání s osobními údaji občana jsou v informačním systému evidovány a lze je zpětně ověřit).

Biometrické údaje žadatelů jsou ihned po pořízení, tzn. ještě na počítači na obecním úřadě obce s rozšířenou působností před odesláním do centrálního systému, zašifrovány tak, že dešifrovat je mohou pouze oprávněné subjekty. Po vydání (vyrobení) nového cestovního pasu jsou biometrické údaje po 60 dnech výrobcem zlikvidovány a zůstanou pouze v nosiči dat cestovního pasu se strojově čitelnými údaji.

Bezpečnost dat před výpadkem elektrického proudu je řešena záložním zdrojem umístěným přímo v kanceláři. Tento záložní zdroj dovoluje práci se systémem po výpadku elektrické energie ze sítě ještě asi 5-7 minut. Tahle doba je dostačující pro dokončení řízení o žádost s žadatelem o biometrický pas, nikoliv však pro delší dobu práce po celou dobu úředního dne.

Obrázek 36: Záložní zdroj systému

ZÁVĚR

Pro člověka se stala oblast biometrie poměrně rozšířenou záležitostí, jelikož přešla od jednoduchých metod měření pouhých fyzických znaků i do oblasti behaviorálních a více efektivnějších systémů.Technologie biometrických systémů je již ověřená a dostupná pro masové použití, ale ještě je potřeba překonat informovaností a popularizací bariéru na straně uživatelů, pro něž je používání některých systémů nepohodlné (snímání otisků), nebo se jich dokonce mohou obávat (snímání oční sítnice či duhovky).

Cílem diplomové práce bylo předvést ucelený materiál týkající se biometrických identifikačních metod s vysvětlením základních a nezbytných pojmů důležitých k pochopení celé problematiky a objasnit jednotlivé metody identifikace včetně hodnocení kritérií. Praktická část zahrnuje většinu dostupných a využívaných metod biometrické identifikace a dále se zaměřuje na dnes už rozšířené biometrické pasy, které v sobě skrývají jak vizuální administrativní informace, ale také za pomocí popsaných metod jsou získávány biometrické informace o člověku a tyto jsou uloženy v digitální formě na radiofrekvenčním čipu. Veškeré pracoviště pro sběr biometrických informací je vybaveno nejmodernější technikou, která zahrnuje výpočetní techniku, software určený pro zpracování informací a hardware potřebný k zajištění snímání biometrických vlastností. Práce rozpracovává přesný postup pracovníka při řízení žádosti, bezpečnostní opatření a profesionální přístup k získávání citlivých biometrických vlastností. Cílem vydávání biometrických e-pasů je zjednodušení kontroly identity člověka a hlavně zvýšení bezpečnosti. Nejedná se tedy o sběr biometrických informací o člověku a vytváření nějaké databáze (což si laická veřejnost často myslí), všechny informace jsou po záruční lhůtě zničeny a biometrická informace zůstává jen v digitální podobě na čipu e-pasu.

ZÁVĚR V ANGLIČTINĚ

For a person with the biometrics become quite widespread issue since moving from simple methods of measuring just physical characteristics into the behavioral and more efficient systémů.Technologie biometric systems are already proven and available for mass use, but still need to overcome the awareness and popularization of the barrier users, for whom the use of certain systems uncomfortable (fingerprinting), or they may even fear (retinal scan or iris).

Aim of this thesis was to present a comprehensive material for biometric identification methods with an explanation of basic and essential concepts relevant to understanding the whole issue and clarify the various identification methods including the evaluation criteria. The practical part includes most of the available and used methods of biometric identification and focus on the now widespread biometric passports to create the visual as administrative information, but also using the methods described are obtained biometric information about the man and they are stored in digital form radiofrequency chip. All work to collect biometric information is equipped with the latest technology, including computer equipment, software for data processing and hardware required to provide biometric sensing properties. Work develops a rigorous procedure in the management of application security measures and professional approach to obtain sensitive biometric features. The aim of the issuance of biometric e-passports is to facilitate the control of human identity, and especially safer. It is not a collection of biometric information of people and creating a database (which the general public often think), all information is destroyed after the warranty period, and biometric information remains only in digital form on the e-passport chip.

SEZNAM POUŽITÉ LITERATURY

[1]http://www.cz-pes.cz/literatura-sl-kynologie-3.php

[2] Porada, V. a kol., Kriminalistika, Akademické nakladatelství CERM, Brno 2001

[3] Ščurek, R., Biometrické metody identifikace osob v bezpečnostní praxi, 2008

[4] Drahanský, M., Přehled biometrických systémů a testování jejich spolehlivosti, VUT Brno

[5] Čandík, M., Objektová bezpečnost II, UTB Zlín 2004

[6] Lacký, V., Technologie v komerční bezpečnosti I, UTB Zlín 2004

[7] Musil, J. a kol., Kriminalistika, Praha C.H.BECK 2001

[8] Ing. Rita Pužmanová, CSc., MBA, Biometrické systémy v praxi, IT SYSTEM 3/2004 – BEZPEČNOST, Dostupný z WWW:
<http://www.systemonline.cz/site/bezpecnost/04_02puzman.htm>

[9] http://www.radio.cz/cz/clanek/73041

[10] Kazderova, J., Význam a charakteristika identifikačních biometrických systémů v průmyslu komerční bezpečnosti, UTB ve Zlíně 2007

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

LDA	Linear Discriminant Analysis
PCA	Principal Components Analysis
EBGM	Elastic bunch graph matching
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTE/FER	Failure to Enroll Rate
FIR	False Identification Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
CCD	Charge-couple device
IR	Infračervené záření
CMOS	Complementary Metal Oxid Semiconductor
TFT	Thin Film Transistor
AFIS	Automated Fingerprint Identification System
FBI	Federal Bureau Of Investigation
ACS	Access Control Systems
DNA	Deoxyribonukleová kyselina

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ