Význam a charakteristika identifikačních biometrických systémů v průmyslu komerční bezpečnosti

Meaning and characteristic of identification biometric systems in the industry of commercial security

Jaroslava KAZDEROVÁ

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jaroslava KAZDEROVÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Význam a charakteristika identifikačních biometrických systémů v průmyslu komerční bezpečnosti.**

Zásady pro vypracování:

1. Seznámení se s problematikou využití, technickými parametry a konstrukcemi identifikačních biometrických systémů pro kontrolu osob.
2. Biometrické metody identifikace, identifikace podle otisku prstů, biometrické aplikace, informační obsah řeči.
3. Zpracování akustického signálu, fonetická analýza a vektorová kvantizace.
4. Obsahem bakalářské práce budou nové trendy ve vývoji, zpracování řeči v časové oblasti a analýza.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

SOJKA E.: Digitální zpracování a analýza obrazů, VŠB Ostrava 2000
KŘEČEK S.: Příručka zabezpečovací techniky, Praha, 2003
UHLÁŘ: Technická ochrana objektů, PA ČR, Praha, 2001
BITTO O.: Šifrování a biometrika, ComputerMedia, 2005
PETR J.A KOLEKTIV: Mluvnice češtiny, Praha: Akademia, 1986

Vedoucí bakalářské práce: **Ing. Ján Ivanka**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **29. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ve své bakalářské práci se zabývám biometrií, neboli metodou jednoznačné identifikace osob na základě jedinečnosti fyziologických a behaviorálních vlastností lidského těla. Práce objasňuje význam slova „ biometrie “, základní pojmy, s kterými se v dané oblasti setkáváme, dále proces registrace, ukládání a zpracování biometrických dat. Přehled jednotlivých metod a principů funkcí biometrické identifikace poskytuje informace o vhodnosti aplikace uvedených metod v praxi. Na podkladě historického vývoje dokumentuji změny a rozvoj biometrických metod a úspěšnou implementaci do řady oborů a to především na základě revolučních změn v oblasti informačních technologií

Závěrečná část bakalářské práce je zaměřena na prezentaci možností a významu využití biometrie v běžném životě dnešních i budoucích generací.

Klíčová slova: biometrie, verifikace, identifikace, etalon, token,

ABSTRACT

In my bachelor work I deal with biometrics alias the method of unique identification of people on the basis of unique physiological and behavioral characteristics of human body. The work clarifies the meaning of the word „ biometrics “ , basic definitions which we encounter in given field, furthermore the process of registering, storing and processing of biometrical data. The overview of individual methods and principles of biometrical identification functions is giving information about the suitability for application of mentioned methods in real use. On the basis of historical progress I have documented here the changes and development of biometrical methods as well as successful implementation into a range of departments mainly thanks to revolutional changes in the field of information technologies.

The last chapter of my bachelor work is dedicated to the presentation of options and importance of biometric in common life todays and future generations.

Keywords: biometrics, verification, identification, standard, token

V úvodu své práce bych chtěla poděkovat Ing. Jánu Ivankovi za odborné znalosti, vědomosti a rady poskytnuté v rámci odborných konzultací, za připomínky a návrhy k úpravě a formě zpracování bakalářské práce.

Dále bych ráda poděkovala své rodině za podporu, kterou mi věnovali během mého studia.

Prohlašuji, že jsem na bakalářské práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uvedena jako spoluautor.

Ve Zlíně

…….

Podpis diplomanta

OBSAH

ÚVOD

Biometriky a moderní biometrické systémy zaznamenávají zvýšenou pozornost především v několika posledních letech a desetiletích, ačkoliv kořeny biometrik sahají až do období několika tisíc let před naším letopočtem. V současné době je svět aktivizován v boji proti terorismu. Biometrické metody se stávají aktuálními při bezpečném zjišťování identity osob legálně překračujících hranice států, vstupujících do významných střežených objektů, jako jsou banky, letiště, vojenské a státní budovy apod., a při vyhledávání osob se záznamem v databázi, např. mezi diváky na sportovních střetnutích, v zábavních podnicích apod.

V každodenním životě, osobním i pracovním, se v současné době otevírá pro biometrické metody široká oblast aplikací na nespočetně mnoha rozhraních mezi člověkem a počítači i výpočetními systémy, např. zajišťujícími uskutečňování nejrůznějších finančních transakcí, fungujících ve spotřební elektronice a v neposlední řadě také při řízení správních a technologických procesů v průmyslu. Posuzovat jednotlivé biometrické metody není jednoduché a případná volba některé z nich závisí na mnoha faktorech. Především je třeba vyjasnit, kde a které biometrické systémy nebo technologie lze v široké míře uplatnit, aby byly maximálně využity jejich přednosti a minimalizovány jejich zápory - zachování dlouhodobé přesnosti a spolehlivosti biometrické metody, náklady na pořizování biometrických dat a jejich kontrolu, ochrana biometrických dat před zcizením nebo znehodnocením apod. Značná péče je věnována zejména ochraně biometrických dat použitých v podobě digitálního osobního průkazu.

Jedním ze základních problémů při volbě biometrické metody je optimálně stanovit úroveň bezpečnosti. Se systémem nastaveným především na stranu bezpečnosti lze dosáhnout malé nebo i nulové pravděpodobnosti „ falešného přijetí “ (ang. v. False Akcept Rate, dále jen FAR), ale za cenu poměrně velkého počtu případů „ falešného odmítnutí “ (ang. v. False Reject Rate, dále jen FRR). To může některé uživatele při přihlašování nežádoucím způsobem flustrovat. Systém nastavený na menší hodnotu FRR se sice bude naopak příjemně používat, ale pravděpodobnost průniku neoprávněného uživatele do systému bude větší.

Identity management, tedy identifikace osob pomocí biometrických metod a související aplikace, stojí a padají s pozitivním vnímáním veřejnosti. Hlavní podstatou problému je porozumět regionálním či národním pohledům na biometrické metody a jejich používání.

S postupující globalizací budou systémy pro identity management přerůstat hranice – a je důležité, aby nenarazily na kulturní, sociální nebo etické bariéry.

Velice důležitým krokem k širokému uplatnění biometrie v našem každodenním životě je mimo technického pokroku v této oblasti rovněž osvěta, která veřejnost seznámí s podstatou identifikace osob pomocí biometrických metod, jednotlivými biometrickými metodami a způsoby jejich uplatnění.

Cílem osvěty je a bude snaha odstranit nedůvěru, obavy a neznalost laické veřejnosti v oboru biometrie.

1 BIOMETRIE

Slovo **biometrie** vzniklo spojením dvou řeckých slov **bio** a **metric**, kde prvně jmenované znamená život a druhé měření. Biometrie měří určité charakteristiky člověka na základě jeho unikátních měřitelných fyziologických nebo behaviorálních vlastností.

1.1 Biometrické parametry

1.1.1 Biometrická systematika

Biometrická systematika je metoda klasifikace biometrie. Klasifikací biometrie existuje celá řada. Například podle klasifikace, kterou používá San Jose State University se biometrie dělí podle úlohy biometrie v dané biometrické aplikaci. Podle uvedené metodiky můžeme rozdělit aplikace na:

- vyžadující / nevyžadující spolupráci uživatele
- viditelný / skrytý biometrický systém
- obvyklá / nezvyklá
- řízená / neřízená uživatelem
- se standardním / nestandardním uživatelským rozhraním

1.1.2 Biometrický systém

Jedná se o automatizovaný systém, který umožňuje nasnímat biometrický vzorek uživatele, což jsou data reprezentující biometrickou vlastnost uživatele, jak byla nasnímána biometrickým systémem. Získaná data systém zpracuje a porovná s jednou nebo více referenčními šablonami v systému. Na základě porovnání následně rozhodne nakolik se shodují a indikuje, jestli byla nebo nebyla totožnost uživatele identifikována nebo ověřena.

1.1.3 Fyziologické a behaviorální vlastnosti

Mezi fyziologické vlastnosti každého z nás patří například otisk prstu nebo geometrie ruky, příkladem behaviorálních charakteristik, tedy charakteristik týkajících se chování, mohou být dynamika podpisu či dynamika stisku kláves na klávesnici.

Tab. 1.: Přehled základních biometrických metod

PŘEHLED ZÁKLADNÍCH BIOMETRIK			
Typ	Biometrika	Přesnost	Cena
Fyziologické	Otisk prstu	* * *	*
	Geometrie ruky	* *	* *
	Rozpoznání obličeje	* *	* *
	Oční duhovka	* * *	* * *
	Oční sítnice	* * *	* * *
	Lůžko nehtu	* * *	* *
	DNA	* * *	* * *
PŘEHLED ZÁKLADNÍCH BIOMETRIK			
Typ	Biometrika	Přesnost	Cena
Behaviorální	Ověřování hlasu	*	*
	Dynamika podpisu	*	*
	Dynamika stisku kláves	* *	*

* - nízká hodnota přesnosti biometrické metody / nízká cena

** - střední hodnota přesnosti biometrické metody / střední cena

*** - vysoká hodnota přesnosti biometrické metody / vysoká cena

1.1.4 Identifikace a verifikace

Biometrické systémy pracují ve dvou režimech: **verifikačním** a **identifikačním.**

Mnoho lidí se mylně domnívá, že oba režimy jsou totožné.

Při **verifikaci** (ověřování identity) uživatel předkládá svoji totožnost, kterou následně potvrzuje znalostí nějakého sdíleného tajemství. Skutečná biometrická verifikace probíhá tak, že uživatel předloží svou identitu (login - neboli uživatelské jméno, jímž se obvykle uživatel odlišuje od uživatelů ostatních, uživatelské jméno je obvykle veřejně známé; identifikační kartu) a následně mu čtecí zařízení nasnímá danou biometriku. Proces verifikace nazýváme rovněž porovnáním „ 1 : 1 „ (ang. v. one-to-one), protože dochází k porovnání jedněch vstupních dat s jedněmi daty z databáze.

Při **identifikaci** je uživatel rozpoznán systémem automaticky, tj. bez předchozího předkládání totožnosti, a jedná se tedy jak o časově, tak výpočetně náročnější proces než v případě verifikace. Proces identifikace nazýváme rovněž porovnáním „ 1 : N „ (ang. v. one-to-many).

Rozdělení autentizačních přístupů je založeno na tom :

- co člověk zná (přístupové heslo)
- co člověk vlastní (identifikační karta)
- čím je člověk tvořen (obrazec papilárních linií)

Hovoříme tedy, že je použita:

- autentizace heslem (autentizace založená na znalosti hesla)
- autentizace předmětem (autentizace založená na vlastnictví předmětu)
- biometrická autentizace (autentizace založená na biometrických charakteristikách člověka)

1.1.5 Autentizace heslem

Autentizace heslem je metoda založená na znalosti hesla, které je utajené a je známo pouze konkrétnímu uživateli.

Výhodou tohoto přístupu je jednoduchá technologická programová realizace a s tím související nízká pořizovací cena.

Nevýhodou je relativně jednoduchá možnost prolomení hesla, proto se používá k přístupu v prostředí s minimálními bezpečnostními požadavky.

Autentizační systémy založené výhradně na hesle musí mít dostatečně zabezpečený mechanismus pro generaci, distribuci a užití hesel.

Kvalitní heslo je charakterizováno těmito parametry:

- je distribuováno zabezpečeným způsobem
- obsahuje malá i velká písmena, číslice a další znaky dostupné na klávesnici
- má dostatečnou délku – alespoň 6 znaků
- nelze jej odvodit ze znalosti osoby vlastníka
- je často obměňováno – alespoň každé dva měsíce
- není nikde poznamenáno

1.1.6 Autentizace předmětem

Základem uvedené autentizace je vlastnictví identifikačního předmětu. Jako obecné označení autentizačního předmětu, který potvrzuje identitu vlastníka se používá termín **token.** Ten musí splňovat požadavky jedinečnosti (unikátnosti) a těžké padělatelnosti.

Z bezpečnostního hlediska spočívá síla autentizace založené na vlastnictví předmětu v tom, že předmět obsahující informaci, která ověřuje identitu uživatele, je přenosný; autentizační informace je pak vlastnictvím uživatele.

Tato metoda představuje vyšší úroveň zabezpečení, nevýhodou je možnost odcizení nebo ztráty autentizačního předmětu. Tato hrozba může být zmírněna tím, že autentizační systém požaduje nejen token, ale i heslo. Jedná se pak o kombinaci dvou autentizačních metod – autentizace heslem a předmětem.

Jako autentizační předměty se používají :

- **tokeny pouze s pamětí** (magnetické, elektronické nebo optické karty) – jsou obdobou mechanických klíčů; paměť obsahuje jednoznačný identifikační řetězec
- **tokeny udržující hesla** – vydají určený kvalitní klíč po zadání jednoduchého uživatelského hesla
- **tokeny s logikou –** umějí zpracovávat jednoduché podněty; např.: vydej následující klíč, vydej cyklickou sekvenci klíčů
- **inteligentní tokeny** (smart cards) – mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu, mohou šifrovat, generovat náhodná čísla, apod.

1.1.7 Biometrická autentizace

Podstatou biometrické autentizace je skutečnost jedinečnosti biometrických charakteristik jednotlivých osob. Biometrická autentizace je metoda, která dokazuje autentičnost (hodnověrnost) dané osoby. Biometrických charakteristik je celá řada a bývají nejčastěji rozdělovány do dvou skupin, a to na fyziologické a behaviorální. Největší výhodou této metody autentizace je bezesporu, nepřenositelnost znaků, jejich nezaměnitelnost a rovněž nulové náklady na jejich pořízení.

Souhrnně hesla, autentizační tokeny i biometriky mohou být podrobeny různým útokům. Heslo může být prolomeno, token může být ukraden a biometrika může být sofistikovaně napodobena. Uvedené hrozby mohou být výrazně zmenšeny použitím jednotlivých autentizačních metod ve vzájemné kombinaci.

Podle počtu použitých metod k autentizaci se rozlišuje:

1) jednofaktorová autentizace – použití jedné metody
2) dvoufaktorová autentizace - kombinace dvou metod
3) třífaktorová autentizace – kombinace tří metod

1.1.8 Výhody biometrických identifikačních metod

1) Univerzálnost (ang. v. *UNIVERSALITY)* – každý uživatel je jejich nositelem

2) Jedinečnost (ang. v. *UNIQUENESS*) – neexistují dvě osoby se stejnými biometrickými charakteristikami

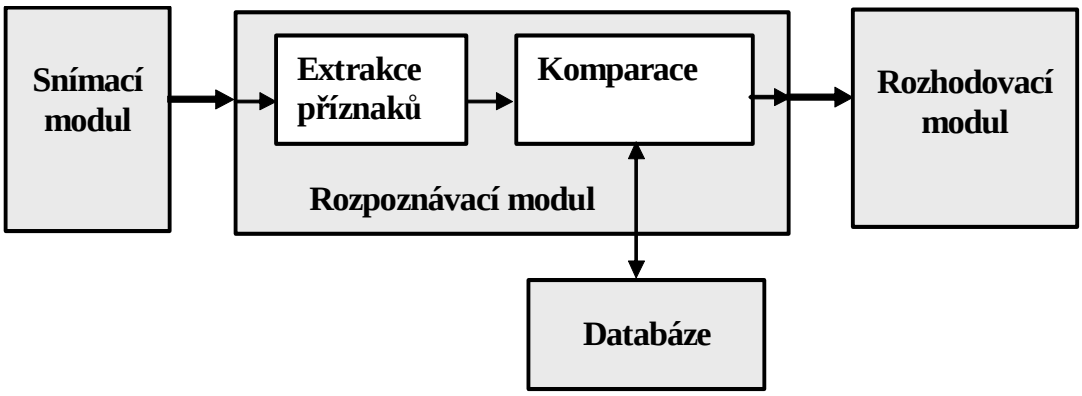
3) Permanence (ang. v. *PERMANENCE*) – biometrická charakteristika je časově neměnná

4) Jednoduchost (ang.v. SIMPLICITY) – biometrické charakteristiky jsou kvantitativně měřitelné charakteristiky jsou jednoduché a přesné

5) Přijatelnost (ang. v. *ACCEPTABILITY*) – snímání biometrických charakteristik je nenáročné, uživatelsky přijatelné

1.1.9 Proces práce s biometrikami

Biometrické systémy se skládají z několika logických (funkčních) bloků. Princip biometrických systémů je možné popsat na základě následujícího blokového schématu.



Obr. 1.: Princip činnosti biometrického systému

Biometrický identifikační systém se skládá ze snímacího modulu, rozpoznávacího modulu, databáze a rozhodovacího modulu. Snímací modul slouží k získávání biometrických dat osoby. Rozpoznávací modul se skládá z modulu pro extrakci příznaků a porovnávacího modulu. Pro identifikaci osoby se nepoužívají všechny snímané informace, ale jen některé jejich významné části (tzv. příznaky). S extrahovanými příznaky se uskutečňují různé matematické operace, na základě kterých se realizuje identifikace osoby. Použité extrakce příznaků souvisí s rychlostí celkové identifikace osoby. V porovnávacím modulu se na základě získaných příznaků uskutečňuje porovnávání s daty uloženými v databázi (uživatelů).

Závěrečné rozhodnutí, zda-li snímané údaje korespondují (jsou shodné) s daty uloženými v databázi, se vykonává v rozhodovacím modulu.

Pro každodenní použití biometrického systému v praxi, je třeba nejprve provést několik základních kroků.

1.1.10 Fáze registrace

V průběhu registrační etapy se uživatelé registrují do biometrického systému poskytováním dat reprezentativních biometrických vzorků nazývaných **šablony** neboli **etalony**. Dochází k několikerému snímání daného biometrického vzorku a k vytvoření šablony se pak použije pouze ten nejlepší z nich. V šabloně není uložen biometrický vzorek jako takový, ale pouze odpovídající matematický kód, který z nasnímaného vzorku vznikne extrakcí jeho unikátních znaků. Následně je šabloně 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. Etalon se špatnou kvalitou může být následně příčinou problémů.

1.1.11 Uložení etalonů

Získanou šablonu je následně zapotřebí někde vhodně uchovávat. Možná řešení jsou následující:

Uložení etalonu v biometrickém čtecím zařízení

Uložení etalonu v biometrickém čtecím zařízení má své výhody i nevýhody v závislosti na konkrétní realizaci. Výhodou je rychlá reakce, tedy krátká doba odezvy čtecího zařízení a nezávislost na externích procesech nebo datovém spojení při zpřístupnění etalonu. Nevýhodou je, že etalony jsou svým způsobem zranitelné a jsou závislé na přítomnosti a funkčnosti daného čtecího zařízení. V případě poruchy nebo poškození zařízení je pak nezbytná nová instalace databáze etalonů, případně opětovná etapa zápisu.

Uložení etalonu ve vzdálené centrální databázi

Uložení etalonu ve vzdálené centrální databázi, je nejpřirozenější možnost, díky použití současných moderních technologií a systémů. Nelze však opomenout možnost výpadku sítě a tím vyřazení biometrického systému z činnosti. Pro tyto případy je nutné zabezpečit

systém alternativním řešením, kterým může být prostá autentizace heslem nebo předmětem.

Uložení etalonu v přenosných zařízeních (tokeny, čipové karty)

Uložení etalonu v tokenu, nese s sebou dvě výhody:

- nevyžaduje žádné lokální nebo centrální ukládání etalonů
- uživatel si nosí svůj etalon s sebou a může jej použít všude tam, kde má povolen autorizovaný přístup

Nevýhodou je vyšší cena a složitost biometrického systému z důvodu kombinace tokenového a biometrického čtecího zařízení na všech verifikačních místech.

Libovolná kombinace předcházejících způsobů

Kombinace předcházejících řešení, může poměrně efektivně eliminovat nevýhody jednotlivých samostatných možností.

1.1.12 Fáze verifikace / identifikace

Po vytvoření databáze šablon během registrace lze přistoupit k vlastní verifikaci nebo identifikaci uživatele. Z biometrického vzorku získaného pomocí čtecího zařízení se opět vytvoří odpovídající šablona a ta je následně porovnávána s dříve uloženým etalonem.

Identifikátor slouží k vyvolání vzorku v etapě verifikace. Etapa zápisu a kvalita výsledného reprezentativního vzorku jsou kritické faktory ovlivňující úspěšnost biometrického systému.

Etalon špatné kvality je pak velmi častou příčinou nesprávného rozpoznání identifikované osoby.

Základní úlohou biometrických systémů, na rozdíl od jiných autentizačních metod, není poskytnutí odpovědi typu ano/ne, ale informace s jakou pravděpodobností osobu identifikoval. U biometrických systémů prakticky nikdy nenastane stoprocentní shoda

mezi uloženou referenční šablonou a šablonou právě získanou, takže je systému povolena jistá odchylka neboli variabilita. Variabilita udává, při níž jsou porovnávané šablony ještě považovány za shodné. Takto nastavenou variabilitu nazýváme bezpečnostní prahovou hodnotou.V případě, že není tato prahová hodnota nastavena optimálně, systém vykazuje dva základní typy chyb – chybné přijetí, neboli akceptace a chybné odmítnutí.

1.1.13 Negativní a pozitivní identifikace

U identifikace se rozlišují dvě její varianty – **pozitivní** a **negativní identifikace.**

Při pozitivní identifikaci systému uživatel dokazuje, že někým je. Naopak při negativní identifikaci se snaží prokázat, že někým není.

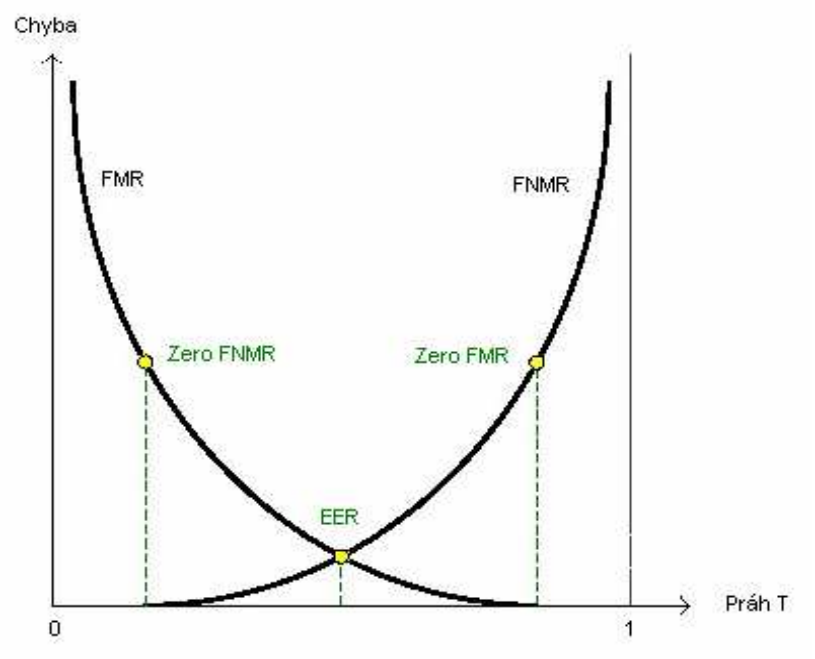
Chybné přijetí a chybné odmítnutí

Ve fázi registrace, byla získána referenční šablona jako nejreprezentativnější z několika vzorků. Při následné identifikaci pak nezískáme úplnou shodu. Z tohoto důvodu může dojít ke dvěma chybám – **chybnému přijetí** a **chybnému odmítnutí**. Při chybném přijetí je osoba nesprávně identifikována jako oprávněný uživatel, při chybném odmítnutí naopak není autorizovaný uživatel rozpoznán a je označen za neoprávněného uživatele.

Výskyt těchto dvou chyb je úzce spjat s vlastnostmi konkrétního biometrického systému a nastavenou úrovní zabezpečení.

Míry chybného přijetí a odmítnutí typu FAR, FRR a ERR

Hodnoty chybného přijetí a chybného odmítnutí se většinou neuvádějí v absolutních číslech, ale jejich relativních ekvivalentech. Jsou jimi **míra chybného přijetí (ang. v. False Asseptance Rate, dále jen FAR)** a **míra chybného odmítnutí (ang. v. False Rejection Rate, dále jen FRR)**. **FAR** a **FRR** vyjadřují pravděpodobnost výskytu dané chyby v procentech.



Obr. 2.: Graf závislosti EER, Zero FMR a Zero FNMR

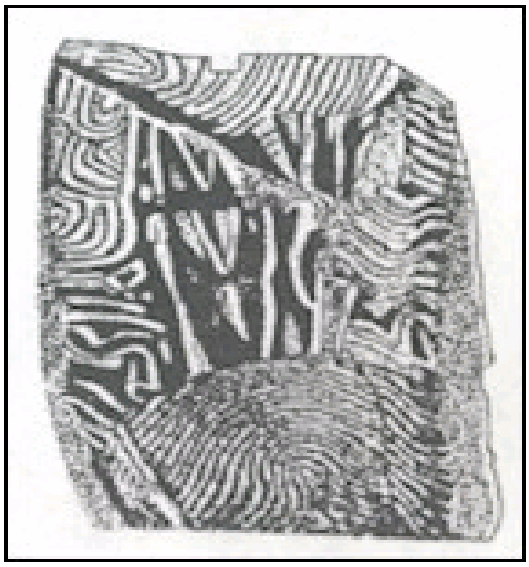
Z uvedeného vyplývá, že čím nižší je **FAR**, tím vyšší je **FRR**, a naopak. Obě míry jsou závislé na nastavené prahové hodnotě. Hodnota, při které se **FAR** a **FRR** rovnají, se označuje jako **míra rovné chyby (ang. v. Equal Error Rate, dále jen EER)**. Podle **EER** lze určit bezpečnost biometrického systému, nicméně **FAR** a **FRR** mají daleko vyšší vypovídací hodnotu.

2 BIOMETRICKÉ PŘÍSTUPY

2.1 Historie daktyloskopie

Technologie otisku prstu má mnohaletou bohatou historii. Jedny z nejstarších vyobrazení otisků prstů sahají do doby několika set let před naším letopočtem.

Ze všech dnes používaných biometrických technologií je nejznámější a také nejstarší metodou otisk prstu. Znalost o existenci papilárních linií na lidské kůži se objevuje u celé řady civilizací. Na území dnešního státu Indiana byly nalezeny kameny s rytými obrazy, tzv. " petroglyfy ", znázorňující lidskou ruku s vyznačenými papilárními liniemi. Vytvořily je indiánské kmeny obývající tato území v období několika tisíc let před naším letopočtem.



Obr. 3.: Kámen s naznačenými papilárními liniemi

Také u Asyřanů se našli pozůstatky otisků prstů. Ve zříceninách starověkého asyrského města Ninive byla objevena část slavné Aššurbanipalovy knihovny založené již v 9. století před naším letopočtem. Na nalezených úlomcích hliněných tabulek se kromě rozličných textů nacházely otisky prstů.

Pravděpodobně první písemně doložená zmínka o praktickém využití některé biometrické metody pochází od cestovatele jménem Joao de Barros, který popisuje užití určité obdoby dnes známého otisku prstu ve středověké Číně 14tého století.

Právě z tohoto období totiž pocházejí asyrské hliněné tabulky, na jejichž úlomcích se nacházejí jména lidí spolu s otisky jejich prstů.

V roce 1880 publikoval Angličan Henry Faulds článek zabývající se snímáním otisku prstu pomocí inkoustu. Faulds je zároveň považován za prvního člověka, kterému se podařilo získat otisk prstu z předmětu.

Základy moderní daktyloskopie publikoval v roce 1888 anglický přírodovědec Francis Galton.

Moderní historie biometrie se datuje od roku 1882, kdy antropolog a šéf oddělení identifikace pachatelů pařížské policie Alphonse Bertillion hledal nějaký způsob, který by mu umožnil identifikovat již jednou odsouzené zločince. Především jeho zásluhou se biometrie stala reálným předmětem studia. Metoda, která se stala prostředkem k záznamu různých lidských rozměrů a jejich následnému použití k identifikaci nebo verifikaci je známá pod názvem „ Bertillionáž “, který je shodný s pojmem antropometrie.

V rámci antropometrie bylo prokázáno, že:

- po 20. roce života zůstávají tělesné rozměry neměnné
- s vyšším počtem korektně změřených rozměrů těla klesá riziko záměny osob
- měřením a registrováním tělesných rozměrů je možné osobu jednoznačně identifikovat, případně verifikovat

Obr. 4.: Měření tělesných rozměrů (antropometrie) a karta pro jejich záznam

Pro měření bylo použito 11 tělesných rozměrů:

1) tělesná výška
2) délka natažené paže
3) výška v sedu
4) délka hlavy
5) šířka hlavy
6) délka pravého ucha
7) šířka pravého ucha
8) délka levé nohy
9) délka levého prostředníčku
10) délka levého malíčku
11) délka levého předloktí

V květnu roku 1988 publikoval svoji práci anglický přírodovědec Francis Galton (1822-1911). Položil v ní teoreticko - vědecké základy daktyloskopie, vědy zabývající se otisky prstů. Matematickými metodami vypočítal, že existuje celkem 64 miliardy různých variant uspořádání papilárních linií. Galton prakticky vyloučil možnost výskytu dvou jedinců se stejným otiskem prstu. První praktické základy daktyloskopické identifikace položil sir William James Herschel (1833-1917).

2.2 Metody identifikace

2.2.1 Biometrie ruky

Lidská ruka každého z nás poskytuje hned několik unikátních a zároveň měřitelných vlastností. Nejznámější a v praxi nejrozšířenější z nich je bezesporu otisk prstu. Kromě toho je možné měřit také geometrii ruky, dynamiku podpisu, dynamiku psaní na klávesnici, vzor krevního řečiště, tvar lůžka nehtu či absorpční spektrum lidské kůže.

2.2.2 Identifikace podle otisku prstů

Klasifikace vzorů otisku prstu

Na bříšcích prstů rukou, nohou a na kůži dlaně se nachází drobné prolákliny a vyvýšeniny. Vznikají tak, že škára vybíhá proti pokožce v takzvaných **papilárách** – odtud také pochází používaný výraz **papilární linie.** Grafickou reprezentaci papilárních linií tvoří otisk prstu. Papilární linie se formují během embryonálního vývoje. Výška papilárních linií leží v rozmezí 0,1 – 0,4 mm a šířka papilárních linií v rozmezí 0,2 – 0,5 mm.

Jako první popsal jednotlivé typy charakteristických vzorů papilárních linií český přírodovědec **Jan Evangelista Purkyně** (1787 – 1869). Tyto papilární linie klasifikoval do devíti základních vzorů. Rovněž upozornil na trojúhelníkové seskupení papilárních linií (tzv. deltu) jako na důležitý klasifikační znak.

Z tohoto dělení těží také novodobá klasifikace, která rozeznává tři úplně základní vzory:

1) **Vzor typu: vír**

   Papilární linie vytvářejí kruhové, oválné nebo spirálovité obrazce s jádrem uprostřed. Vzor musí obsahovat alespoň dvě delty s alespoň jednou samostatně probíhající linií.

2) **Vzor typu: smyčka**

   Papilární linie vytvářejí smyčku. Mezi deltou a středem musí být alespoň jedna probíhající linie.

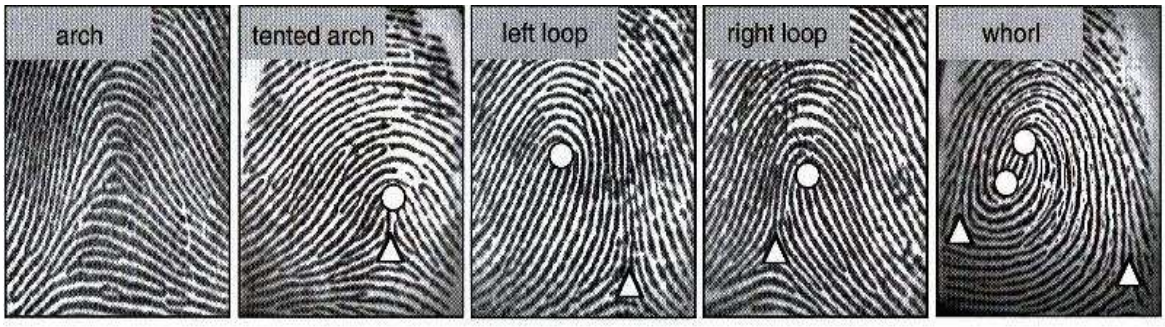
3) Vzor typu: oblouk

Papilární linie vytvářejí jednoduché oblouky. Vzor neobsahuje žádné tzv. delty, tj. útvary, v nichž se papilární linie rozbíhají do tří směrů.

Obr. 5.: Otisky prstů: a) válený; b) píchaný; c) latentní

Existují následující **třídy otisků prstů, a to :**

- **oblouk** (ang. v. Arch)
- **klenutý oblouk** (ang. v. Tended Arch)
- **spirála / závit** (ang. v. Whorl)
- **levá smyčka** (ang. v. Left Loop)
- **pravá smyčka** (ang. v. Right Loop)
- **dvojitá smyčka** (ang. v. Twin Loop)



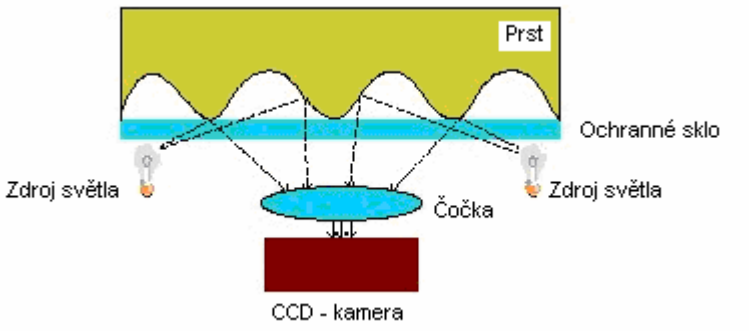
Obr. 6.: Třídy otisků prstů

Snímače otisků prstů

Optické snímače prstů

Jedná se o nejstarší a zároveň nejrozšířenější snímače otisků. Fungují na základě rozdílného rozptylu nebo odrazu světla v bodech, kde se stýkají papilární linie přiloženého prstu se snímací plochou. Prst přiložený na plochu snímače je nejprve osvícen. Světlo se odrazí od pokožky prstu a po postupném průchodu hranolem, optickým filtrem a čočkou dopadá na CCD detektor. Pomocí něho je obraz otisku digitalizován a následně zpracován algoritmem pro rozpoznání otisku prstu.

Optické snímače poskytují kvalitní obraz. Některé levnější snímače mohou mít problémy s latentními otisky prstů, tedy s otisky, které zůstanou na snímací ploše po identifikaci předchozího člověka. Latentní otisk může značně zkreslit nasnímaný obraz a tím znemožnit identifikaci. Optické snímače jsou také značně náchylné na nadměrnou vlhkost prstu. V takovém případě dochází k vzájemnému slití obrazu jednotlivých papilárních linií. Optické snímače dále mívají problémy s prsty ušpiněnými jakoukoliv tmavou barvou. Tmavý povrch totiž dopadající světlo pohltí, což se při zpracování nasnímané předlohy projeví bílým místem na obrazu.



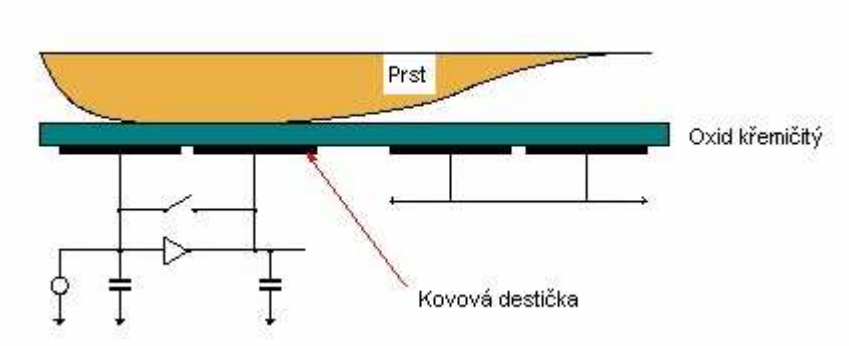
Obr. 7.: Princip optického snímání otisku prstu

Kapacitní snímače

Tento typ snímačů (též nazývaných **silikonové**) měří kapacitní odpor v ploše dotyku. Silikonový plátek snímacího zařízení funguje jako jedna deska kondenzátoru a přiložený prst jako druhá. Vyvýšené linie povrchu prstu jsou více přilehlé než prostory mezi nimi, a mají tak vyšší kapacitní odpor. Měřením napětí na kondenzátoru lze určit místa (pixely), na kterých se prst dotýká snímače těsněji než na jiných, a podle získaných hodnot následně sestavit obraz otisku.

Velkou výhodu kapacitních snímačů představuje nejen jejich poměrně nízká cena, ale především malá velikost.

Také kapacitní snímače ovšem mají problém s příliš suchými nebo naopak vlhkými prsty. Vlhkost na prstu totiž výrazně ovlivňuje kapacitní odpor.



Obr. 8.: Princip kapacitního snímače otisku prstu

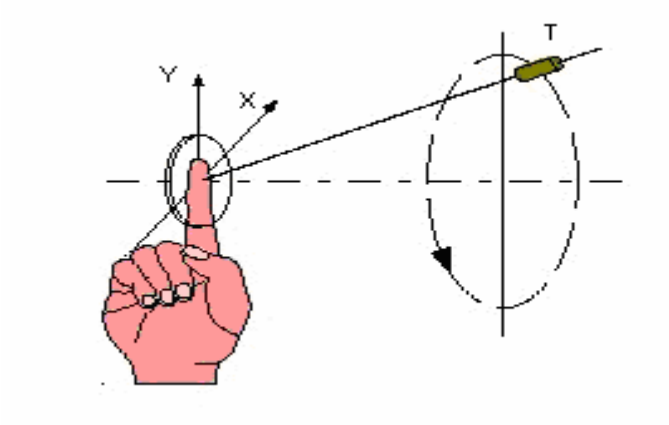
Ultrazvukové snímače

Ultrazvukové snímače nejsou tolik rozšířené jako snímače předešlé. Jedná se o poměrně novou metodu snímání otisků prstů.

Princip této technologie je založen na rotujícím ultrazvukovém vysílači, v němž je zabudován i přijímač. Tento rotuje po kruhové dráze a snímá otisk prstu a následným měřením odporu kůže je získán vzor papilárních linií na snímaném prstu.

Ultrazvukové vlny proniknou i pod povrch kůže, tzn. že tato technologie může lehce odhalit falešné prsty.

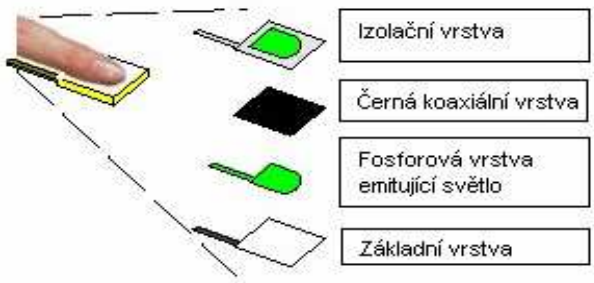
Ultrazvukové snímače mají větší rozměry. Tato nevýhoda je však vyvážena odolností vůči potu a nečistotám zachyceným na prstu.



Obr. 9.: Princip ultrazvukové technologie snímání otisku prstu

Elektrooptická technologie

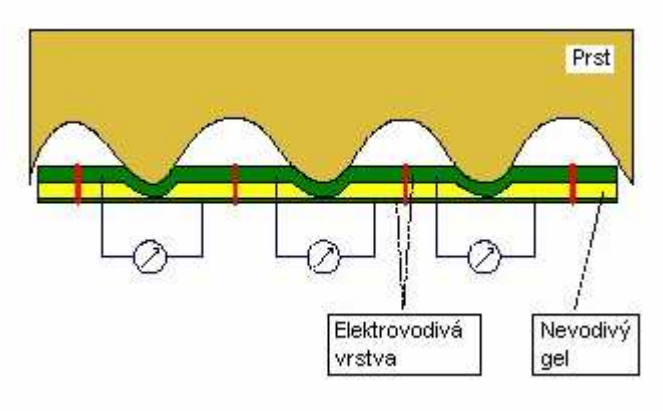
Elektrooptická technologie zahrnuje v podstatě senzor, který je složen ze čtyř vrstev, přičemž přítlakem prstu vybudí styk černé koaxiální vrstvy emitování světla ve fosforové vrstvě. Toto záření projde základní vrstvou do senzoru.



Obr. 10.: Princip elektrooptické technologie snímání otisku prstu

Tlaková snímače

V technologii tlakových snímačeů je senzor složen ze tří vrstev, přičemž mezi elektrovodivé vrstvy je vložen nevodivý gel. Přiložením prstu na plochu senzoru dojde ke stisku nevodivého gelu tak, že se elektrovodivé vrstvy dotknou.

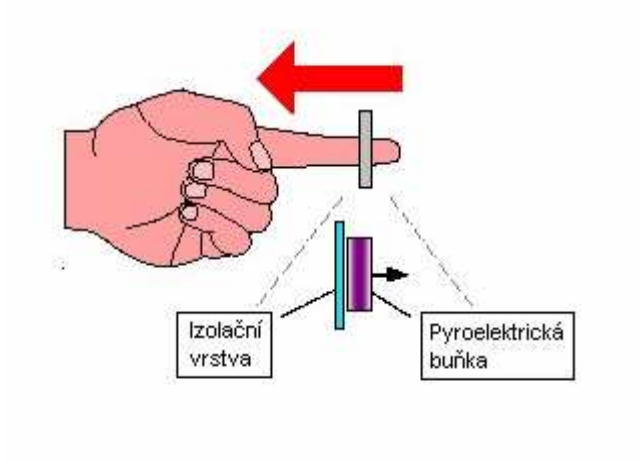


Obr. 11.: Princip tlakové technologie snímání otisku prstu

Termická technologie

Princip je založen na tepelném záření – papilární linie mají vyšší vyzařování tepla jak prohlubně mezi nimi. Prst je protažen přes pyroelektrickou buňku, která snímá tepelné vyzařování. Pro získání obrazu otisku prstu je nutné přejíždět prstem přes citlivou plochu snímače. Na výstupu snímače je získán obraz otisků ve formě digitálních pásů, které se softwarově skládají do výsledného obrazu otisku prstu.

Značnou nevýhodou snímače je, že otisk je získán pouze pohybem prstu přes citlivou vrstvu čipu. Při pohybu se velmi obtížně určuje počáteční poloha, takže výsledkem je, že při několika pokusech jsou získány obrazy otisků různých částí prstu.



Obr. 12.: Princip termické technologie
snímání otisku prstu

2.2.3 Geometrie ruky

Každý člověk má jinak tvarovanou ruku a tento tvar se u dospělého člověka během života nemění. Toho využívají biometrické systémy založené na snímání geometrie ruky.

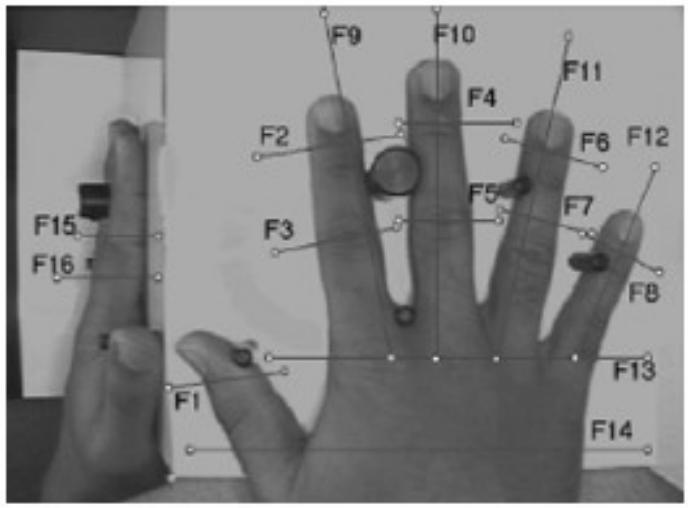
Obr. 13.: Systém pro rozpoznávání geometrie ruky HandKey II

Proces snímání:

Podobně jako u jiných typů biometrik i zde se nejprve musí pořídit celkový obraz ruky. K tomuto účelu bývají nejčastěji využívány optické snímače, které vytvoří černobílý

3-dimensionální snímek obsahující **siluetu ruky**. Při snímání se ruka položí na danou plochu. Distanční sloupky určují přesnou plochu, aby ruka byla správně nasnímána. Přístroj ruku nasnímá z vrchní a z boční strany. Vrchní pohled slouží ke zjištění šířek a délek ruky, boční pohled slouží k určení tloušťky ruky. Dva pohledy ruky jsou nasnímány pomocí digitální kamery, umístěné mezi zrcadly, která jsou v úhlu 45 stupňů.

Výsledné šablony obsahují informace o měřitelných prvcích ruky, kterými jsou: délka a šířka prstů, poměr plochy dlaně a prstů, šířka a tloušťka dlaně a dále sem řadíme různá zakřivení a lokální anomálie ruky.



Obr. 14.: Příklad snímků geometrie ruky,

včetně charakteristik

Tab. 2.: Tabulka s charakteristikami

CHARAKTERISTIKY PŘI SNÍMÁNÍ OTISKU RUKY			
Rys	Popis	Rys	Popis
F1	šířka palce ve druhém článku	F9	délka ukazováčku
F2	šířka ukazováčku ve třetím článku	F10	délka prostředníčku
F3	šířka ukazováčku ve druhém článku	F11	délka prsteníčku
F4	šířka prostředníčku ve třetím článku	F12	délka malíčku
F5	šířka prostředníčku ve druhém článku	F13	šířka dlaně u prstů
F6	šířka prsteníčku ve třetím článku	F14	šířka dlaně u palce
F7	šířka prsteníčku ve druhém článku	F15	tloušťka ruky u druhého článku
F8	šířka malíčku ve třetím článku	F16	tloušťka ruky u třetího článku

Popisovaná biometrická technologie se nevyznačuje nijak vysokou přesností, a proto bývá používána především při verifikaci, nikoliv identifikaci. Oproti snímání otisků prstů má tu výhodu, že ignoruje některé časem se měnící detaily, jako pot, špínu či drobná poranění. K dalším výhodám patří: uživatelská přívětivost, snadné použití a rovněž velikost šablony. (např.: systémy RSI používají velikost šablony 9 byte, což je extrémně málo, ve srovnání např. s otiskem prstu, který vyžaduje 250-1000 bytů, nebo s rozpoznáním řeči, které vyžaduje 1500 – 3000 bytů).

2.2.4 Dynamika podpisu

Uvedená biometrická technika má původ v konvenčním pojetí podpisu. Rozdíl je však v tom, že namísto vizuální podoby se vzorem dochází k porovnávání vlastního průběhu psaní. Není tedy důležitá podoba podpisu či tvar písmen, i když o to jde samozřejmě také, ale důraz je kladen na dynamiku podpisu, provedení jednotlivých tahů, sílu, kterou tlačíme

při psaní na podložku, rychlost psaní apod. Technologie rozpoznávání je založena na porovnávání změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na a nad papírem.

Pro nasnímání podpisu mohou sloužit dotekové displeje, tablety i jiná specializovaná zařízení.

Obr. 15.: Technika pro snímání podpisu

Hlavním problémem je odlišení konstantních částí podpisu a částí, které se liší při každém psaní. Tvar a dynamika psaní podpisu se navíc v průběhu času u většiny lidí výrazně mění. To klade vysoké nároky na inteligentní rozpoznávání, tedy vysoké nároky na kvalitní software.

Dynamika podpisu patří mezi behaviorální charakteristiky.

2.2.5 Dynamika stisku kláves

Dalším zástupcem behaviorálních charakteristik je dynamika stisku kláves. Je to proces analýzy způsobu psaní uživatele na klávesnici. Nezabývá se tím, co píšeme, ale tím, jak píšeme.

Dynamika stisku kláves zahrnuje měření několika různých charakteristických vlastností, kterými jsou:

- doba mezi stiskem jednotlivých kláves
- doba trvání stisku klávesy
- celková rychlost psaní
- počet chyb
- zvyk používat dodatečné klávesy, jako např. čísla na numerické klávesnici
- pořadí v kterém uživatel uvolní klávesy při psaní velkých písmen pomocí klávesy Shift
- síla, s jakou je proveden stisk klávesy

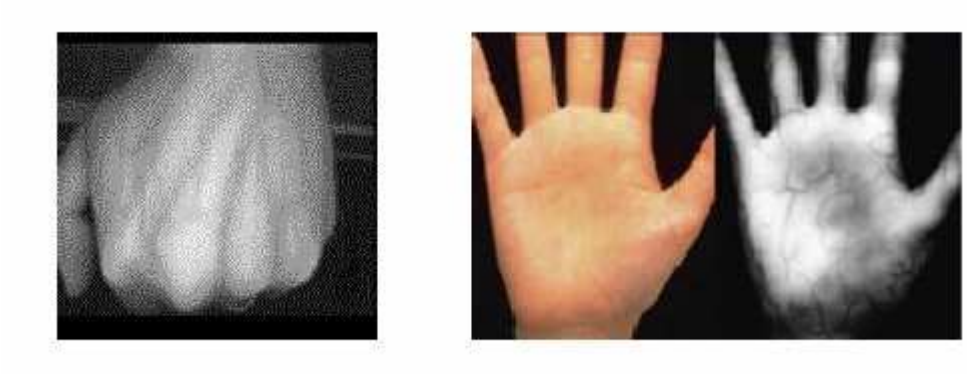
Tato technologie však kvůli své nižší přesnosti není vhodná pro identifikaci, a proto se používá především k verifikaci.

Největší výhodou, kterou s sebou technika dynamiky stisku kláves přináší, je její hardwarová nenáročnost.

Popisované měřitelné charakteristiky ruky patří mezi ty nejznámější a nejrozšířenější. Kromě nich ale lidská ruka poskytuje také řadu dalších vlastností, které se dají zkoumat – tvar krevního řečiště ruky, lůžko nehtu nebo absorpční spektrum lidské kůže.

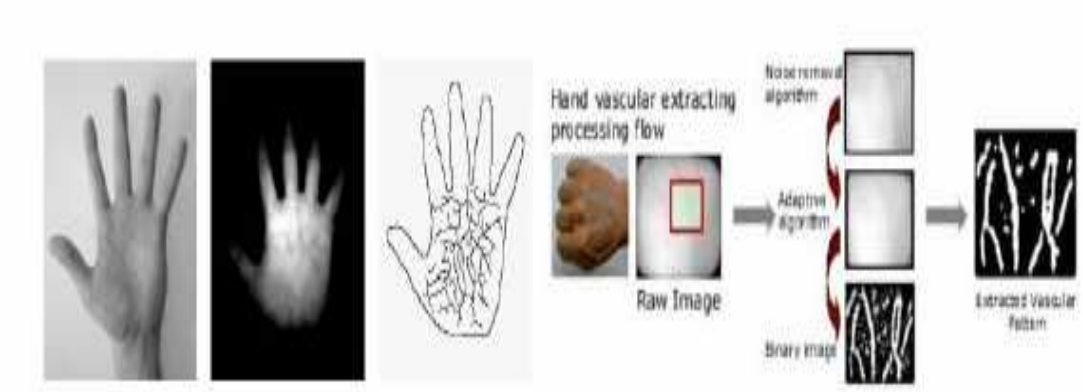
2.2.6 Tvar krevního řečiště ruky

Jedná se o velmi málo známou a rozšířenou biometrickou metodu. Pro snímání krevního řečiště ruky není zapotřebí nákladný hardware. Tvar krevního řečiště se měří buď na dlani, nebo na hřbetu ruky.



Obr. 16.: a) Žíly hřbetu ruky (vlevo); b) Žíly dlaně ruky (vpravo)

Při snímání uživatel vloží ruku do čtecího zařízení. V něm umístěný zdroj infračerveného záření pořídí obraz snímané ruky. Pomocí infračerveného záření je vytvořen snímek s barevnou hloubkou 256 odstínů šedi. Použitím zobrazení ve spektru blízkému infračervenému světlu (dále jen IR záření) se zvýrazní kontrast mezi cévním řečištěm hřbetu ruky a okolní kůží. Žíly dané záření pohlcují a vytvářejí zřetelnou síť tmavých čar, které reprezentují tvar krevního řečiště. Hloubka absorpce IR záření živou tkání je přibližně 3mm, tzn. že termální IR záření proniká do hřbetu ruky jen povrchově a v nasnímaném obrazu je pak nejvíce rozeznatelné právě celé cévní řečiště. Po nasnímání potřebného obrazu hřbetu ruky nastupuje další fáze rozpoznání žil ruky, která se může skládat ze čtyř kroků. Prvním krokem je segmentace obrazu (ang. v. hand region segmentation). Účelem tohoto primárního kroku je rozdělit nasnímaný obraz na požadované části a pozadí obrazu. Následně se provádí vyhlazení a redukce šumu (ang. v. difussion smoothing). Pro redukci šumu a vyhlazení obrazu se používá např. filtr Gaussovské rozmazání (nezachovává hrany) nebo nelineární rozptýlení (zachovává hrany). Tento krok slouží k vyhlazení obrazu cévního řečiště a k potlačení případného vlivu tvaru hřbetu ruky. Následné prahování (ang. v. local tresholding) má za úkol oddělit vzor žilní struktury od zbytku obrazu. Posledním krokem zpracování je postprocessing, kde se již po finálních úpravách na obrázku vyskytuje pouze struktura žil hřbetu ruky ve tvaru, který nazýváme šablonou.



Obr. 17.: a) Postup verifikace na základě žil ruky, b) Detaily

Obr. 18.: Technologie žil dlaně ruky

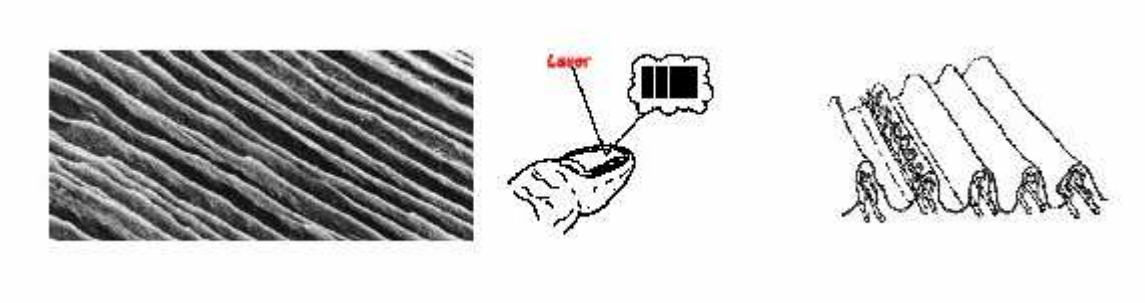
2.2.7 Tvar lůžka nehtu

Podíváme-li se zblízka na svůj nehet, zjistíme, že jeho povrch zdaleka není rovný. Při svém růstu totiž nehet kopíruje tvar lůžka nehtu, které se nachází pod ním, a tím získává svůj vlnitý tvar. Nejen že dva vybraní jedinci mají odlišný tvar lůžka nehtu vybraného prstu, ale dokonce každý prst má lůžko jinak tvarované.

Mezi nehtem a lůžkem se nachází přírodní polymer keratin. Tento přírodní polymer mění orientaci dopadajícího polarizovaného světla. Při osvícení pod správným úhlem tak lze

analyzovat fázové změny paprsku po odrazu a jako výsledek získat jednorozměrnou strukturu lůžka nehtu, číselnou sekvenci, která připomíná sekvenci čárového kódu.

Nevýhodou je nízká odolnost proti podvrhům a nefunkčnost v případě kosmetické úpravy nehtu.



Obr. 19.: a) „Čárový kód“ nehtu (vlevo) b) Podkožní struktura nehtu (vpravo)

2.2.8 Absorpční spektrum lidské kůže

Jednotlivé vrstvy kůže mají různou tloušťku, rozhraní mezi nimi se odlišně vlní a například také tvar a hustota buněk uvnitř těchto vrstev je nestejná. Čtecí zařízení ozařuje kůži zářením o různých vlnových délkách a poté analyzuje jejich odraz.

2.2.9 Biometrie hlavy

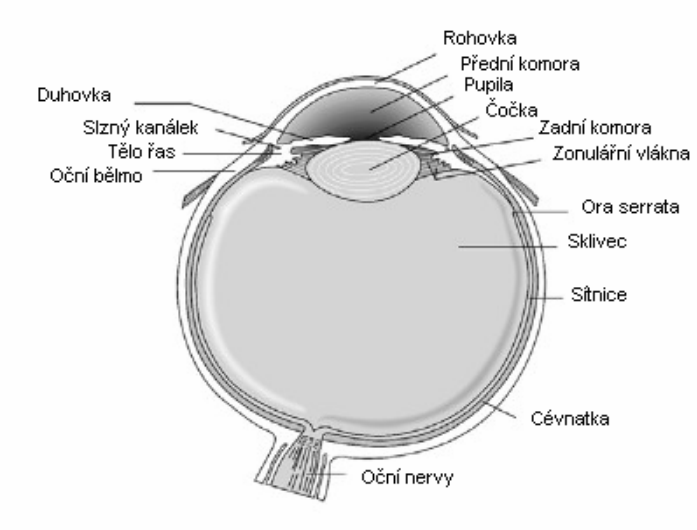
Snímání oční duhovky nebo sítnice patří k nejpřesnějším biometrikám vůbec.

2.2.10 Oční duhovka

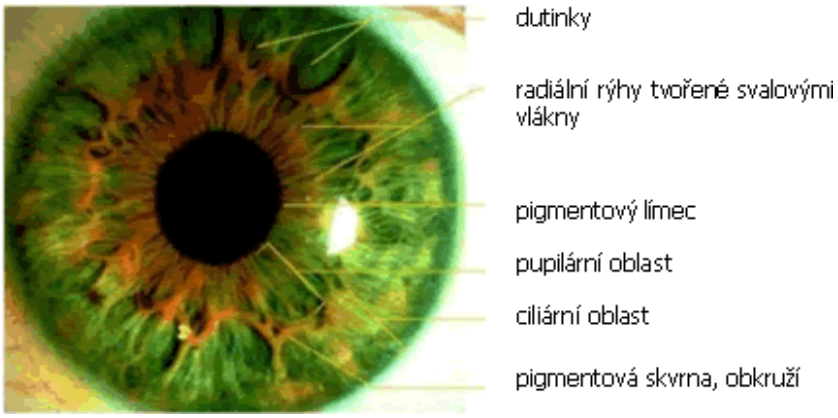
Oční duhovka každého člověka je co do podobnosti unikátní. Jde o pigmentovanou membránu obklopující zřítelnici oka. Duhovka kontroluje úroveň světla, které vstupuje do oka. Černý otvor ve středu duhovky se nazývá pupila (panenka). Duhovka je spojena s jemnými svaly, které duhovku buď rozšiřují nebo zužují. Je plochá a rozděluje oko na přední a zadní část. Barva duhovky je způsobena barvivem, které se nazývá melanin. Vizuální textura se formuje během prvních dvou let života a základní struktura zůstává

během života neměnná a pro každou osobu jedinečná. Dokonce i duhovka u dvojčat je odlišná.

Identifikace osob na základě měření unikátních vlastností duhovky se považuje za jednu z nejpřesnějších biometrických technik.



Obr. 20.: Složení lidského oka

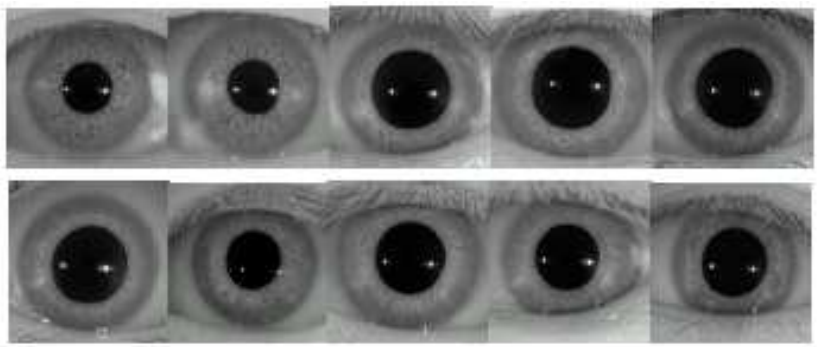


Obr. 21.: Struktura duhovky – rysy

Každá duhovka má unikátní strukturu danou stavbou tkání, jimiž je tvořena. Jsou to především svalová vlákna, pigment a vazivo.

Při detailním zkoumání lidského oka můžete zjistit, že duhovka má několik jasně viditelných vnějších charakteristik – mezi ně patří například **záhyby, skvrny, rýhy, krypty** apod. Identifikace biometrickými systémy je založena na digitalizaci těchto rysů a jejich následném srovnání s registračními vzorky uloženými v databázi.

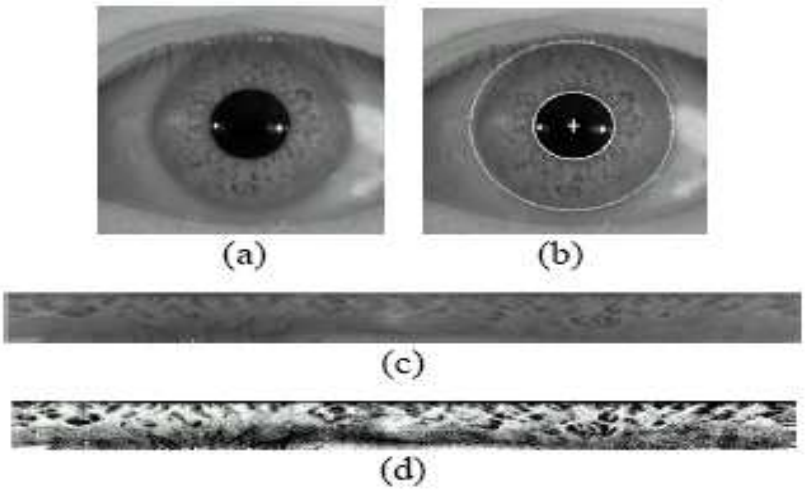
- **Krypty** - jedná se o velmi tmavá místa, kde je duhovka poměrně tenká. Zpravidla se nalézají poblíž rozhraní mezi řasnatou a zornicovou oblastí.
- **Radiální rýhy** – začínají poblíž zornice a paprskovitě vybíhají směrem k okraji duhovky.
- **Pigmentové skvrny –** náhodné shluky pigmentových buněk u povrchu duhovky. Vyskytují se v řasnaté oblasti.
- **Pigmentové záhyby** – vznikají jako důsledek vystupující spodní vrstvy duhovky v blízkosti zornice.



Obr. 22.: Příklad deseti rozdílných obrazů duhovek

Jako snímací zařízení se využívají běžné CCD kamery, přičemž není vyžadován blízký kontakt mezi uživatelem a snímačem. Ve skutečnosti může být snímek oka pořízen až ze vzdálenosti jednoho metru. Duhovka může být zachycena a zpracována i u osob se zhoršeným zrakem, pokud nemají poškozenou samotnou duhovku. Dokonce ani brýle na očích a ani kontaktní čočky nejsou pro tuto technologii žádnou překážkou. Vzhledem k tomu, že tato technika nevyžaduje fyzický kontakt uživatele se snímačem, není pro něj nikterak obtěžující a je přijímána velmi kladně.

Obr. 23.: Snímání obrazu duhovky



Obr. 24.: Předzpracování obrazu: a) Původní obraz duhovky b) Obraz po lokalizaci duhovky c) Rozvinutá textura duhovky d) Textura po zvýraznění charakteristik

V současné době se systémy identifikující osobu podle vlastností oční duhovky využívají například v některých věznicích, přístavech nebo letištích.

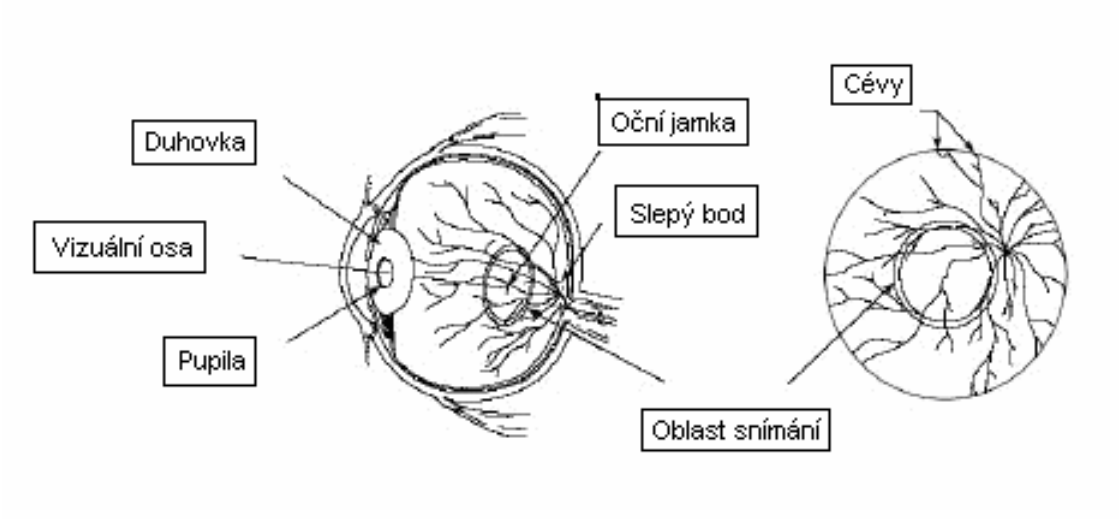
Mezi výhody této techniky identifikace patří vysoká přesnost, skutečnost, že uživatel nemusí mít při snímání žádný kontakt se snímacím zařízením a skutečnost, že duhovka je prvek unikátní a během života jedince neměnný.

Nevýhodou jsou pak především vyšší pořizovací náklady, přetrvávající obavy uživatelů z poškození oka, nemožnost použití u osob s aniridií (porucha vývoje duhovky) a vážným fyzickým poškozením duhovky.

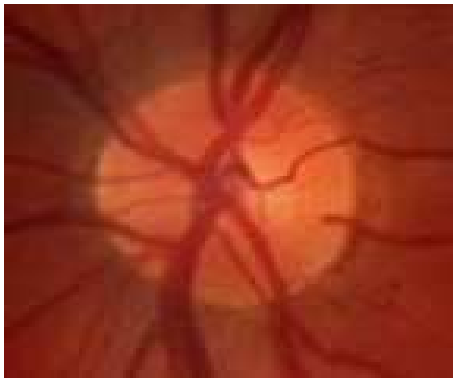
2.2.11 Oční sítnice

Jedná se o světlocitlivý povrch zadní strany oka. Je složen z nervových buněk tyčinek a čípků, které převádějí přicházející světelné paprsky na nervové signály. Tyčinky poskytují černobílé a čípky barevné vidění. Oční nerv, společně s artérií sítnice, vystupují z oka v místě, kde se nenacházejí žádné tyčinky ani čípky. Označujeme jej pojmem **slepá skvrna**.

Popisovaná biometrická technologie porovnává právě strukturu sítnice v okolí slepé skvrny. Snímání se provádí zaměřením infračerveného paprsku o nízké intenzitě skrz zornici na vzor cév nacházejících se na zadní straně oka. Sítnice je u této vlnové délky průhledná, zatímco cévy sítnice infračervené světlo reflektují.



Obr. 25.: Funkční princip sítnice oka



Obr.26.: Snímek oka po záběru infračervenou kamerou

Mezi výhody skenování oční sítnice patří vysoká přesnost, unikátnost žilního obrazce pro každého jedince.

Mezi nevýhody patří skutečnost, že vstupní čtecí zařízení je primárně konstruováno pro uchycení na zeď, což automaticky znepříjemňuje nebo znemožňuje identifikaci osob „ nevhodné “ výšky. Metoda vyžaduje, aby se uživatel díval do přesně vymezeného prostoru a měl zaostřeno na daný bod. Tento požadavek není vhodný v případě, že uživatel nosí brýle, nebo je mu nepříjemný kontakt se snímacím zařízením. Vlastní snímání dokonce patří k nejvíce nepříjemným a nepohodlným ze všech biometrických systémů. Další nevýhodou jsou přetrvávající předsudky mezi lidmi o nebezpečí snímání sítnice a vysoká pořizovací cena snímacího zařízení.

2.2.12 Rozpoznání obličeje

V případě měření geometrie obličeje dochází k určování pozic význačných částí obličeje, jakými jsou například oči, nos, ústa apod., a měření vzdáleností mezi nimi. Při použití této metody se z těchto snadno rozlišitelných prvků obličeje vytvoří číselný vektor, který uchovává naměřené hodnoty.

Biometrické systémy identifikující osoby pomocí rozpoznání jejich obličeje mají velmi dobré výsledky v laboratorních podmínkách, nicméně v praxi nepatří mezi nejpřesnější technologie.

2.2.13 Řeč

Verifikace hlasu spočívá v analýze řeči analyzované osoby.

Lidská řeč je charakteristická svou akustickou strukturou:

- amplitudové frekvenční spektrum měnící se v čase
- lingvistická struktura (diagnostika a skladba řeči)
- osobnost řečníka (intonace, rytmus, barva hlasu)

Zdrojem řečových kmitů jsou řečové orgány, tzv. vokálový trakt. Mírou rozpoznávání jsou řečové charakteristiky osoby, které jsou závislé na rozměrech vokálového traktu osoby.

Složení hlasového traktu a mluvních orgánů:

Aktivní mluvní orgány

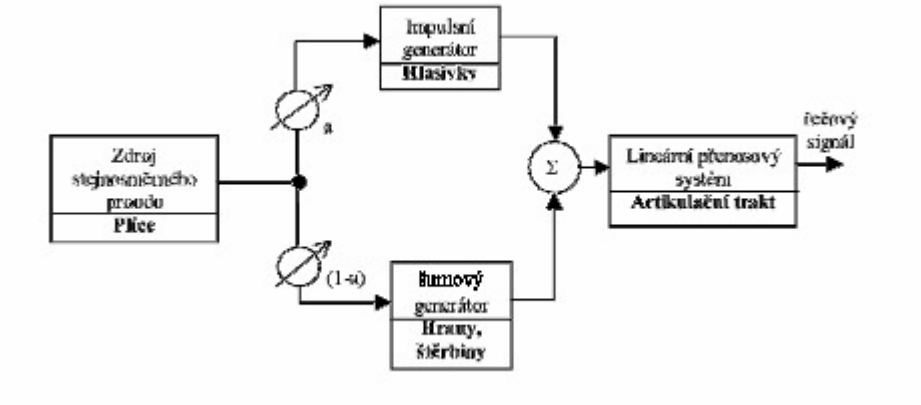
- A – mandibula (dolní čelist)
- B – labia (rty)
- C – Lingea (jazyk)
- D – velum (měkké patro)
- E – chordae vocales (hlasivky)

Vokální (hlasový) trakt

- Dutina ústní – orální
- Dutina nosní – nasální
- Dutina hrdelní – laryngální
- Velum, měkké patro

Generování řeči se skládá z:

- Plíce (zdroj stejnosměrného proudu)
- Hlasivky (impulsní generátor)
- Hrany, štěrbiny (šumový generátor)
- Artikulační trakt (lineární přenosový systém)



Obr. 27.: Generování řeči

Rozlišujeme dva přístupy:

- textově závislé – ang. v. TEXT DEPENDENTIT
  - identifikovaná osoba musí říct předem danou frázi

- textově nezávislé – ang. v. TEXT INDEPEDENTIT
  - identifikovaná osoba musí říct libovolnou frázi

Výhodou biometrických systémů založených na verifikaci hlasu je jejich nízká hardwarová náročnost.

Nevýhodou použití této biometrické technologie je její vysoká závislost na aktuálním stavu mluvčího, protože pokud má uživatel například rýmu nebo kašel, jsou podmínky identifikace značně ztížené.

2.2.14 DNA

Metoda vznikla jako vedlejší produkt výzkumu zaměřeného na studium struktury lidského genetického materiálu, za účelem diagnostiky onemocnění.

DNA (deoxyribonukleová kyselina) slouží jako základní nositelka genetické informace. Společně s RNA (ribonukleová kyselina) se řadí mezi tzv. nukleové kyseliny. Veškerá dědičná informace o organizmu, tedy soubor všech jeho molekul DNA se nazývá genom. Přečtením lidského genomu vedlo ke zjištění, že z počtu více než tří miliard „ písmen “

lidského genomu jich téměř 95 % nekóduje vůbec nic. Právě tyto nekódující oblasti DNA nalezly uplatnění při genetické identifikaci osob.

Pro identifikaci člověka podle jeho DNA ve skutečnosti postačuje obdržet jeho jednu jakoukoliv jadernou buňku. Mezi takové jaderné buňky patří například bílá krvinka (leukocyt), kterou lze poměrně snadno získat ze slin nebo krve. Dále mohou vytyčenému cíli posloužit také jiné buňky, odebrané z ostatních tělních tekutin nebo tělesné tkáně.

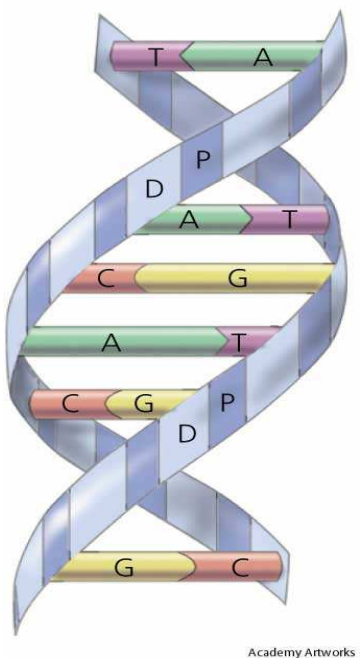
K identifikaci lze využít i buňky neobsahující jádro, jimiž jsou tvořeny například kosti a zuby. Přestože takové buňky nejsou úplné a neobsahují celou DNA, nacházejí se v nich tělíska zvaná mitochondrie – ty jsou součástí buňky a vytvářejí pro ni energii. Převážná většina genetického kódu je sice uložena v chromozomech (jaderná DNA), ale jeho malá část je přítomna i v mitochondriích jako takzvaná mitochondriální DNA.

Izolace molekuly DNA z buňky se nejčastěji provádí metodou zvanou fenolchloroformová extrakce.

K tomu, aby bylo možné provést analýzu dědičné informace člověka a na jejím základě vykonat identifikaci, je nejprve nutné jeho DNA přečíst. Určování pořadí (sekvence) nukleotidů v nukleových kyselinách se nazývá **sekvenování**.

Genetický kód DNA tvoří pouze čtyři nukleotidy (nukleové kyseliny):

- Adenin (A)
- Thymin (T)
- Guanin (G)
- Cytosin (C)



Obr. 28.: Struktura DNA

Řetězec DNA je protínán pohybujícím se paprskem vysoce výkonného laseru a přitom dochází ke vzniku mikroskopických záblesků modré, zelené, žluté a červené barvy. Citlivý detektor napojený na počítač zaznamenává kromě barvy těchto záblesků také jejich intenzitu a dobu trvání. Získané údaje jsou počítačově vyhodnocovány a převáděny do digitální podoby.

2.1.1.1 Metody sekvenování DNA

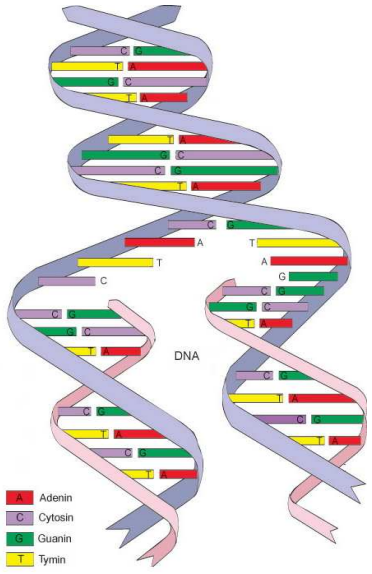
RFLP metoda

Metoda RFLP (ang. v. Restriction Fragment Length Polymorphism, dále jen RFLP) je založena na porovnávání nikoliv celé DNA, ale pouze jejích určitých úseků v chromozomech.

Ze všech doposud známých metod je právě RFLP, která na konkrétním úseku DNA dokáže nalézt nejvyšší počet variací nukleotidů. Čím více fragmentů DNA je při RFLP analýze zkoumáno, tím vyšší je šance na nalezení rozdílu mezi dvěma jedinci, nebo naopak na spolehlivější identifikaci daného člověka.

PCR metoda

Proces, při kterém se v přírodě z jedné dvojité šroubovice DNA stanou rozpojením jejich řetězců a doplněním odpovídajících nukleotidů dvě identické kopie téže DNA, lze aplikovat i v laboratorních podmínkách. A právě takovéto zmnožení (neboli amplifikace) vybraných sekvencí DNA je základem techniky nazývané PCR (ang. v. Polymerace Chin Reaction, dále jen PCR).



Obr. 29.: Replikace DNA

Výsledky analýzy jsou reprezentovány řadou modrých kruhových skvrn na detekčních proužcích. Porovnáním skvrn na dvou či více detekčních proužcích lze poté určit, zda dané genetické profily patří téže osobě, či nikoliv. Předností této techniky je rychlost celé analýzy, na druhou stranu však srovnávání barevných intenzit skvrn nemusí být vždy naprosto jednoznačné.

V dnešní době se pro identifikaci osob užívá spíše metod založených na délkovém polymorfismu – nejčastěji na hledání takzvaných STR polymorfismů (ang. v. Short Tandem Repeat, dále jen STR). Technika STR je částečně podobná metodě RFLP.

Budoucnost praktického využití DNA metod pro biometrické systémy spočívá jednoznačně v jejich automatizaci, zkrácení doby analýzy z dnů a týdnů na hodiny nebo spíše minuty a v miniaturizaci automatů. Kromě toho je potřeba také vyřešit problematiku získávání vzorků DNA.

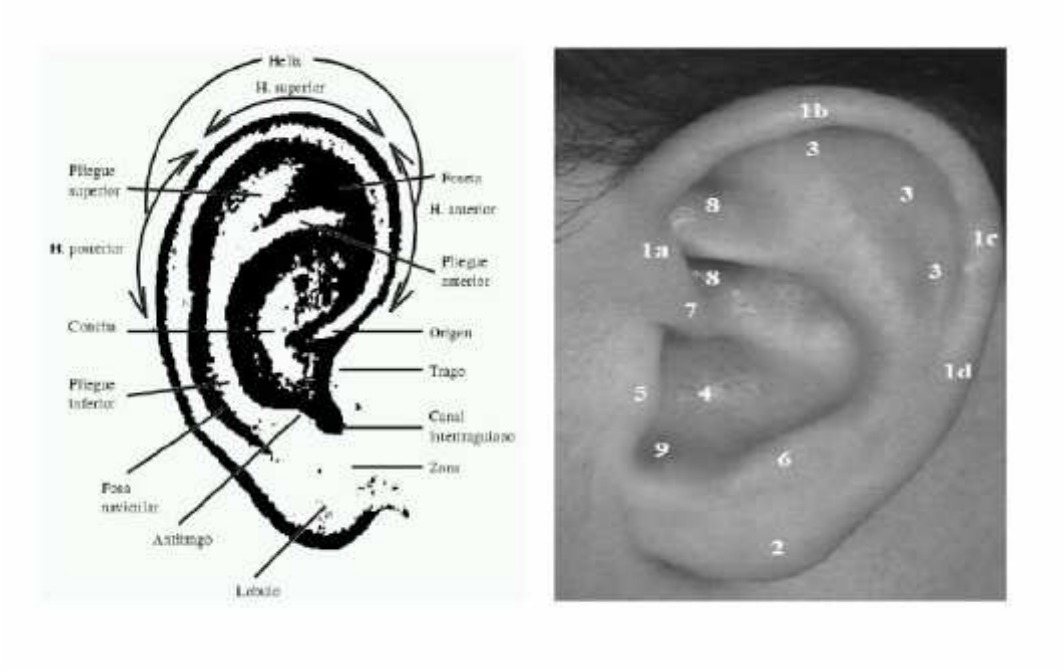
V tomto případě je nutné věnovat zvláštní pozornost také zajištění ochrany soukromí člověka, který používá biometrický systém na bázi srovnávání DNA profilů a poskytuje k analýze svoji DNA.

2.2.15 Ucho

Identifikace člověka pomocí biometrie ušního boltce je založená na individuálním tvaru a morfometrické stavbě ušního boltce každého jedince. Tvar ucha může sloužit jak k verifikaci, tak i k identifikaci. Porovnání je provedeno na základě komplexní struktury ucha. Růst ucha probíhá v prvních 4 měsících, následně se jen zvětšují proporce.

Anatomie ucha:

- Vnější závit ucha
- Ušní lalůček
- Protizávit ucha
- Concha
- Tragus
- Antitragus
- Ústí vnějšího závitu
- Delta
- Intertragica



Obr. 30.: Tvar ucha s popisem

Metody identifikace:

1) Podle morfometrických vztahů – geometrii ušního boltce, v 2D nebo 3D formě
2) Podle otisku struktur ušního boltce – tato metoda ale pro praxi není příliš „ komfortní“, její využití je ve forenzní oblasti
3) Podle termogramu ušního boltce – termografického snímku, mapujícího rozložení tělesné teploty na ušním boltci
4) Podle ozvěny vrácené kanálkem – tuto metodu navrhl počátkem roku 2003 Dr. Andrew Brown. Jeho systém by jako část čtecího zařízení používal obdobu telefonního sluchátka.

   Při identifikaci se ze sluchátka ozve posloupnost různých klapavých zvuků a následně dojde k analýze vrácené uchem identifikované osoby (jedná se o takzvané otoakustické emise).

2.2.16 Odontologie

Odontologie je atypickou biometrickou metodou identifikace, která je využívána převážně soudní odontologii k identifikaci podle zubů. Dentální informace mají velký význam především při identifikaci lidských těl, při hromadných neštěstích a u těl ve značném stádiu rozkladu, kde se dochovaly převážně kosterní pozůstatky.

2.2.17 Shrnutí biometrických metod

Aby byl biometrický systém snadno aplikovatelný v praxi, musí být uživateli co nejméně nepříjemný – v tomto ohledu lze uvažovat o snímání duhovky, rozpoznání obličeje, ověřování hlasu, dynamice podpisu nebo dynamice stisku kláves.

Všechny zmiňované techniky totiž od uživatele nepožadují přílišnou míru spolupráce a jsou přijímány veskrze kladně. Jednoznačně nejrozšířenější biometriku představují otisky prstu. Stále více se ovšem prosazuje také snímání duhovky oka, především díky vysoké přesnosti a jednoduchosti použití.

Při volbě vhodného biometrického systému je také zapotřebí brát v úvahu, zda bude využíván k identifikaci, nebo verifikaci.

Volba vhodné biometriky vždy závisí na konkrétním případu.

Tab. 3.: Vlastnosti základních biometrik

NĚKTERÉ VLASTNOSTI ZÁKLADNÍCH BIOMETRIK				
Biometrika	**Přesnost**	**Proměnlivost v čase**	**Uživatelská nepříjemnost**	**Cena**
Otisk prstu	***	*	**	*
Geometrie ruky	**	**	**	**
Rozpoznání obličeje	**	**	*	**
Oční duhovka	***	*	*	***
Oční sítnice	***	**	***	***
Lůžko nehtu	***	**	**	**
DNA	***	*	***	***
Ověřování hlasu	*	***	*	*
Dynamika podpisu	*	**	*	*
Dynamika stisku kláves	**	*	*	*

* - nízká hodnota uvedených parametrů biometrické metody / nízká cena

** - střední hodnota uvedených parametrů biometrické metody / střední cena

*** - vysoká hodnota uvedených parametrů biometrické metody / vysoká cena

2.2.18 Řeč a její analýza

Způsobů, jakými lze řeč analyzovat, je vcelku mnoho. Řečový signál je v podstatě jednorozměrný signál, k jehož rozboru existuje dostatečný matematický aparát. Pochopení mechanizmu vzniku řečového signálu a jeho bezchybná analýza, jsou základními předpoklady úspěchu dalšího jeho zpracování.

Řeč člověka je charakterizována akustickou strukturou (amplitudově – frekvenčním časovým spektrem), lingvistickou strukturou (gramatikou a skladbou) a subjektivním vlivem osobnosti řečníka (intonace, rytmus, barva hlasu atd.).

2.2.18.1 Vznik a charakter řeči

Řeč je v podstatě zvukový signál, který lze zobrazit časovým průběhem akustického tlaku. Tento průběh lze interpretovat jako signál s určitými specifickými vlastnostmi. Graficky lze průběh tohoto signálu znázornit jako závislost amplitudy elektrického signálu produkovaného snímacím zařízením (mikrofonem) na čase.

Řeč je generována tímto způsobem: vzduch, který je pod tlakem vytlačován z plic, způsobuje vibraci hlasivek (hlasivkových vláken) a produkuje signál s určitou základní frekvencí (tzv. základní tón řeči) s vyššími harmonickými frekvencemi.

Takto vzniklý signál prochází hlasovým traktem, který lze modelovat jako soustavu na sebe navazujících dutých válců. Tyto válce působí jako dutinové rezonátory a ovlivňují signál podle toho, jaký průřez mají, tj. podle toho, v jaké jsou konfiguraci. Člověk je schopen měnit průřezy jednotlivých „ válců “ a tím i modifikovat charakter výsledného signálu. Výsledkem tohoto procesu je zvuk. Při určité modifikaci hlasového traktu vznikají fonémy, které se člověk naučil interpretovat. Fonémy v určitém sledu tvoří plynulou řeč a jsou dvojího druhu – znělé a neznělé.

Znělé fonémy zachovávají periodičnost – harmoničnost signálu produkovaného hlasivkami. Charakteristickým rysem pro ně je, že jejich energie je soustředěna do několika frekvenčních pásem. Rezonanční frekvence jednotlivých dutin nazývají **formanty**.

Formantů je několik a každému z nich se dá zjednodušeně přiřadit určitá dutina hlasového traktu, která má největší vliv na jeho vznik.

Mezi znělé fonémy patří samohlásky a některé další hlásky („ M “, „ L “ aj.).

Neznělé fonémy mají povahu šumu, tj. jejich frekvenční charakteristika je vyrovnaná a nevykazuje žádné soustředění energie do frekvenčních pásem. Neznělé fonémy vznikají změnou polohy jazyka, rtů a zubů. Dynamickou změnou jejich polohy se mění průřezy dutin a tím i charakter výsledného signálu. Neznělé fonémy jsou pro svůj charakter podobný šumu velice těžce rozpoznatelné a v mnoha případech splývají se šumem pozadí. To může mít za následek jejich chybné rozpoznání. Vhodným matematickým aparátem je ale možné tento nežádoucí efekt minimalizovat (např. použitím mel-spektra nebo mel-kepstra).

2.2.18.2 Získání a předzpracování řečového signálu

Získávání (digitalizace) a předzpracování řečového signálu jsou v procesu rozpoznávání řeči velice důležité kroky. Na jejich správném provedení závisí výsledek celé analýzy.

Snímání a digitalizace

Prvním krokem zpracování hlasu je snímání hlasu pomocí mikrofonu. Tento stupeň analýzy bývá podceňován a může tak docházek ke ztrátám informace použitím nekvalitní techniky. Je vhodné zvolit takové zařízení, které má odpovídající kmitočtový rozsah a velký odstup signálu od šumu (ang. v. Signal to Noise Ratio, dále jen SNR). Pro účely rozpoznání řeči postačí frekvenční rozsah od 100 do 5500 Hz. Signál produkovaný mikrofonem je následně navzorkován a pomocí analogově-digitálního převodníku (ang. v. Analog to Digital Converter, dále jen ADC) digitalizován.

V této fázi zpracování řečového signálu musí být dodrženy některé principy z teorie digitálního zpracování signálů. Především je to vzorkovací teorém:

$$f_{vz} \geq 2 \cdot f_{Max} \qquad (1)$$

Po navzorkování signálu je prováděna digitalizace hodnoty amplitudy signálu pomocí převodníku analogového signálu na digitální. Cílem digitalizace signálu je získání co nejvěrnější digitální kopie původního analogového signálu. Existuje řada AD-převodníků s různými vlastnostmi. Mezi jejich rozhodující vlastnosti patří linearita, rychlost a přesnost digitalizace.

Produktem digitalizace je posloupnost numerických hodnot signálu . Protože byl originální signál konečný, je i posloupnost hodnot konečná. Délka této posloupnosti je N_{celk} a lze vypočítat jako:

$$N_{celk} = f_A \cdot T_{celk} \qquad (2)$$

Jelikož vzorkovací frekvence je v jednotkách [Hz] a celková délka signálu v jednotkách [s], nemá délka posloupnosti N_{celk} žádný rozměr.

Segmentace

Segmentace je dalším krokem zpracování signálu. Hlasový signál, produkovaný různými mluvčími se liší způsobem, jímž byl vyřčen (intonací, délkou vyslovených hlášek, atd.). Způsob a délka vysloveného slova jsou ale i u jediného mluvčího velice rozdílné. Proto není možné pracovat s celým signálem. Pro další práci je stanovena maximální délka signálu. Celý signál je tak rozdělen na tzv. segmenty.

Velmi vhodné je také zvolit určitou úroveň překrývání jednotlivých segmentů. Pokud by žádné překrývání segmentů nebylo zvoleno, mohly by některé krátké a nevýrazné hlásky zaniknout, což by vedlo k chybnému rozpoznání slov.

Po zvolení vhodné délky segmentu a velikosti jejich překrývání, jsou pak z celého signálu sekvenčně vybírány segmenty o této délce. Ty jsou dále zpracovávány následujícími metodami.

Preemfáze

Preemfáze nebo také preakcent řečového signálu je jeho předzpracování za pomoci digitální horní propusti, která posiluje oblast vyšších frekvencí a u znělých fonémů snižuje vliv základního tónu řeči a tím i výraznost prvních formantů. Tím je umožněno lepší rozpoznání jednotlivých hlásek.

Násobení oknem

Před zpracováním signálu dalšími metodami je vhodné signál vynásobit oknem, jehož délka je shodná s délkou segmentu. Nejpoužívanějším oknem je Hammingovo okno.

Analýza řečového signálu

Analýza řečového signálu poskytuje prostředky pro rozpoznávání hlasu. Výsledkem této analýzy jsou parametry (příznaky), které popisují určité vlastnosti signálu. S pomocí těchto příznaků lze analyzovaný segment signálu dále klasifikovat. K analýze se používají známé matematické metody pro zpracování a analýzu jednorozměrných signálů, kterým řečový signál je.

Autokorelace

Korelace dvou signálů udává míru podobnosti dvou signálů. Podobně autokorelace udává míru podobnosti signálu vůči sobě samému. Signál je možné posouvat o určitý počet vzorků. Tento posun se nazývá řád autokorelace. Autokorelace udává, jak je původní signál podobný signálu posunutému. Z toho plyne, že největší hodnotu bude mít autokorelace signálu se sebou samým s nulovým posunem – tj. autokorelace řádu 0.

Nalezení počátku a konce slova

Pro správnou analýzu řečového signálu je velmi důležité, co nejpřesněji stanovit počátek a konec promluvy. Experimentálně bylo zjištěno, že právě přesné určení hranice mezi slovy rozhoduje o úspěšnosti celého systému pro rozpoznávání slov. K nalezení začátku a konce

- metodu sledování obálky
- metodu rozdílnosti příznaků

LPC spektrum a kepstrum

LPC koeficienty (koeficienty lineárního predikčního kódování) hrají velkou roli ve zpracování řečového signálu. Jejich vlastností je to, že pomocí lineární kombinace určitého počtu známých vzorků signálu je možné vypočítat (predikovat, předvídat) následující průběh signálu. Výsledný signál je pak „ hladký “, tj. bez rušivých vlivů. Dojde tedy k potlačení šumu a odstranění těch vlastností signálu, které jsou dány jednotlivými mluvčími.

LPC spektrum

Máme-li vypočítány koeficienty LPC, pak lze pomocí nich vypočítat i tzv. frekvenční LPC spektrum. Toto spektrum se od klasického spektra liší tím, že má velmi kvalitně vyhlazený průběh. To je ve zpracování řeči velkým přínosem, neboť v něm jasně vyniknou rezonanční kmitočty jednotlivých formantů, což velmi usnadní rozpoznávání řeči.

LPC kepstrum

Z kepstra signálu lze zjistit, zda jde o znělý či neznělý segment, neboť u znělých fonémů obsahuje kepstrum výraznou špičku, kterou lze také reprezentovat jako základní frekvenci hlasu, již obsahují pouze znělé fonémy. Naopak u neznělých úseků jsou první hodnoty koeficientů kepstra maximální, protože na jeho počátku jsou kumulovány vyšší frekvence.

V aplikaci zaměřené na rozpoznávání řeči se pracuje s navzorkovaným a digitalizovaným řečovým signálem. Tento signál je zpracován pomocí preemfáze a segmentován. Jednotlivé segmenty jsou násobeny Hammingovým oknem. Tento proces se nazývá **předzpracování řečového signálu.**

3 BIOMETRICKÉ STANDARDY

Nosným pilířem pro rozvoj technického pokroku v oblasti biometrie jsou biometrické standardy. Je nutné standardizovat biometrický slovník a definice, technická rozhraní, formát pro úschovu a přenos biometrických dat, výkonnost biometrických systémů, bezpečnost apod.

Standard

Standard je utvořen běžným a opakovaným používáním pravidel, podmínek, směrnic nebo charakteristik produktů, procesů a produkčních metod.

Technický standard

Technický standard tvoří kombinace těchto pojmů: definice terminologie; klasifikace komponent; nástin procedur; specifikace dimenze materiálu, výkonu, designu a funkčnosti; měřítka kvality a kvantity pro popis materiálu, procesů, produktů, systémů; testovací a vzorkovací metody; popis měřítek přesnosti, velikosti a stability.

Otevřený standard

Otevřený standard je standard plně otevřený veřejnosti.

Úspěšný standard musí být volně dostupný, splňovat požadavky velké skupiny provozovatelů, být flexibilní ke změnám, být konzistentně implementován a být kompatibilní vzhledem ke starším verzím.

Typy standardů pro biometrii

1. Standardy k výměně dat
    - Aplikační struktura
    - Datové formáty

2) Standardy pro výkonnost biometrických systémů
   - *Best Practices* pro testování
   - Standardní databáze
   - Praktiky při tvorbě reportů

3) Standardy pro celkovou bezpečnost systémů
   - Zjišťování zranitelnosti dle standardních postupů
   - Ochrana dat
   - Zajištění funkčnosti komplexní ochrany

Přehled základních organizací, zabývajících se standardy:

- BioAPI Consortium

http://www.bioapi.com

- ANSI X9.F4

http://www.x9.org

- BC Working Group

http://www.biometrics.org/html/work_groups.html

- DoD-BMO, BEMWG

http://www.biometrics.dod.mil

- U.K.BWG, FV2004, FVRT2004, IBG

4 NOVÉ TRENDY VE VÝVOJI

4.1 Bezpečnost

Terorismus se stal fenoménem dvacátého století a v důsledku globalizace zasáhly jeho negativní vlivy rovněž Českou republiku. Byla zpracována již celá řada expertíz zabývajících se mírou ohrožení jednotlivých zemí terorismem. Například podle expertíz vypracovaných jednou z předních globálních pojišťovacích společností AON, která již od roku 2003 vydává materiál, pod názvem „ Expertíza rizika terorismu na pojišťovnictví “ (ang. v. Terrorism Risk Insurance Expertise), byla Česká republika zařazena do skupiny s nejnižší mírou ohrožení, do skupiny „ nízkého rizika „. Roku 2004 byla přeřazena již do skupiny o stupeň vyšší, tedy do skupiny „ riziko vyžadující ostražitost „ (v žebříčku míry rizika ohrožení následuje skupina: „ zvýšené riziko “, „ vysoké riziko “ , „ naprosté riziko “).

Je zřejmé, že rostoucí obavy z bezpečnostních rizik vedou mezinárodní a národní (vládní) instituce i soukromé společnosti k využívání co nejkvalitnějších systémů zabezpečujících přístupy na svá území, do různých objektů či informačních systémů obsahujících strategické údaje. Z tohoto pohledu jsou za nejmodernější způsob k ověřování totožnosti a „ identifikace“ oprávněných osob považovány právě moderní biometrické systémy.

Z hlediska vnitřní bezpečnosti, ochrany života a zdraví osob, ochrany majetku a objektů představuje dnes biometrie skutečně významný fenomén v životě téměř každé země. Rovněž v boji proti terorismu zaujímá podstatnou roli .

Typickým příkladem využití může být vyhledávání a identifikace osob – aktérů politického, kriminálního, resp. patologického terorismu. Podle získaných biometrických dat systém rozpozná, zda se jedná o osobu známou, se záznamem v databázi. Právě tyto osoby používají ke své nelegální činnosti anonymity davu.

O zavádění biometrických technologií se v rámci zajištění bezpečnosti uvažuje i na hraničních přechodech v Evropě. Přednost skenu oční sítnice dává např. Mezinárodní úřad pro civilní letectví CAO (ang. v. International Civil Aviation Organisation). Pro mezinárodní sjednocení průkazů totožnosti a cestovních dokladů je i příslušný úřad OSN.

Bude to čipová karta spojená s digitálním a biometrickým znakem . Tento znak bude na kartě uložen v zašifrované podobě. Autentizace bude probíhat bez porovnání s databází, tzn. výlučně prostřednictvím porovnání znaku na průkazu s odpovídajícím znakem osoby, která průkaz předkládá.

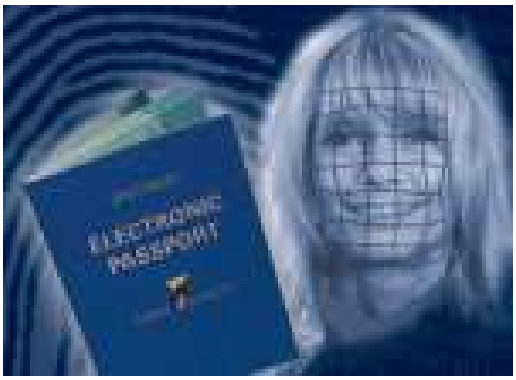
4.2 Nové pasy s biometrickými prvky

V r. 2004 vydala Rada Evropské unie nařízení, podle kterého musí všechny členské státy Unie od září r.2006 vydávat pasy s biometrickými údaji.

V polykarbonátové destičce nebo na krycích deskách pasu je zabudován RFID čip (ang. v. Radio Frequency Identification, dále jen RFID čip). Radiofrekvenční systém identifikace je moderní technologie identifikace objektů pomocí radiofrekvenčních vln. Tento systém lze úspěšně nasadit v mnoha odvětvích a oblastech, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos těchto načtených dat k následnému zpracování. Informace jsou v elektronické podobě ukládány do malých čipů - tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln. Toto zpracování se však neděje po jednotlivých čteních jako u v současnosti používaných čárových kódů, ale hromadně. Současná čtecí zařízení dokážou najednou načíst až několik set tagů za minutu. RFID čip obsahuje digitální fotografii majitele s demografickými údaji z poslední stránky pasu. Od r. 2007 budou biometrické pasy obsahovat otisk prstu a v budoucnu rovněž obraz sítnice oka. Řešení registrace nového pasu se skládá z registrační stanice, což je skener otisku prstu a kamera, která sejme obraz tváře. Z této registrační stanice jdou šifrovaná data do personalizační stanice. Zde se tato data odkryptují, zkontroluje se odchozí a příchozí počet bitů. Následně jsou data importována do čipu v pase. Pas putuje zpět do registrační stanice, kde je předán občanovi na základě konfrontace biometrických a demografických dat. Nikdo cizí tedy nemůže pas převzít.

Pro ověřování identity jsou na hraničních přechodech moderní čtečky pasů, jejichž součástí bude i čtečka otisku prstu. Toto zařízení, po vložení pasu, nejprve přečte demografická data. Následně držitel pasu přiloží prst na čtecí zařízení, které porovná otisk prstu v čipu se skutečností. Současně se na obrazovce objeví obraz tváře a potvrzení, že otisk prstu v čipu souhlasí s otiskem prstu nositele pasu.

Obr. 31.: Pohled do zóny žadatele (vlevo), pohled do zóny úředníka (vpravo)



Obr. 32.: Pas s biometrickými prvky

Rovněž v rámci imigrační politiky se Evropská unie (dále je EU) rozhodla k vybudování „ Vízového informačního systému „ pro svůj takzvaný Schengenský prostor. Standardně tak bude prováděna implementace čipů s biometrickými daty, konkrétně otisky prstů a sken oční duhovky, do pasů. Členské státy EU mají povinnost rutinně ukládat fotografie žadatelů o vízum nebo o dlouhodobý pobyt jako primární biometrický identifikátor. Pomocí kombinace otisků prstů a fotografie se má zamezit zneužití dokladů a také zvýšit bezpečnost. Znamená to také nutnost sjednotit používané biometrické systémy a zajistit jejich vzájemnou spolupráci pro jednotnou evropskou politiku.

4.3 Biometrie a spotřební elektronika

V aplikacích biometrie na rozhraních výpočetních systémů ve službách, spotřební elektronice a průmyslu nacházejí uplatnění především již zmíněné moderní metody založené na elektronickém snímání otisků prstů, především v kombinaci s optikou, metody identifikace hlasem a pro instalace vyžadující vysokou bezpečnost – metody identifikace oční duhovky.

Obr. 33.: Panasonic BM-T120

Kompaktní PC kamera s technologií ověřující identitu uživatele podle oční duhovky, sloužící pro zabezpečení přístupu do počítače nebo počítačové sítě. Připojení zařízení přes USB port.

Obr. 34.: Identix BioTouch USB

Periferní zařízení k PC, snímající otisky prstů, s připojením na USB port. Součástí dodávky je software BioLogon 3 pro zabezpečené přihlášení do systému Windows.

Obr. 35.: Identix BioTouch PC Card

Periferní zařízení ve formátu PC Card, snímající otisky prstů, vhodné zejména k přenosným počítačům. Součástí dodávky je software BioLogon 3 pro zabezpečené přihlášení do systému Windows.

4.4 Biometrie a forenzní aplikace

V minulosti i v době současné se odehrálo mnoho katastrof, při kterých zahynul velký počet lidí. Těla obětí je v současnosti možné identifikovat pomocí běžných biometrických vlastností – např. obličej, otisky prstů. Biometrickou identifikaci lze použít i v případech, kdy těla obětí jsou znetvořena. V těchto případech jsou použity např. dentální informace, DNA. V identifikaci pro účely kriminalistiky je důležité bezchybné rozpoznání identity jedince. Je zde tedy kladen primární požadavek na co nejmenší chybovost systémů, klasické požadavky komfortu při použití zde nemají význam.

V současné kriminalistice je možné biometrické systémy rozdělit z hlediska účelu, jemuž tyto systémy slouží, resp. jakými metodami k „ identifikaci “ osob dochází, na dvě základní kategorie, a to na:

1) biometrické systémy operativní a typovací

Mezi tyto systémy řadíme biometrické metody, které např. pomáhají ustanovit zájmovou osobu podle tělesných znaků - popisu, vytvořením portrétu svědků, pachatelů, podezřelých apod. Patří sem např. systémy portrétní identifikace, které jsou nyní provozovány zejména pomocí speciálně vytvořených počítačových programů známých pod označením „ Poridos “ anebo „ Facette “.

2) biometrické systémy expertizní – forenzní

Jsou to aplikace biometrie, které jsou po zpracování znalcem, resp. kriminalistickým expertem, předkládány v soudním a správním řízení jako znalecké důkazy z příslušných oborů - daktyloskopie, trasologie, antropologie, portrétní identifikace, analýzy DNA, pachové identifikace apod. Zde je možné uvést např. automatizované identifikační systémy AFIS (ang. v. Automated Fingerprint Identification Systeme) a CODIS (ang. v. Combined DNA Index System).

4.5 Biometrie a přístupové systémy

Biometrické metody identifikace osob nacházejí uplatnění i v jiných oblastech než je kriminalistické hledisko, například v oblasti bezpečnostních a přístupových systémů do objektů, kdy jsou různé biometrické metody kombinovány s čipovými přístupovými kartami. Systém zabezpečuje funkce související s řízením pohybu osob po budově. Vzhledem k tomu, že v rámci přístupového systému je každý uživatel jednoznačně identifikován, je možné provázat data přístupového systému např. s evidencí a vyhodnocením docházky, organizací parkování, kontrolou využívání kopírovacích strojů, bezhotovostní úhradou za stravování apod. V poslední době se tyto biometrické metody uplatňují i v zabezpečení přístupu do systémů personálních počítačů a přístupu do firemních informačních sítí .

V aplikacích zabezpečujících fyzický přístup do střeženého objektu je důležité znát stupeň požadovaného zabezpečení, respektive možné negativní důsledky z proniknutí. V případě možných velkých ztrát, je nutné odhlédnout od vynaložených velkých nákladů a použít v daném případě vysoce spolehlivých metod biometrické identifikace, jako např. identifikace oční sítnice, nebo duhovky. V případě nízkého rizika je optimální využití např.

identifikace využívající geometrie ruky. Tato metoda nese výhody v nízkých nákladech, rychlosti, jednoduchosti a spolehlivosti.

4.6 Biometrie a elektronická zdravotní karta

Jedná se o elektronickou zdravotní kartu (ang. v. Computarized Patient Rekord, dále jen CPR), která je lehce dosažitelná pro kteréhokoliv lékaře. Údaje v této kartě jsou chráněny biometrickou informací – verifikace/povolení přístupu k informacím z karty. CPR elektronicky spravuje veškeré informace o zdravotním stavu a péči jedince během jeho celého života. Počítačový záznam kompletně nahrazuje papírovou formu a splňuje veškeré požadavky ze zdravotnického hlediska, právnického hlediska a hlediska ochrany osobních údajů.

4.7 Biometrie a bankovní aplikace

Biometrické aplikace se s úspěchem prosazují i v bankovní sféře, kde zajišťují bezpečnost a zároveň i informace o pohybu osob.

Široké spektrum uplatnění zde nalezla především biometrická identifikace prostřednictvím otisku prstu, která řeší bezpečnost transakcí, síťovou bezpečnost, oblast přístupových systémů a přístup k safetovým (bezpečnostním) schránkám. Oblast telefonního bankovnictví řeší biometrická identifikace hlasová.

Jedním z příkladů praktického využití biometrických metod v bankovní sféře je např. elektronický informační systém určený na evidenci a rychlé vyhledání textových a obrazových informací. Uvedený systém obsahuje informace o klientech, jejich podpisových vzorech, razítkách a biometrických vzorcích a je určen pro potřeby bank s centralizovanými pracovišti. Biometrickou kontrolou nositele podpisu, např. prostřednictvím biometrické čtečky otisku prstu je umožněn rychlý přístup k podpisovým vzorům z bankovního informačního systému z libovolné pobočky centrální banky. Uplatnění biometrie v dané aplikaci zajišťuje bezpečný systém kontroly totožnosti a

oprávněnosti osoby k finančnímu úkonu. Proces manipulace s účtem s touhle dispozicí je bezpečný pro pracovníka banky i klienta.

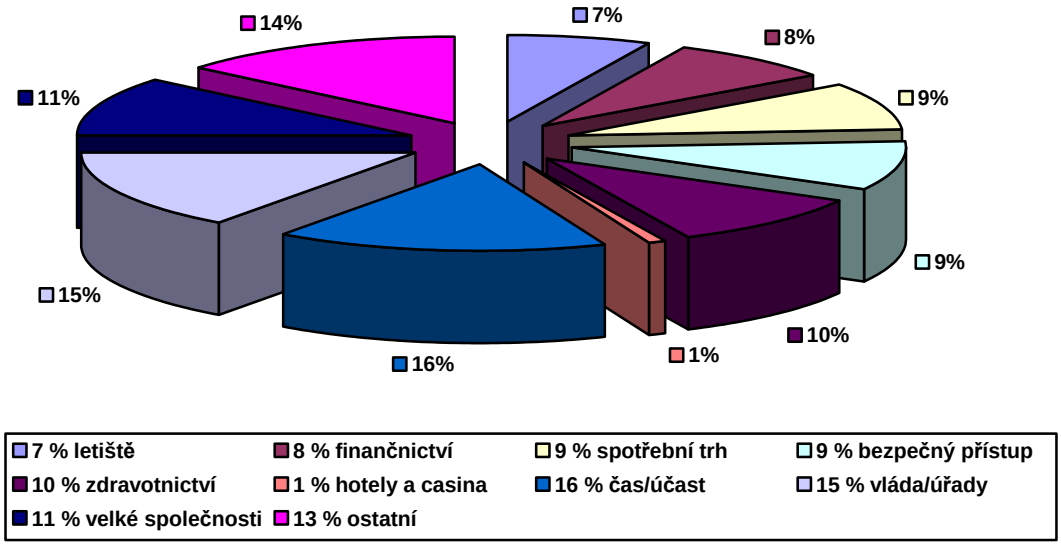
Obr. 36.: Podpisové vzory – BioSigns

ZÁVĚR

Biometrie ve svých počátcích byla spojována především s jednoduchým měřením pouze vnějších fyziologických znaků živých organismů. Dnes je spojována s veškerou živou přírodou včetně měření její vnitřní struktury a vnitřních charakteristik. U člověka se biometrie významně rozšířila od měření pouze fyzických znaků i do oblasti znaků behaviorálních. Od využívání poměrně jednoduchých metod, postupů a technických prostředků měření přešla biometrie k mnohem efektivnějším systémům.

V poslední době jsme svědky prudkého rozvoje v oblasti bezpečnosti. Již nejenom státní instituce, ale i firmy si začínají uvědomovat rizika spojená s vyzrazením důvěrných informací, od nových myšlenek a technologií až po osobní údaje o zaměstnancích. Z těchto důvodů byl zaznamenán vysoký nárůst investic do bezpečnosti a zabezpečení. Společnost si uvědomuje nespolehlivost lidské mysli v otázce bezpečnosti a proto se ji snaží zajistit kvalitnějším způsobem, a to použitím právě biometrie.

Rozvojem informačních technologií se cena biometrických systémů stává příznivější a přijatelnější k širokému uplatnění rovněž pro firmy, nikoliv už jen pouze globálně v rámci zajištění bezpečnosti státu. O této skutečnosti vypovídá následující graf.



Obr. 37.: Přehled využití biometrických systémů

Technologie biometrických systémů je v současné době již ověřená a dostupná pro masové použití. Většina technických a technologických překážek je dnes již vyřešena. Poslední překážkou, která stojí biometrickým systémům a aplikacím na cestě ke skvělé budoucnosti je potřeba překonat informovaností a popularizací bariéru na straně uživatelů, pro něž je používání některých systémů nepohodlné, nebo se jich dokonce obávají.

Ve své práci jsem se zabývala vznikem a časovým vývojem biometrie, biometrickými parametry, což zahrnuje objasnění jednotlivých pojmů, principů a fází, z kterých se skládá proces biometrické identifikace. Další kapitola představuje jednotlivé metody a jejich funkční principy. Pilířem každé kvalitní informační technologie a jejího rozvoje je předpoklad existence a důsledné dodržování příslušných standardů. Nejinak je tomu i v oblasti biometrie. Poslední kapitola je věnována novým vývojovým trendům. Jsou zde uvedeny jednotlivé konkrétní aplikace biometrických systémů, jež umožňují vytvoření konkrétní představy o funkčnosti a výhodách, které přináší z hlediska pohodlí a komfortu pro uživatele a především z hlediska zajištění bezpečnosti, které je a bude naší prioritou.

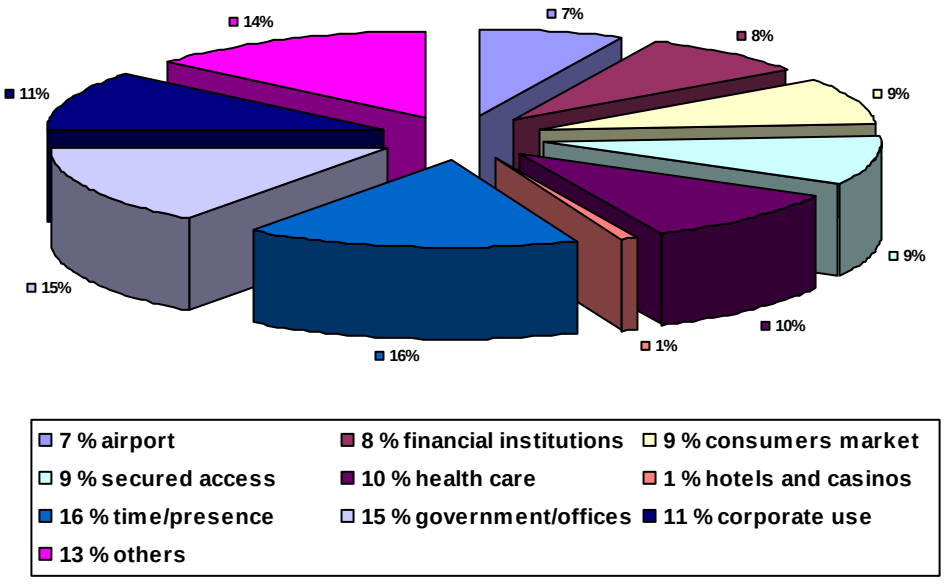
Účelem bakalářské práce bylo podat ucelený přehled a vypracovat edukační materiál pro oblast biometrie, který je možné využít jako učební nebo firemní materiál pro vzdělávání, získávání poznatků a seznámení s problematikou daného oboru.

CONCLUSION

Biometrics at its beginnings had been connected mainly with simple measurments only of external physiological tokens of living organisms. Today it is connected with the whole living nature including the measurments of internal structures and internal characteristics. The biometrics has widened its range when applied to human beings from measuring of just physical tokens to areas of behavioral tokens. From the times when simple methods, procedures and technical measurment resources, the biometrics has moved on to much more efficient systems.

In recent times we have been witnessing rapid progress in the field of security. Not only the state institutions but companies alike have started to appreciate the risk linked to leakage of secret information anywhere from new inventions and technologies to personal details of their employees. For this reason there has been noted increasingly hight investments into security and protection. Companies understand the unreliebility of human mind when the security is concerned and that is why they try to protect themselves by better quality means and by using biometrics.

By further development of information technologies the cost of biometrical systems is becoming more and more favourable and more acceptable for wider application especially among companies and it is no longer exclusive to countries´ security protection. This fact is described in a following graph.



The technology of biometrical systems is at present well verified and accessible for widespread use. Most of technical and technological obstacles have been solved. The last of the obstacles that stands in the way of a bright future for the biometrical systems as well as the applications is the neccessity to overcome the barrier on the side of its users by informing and popularization. It is them who often find the use of some systems uncomfortable and even something to be afraid of.

In my work I have dealt with the origins, the development of biometrics over the years and the biometrical parameters which include clarifications of individual definitions, principles and phases by which the process of biometrical identification is formed. The next chapter introduces particular methods and their functional principles. The base for each good quality information technology and its development is the presumption of an existence and rigorous compliance with correspondent standards. Not excluding the field of biometrics, of course. The last chapter is dedicated to the newest development trends. Some actual applications of biometrical systems are introduced here which allow final users to form a certain image about the functionality as well as advantages of these systems from the point of user´s comfort and more importantly from the point of protecting security which remains and always will remain our priority.

The objective of my bachelor work is to offer comprehensive overview and to draw up an educational material for the field of biometrics which can be used as instructional and corporate material for education, obtaining of findings and introduction to the problematics of given subject.

SEZNAM POUŽITÉ LITERATURY

[1] SOJKA E. *Digitální zpracování a analýza obrazů.* [Skriptum] VŠB Ostrava 2000.

[2] KŘEČEK S. *Příručka zabezpečovací techniky*, Praha, 2003.

[3] BITTO Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*.

[4] UHLÁŘ J. *Technická ochrana objektů*, PA ČR, Praha, 2001.

[5] PETR, J. A KOLEKTIV. *Mluvnice češtiny*. Díl 1. Praha: Akademia, 1986.

[6] Ing. DRAHANSKÝ Martin, Ph.D. *Biometrické systémy – BIO.* [Skriptum] VUT Brno 2006.

[7] *Security Magazín leden / únor 2007:* Je možné měřit míru ohrožení země terorismem? str. 23 – 25

[8] plk. JUDr. VANČO Emil. *Biometrie, biometrika - geneze, vývoj a současné pojetí*.

[9] http://www.mvcr.cz/casopisy/kriminalistika/2005/01/vanco_info.html

[10] http://www.symantec.cz/region/cz/resources/2004/article_1_5.html

[11] http://www.digitus.cz/pristup_pc.php

[12] http://www.automa.cz/automa/2003/au070334.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FAR falešné přijetí (ang. v. False Akcept Rate)

FRR falešné odmítnutí (ang. v. False Reject Rate)

EER míra rovné chyby (ang. v. Equal Error Rate)

DNA deoxyribonukleová kyselina

RNA ribonukleová kyselina

RFLP metoda sekvenování (ang. v. Restriction Fragment Length Polymorphism)

PCR metoda sekvenování (ang. v. Polymerace Chin Reaction)

STR (ang. v. Short Tandem Repeat)

SNR odstup signálu od šumu (ang. v. Signal to Noise Ratio)

ADC analogově digitální převodník (ang. v. Analog to Digital Converter)

LPC koeficienty lineárního predikčního kódování

CAO Mezinárodní úřad pro civilní letectví

(ang. v. International Civil Aviation Organisation)

RFID radiofrekvenční systém identifikace (ang. v. Radio Frequency Identification)

CPR elektronická zdravotní karta (ang. v. Computarized Patient Rekord)

AFIS Automated Fingerprint Identification Systeme

CODIS Combined DNA Index System

SEZNAM OBRÁZKŮ

SEZNAM TABULEK