

# Biometrické systémy

## BIO

Studijní opora

Ing. Martin Drahanský, Ph.D.

Verze: 01.2006

Tato publikace je určena výhradně jako podpůrný text pro potřeby výuky. Bude užita v přednášce výlučně k účelům vyučovacím či k jiným vzdělávacím účelům. Nesmí být používána komerčně. Bez předchozího písemného svolení autora nesmí být kterákoliv část této publikace kopírována nebo rozmnožována jakoukoliv formou (tisk, fotokopie, mikrofilm, snímání scannerem či jiný postup), vložena do informačního systému nebo jiného počítačového systému nebo přenášena v jiné formě nebo jinými prostředky. Všechna práva vyhrazena – © Martin Drahanský.

Tento učební text vznikl za podpory projektu *Zvýšení konkurenční schopnosti IT odborníků – absolventů pro Evropský trh práce*, reg. č. CZ.04.1.03./3.2.15.1/0003. Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

# Obsah

1.	Úvod	1
1.1	Úvod .....	1
1.2	Značení, symboly, konvence .....	1
2.	Úvod do biometrických systémů .....	3
2.1	Historie .....	3
2.1.1	Antropometrie .....	4
2.2	Identita, Identifikace, Verifikace .....	5
2.3	Biometrie, Biometrický systém .....	8
3.	Teorie zpracování zvukových a obrazových informací .....	14
3.1	Senzory a měření .....	14
3.2	Matematické a statistické základy .....	17
4.	Hodnocení spolehlivosti a kvality biometrických systémů .....	24
4.1	Statistické základy pro hodnocení .....	24
4.2	Porovnání a jeho chyby .....	26
5.	Rozpoznávání podle otisků prstů .....	35
5.1	Základy .....	35
5.2	Technologie senzorů .....	39
5.3	Funkce systému .....	40
6.	Rozpoznávání podle geometrie ruky, žil ruky a nehtu .....	47
6.1	Rozpoznávání podle geometrie ruky .....	47
6.2	Rozpoznávání podle žil ruky .....	51
6.3	Rozpoznávání podle nehtu .....	53
7.	Rozpoznávání podle obličeje a termogramu obličeje .....	54
7.1	Detekce obličeje .....	55
7.2	2D rozpoznávání obličeje .....	56
7.3	3D rozpoznávání obličeje .....	59
7.4	Rozpoznávání termogramu obličeje .....	64
8.	Rozpoznávání podle duhovky a sítnice .....	66
8.1	Rozpoznávání podle duhovky oka .....	66
8.2	Rozpoznávání podle sítnice oka .....	72
9.	Rozpoznávání podle hlasu .....	75
9.1	Základní pojmy .....	75
9.2	Zpracování hlasu a jeho příznaky .....	77
10.	Rozpoznávání podle písma a podpisu .....	85
10.1	Základy rozpoznávání písma a podpisu .....	85
10.2	Metody rozpoznávání podpisu .....	88
11.	Dynamické biometrické vlastnosti .....	95
11.1	Rozpoznávání dynamiky stisku kláves .....	95
11.2	Rozpoznávání chůze .....	98
11.3	Rozpoznávání pohybu rtů .....	100
12.	DNA a její využití v biometrii .....	103
12.1	Základy .....	103
12.2	Práce s DNA .....	105
13.	Biometrické standardy .....	109
14.	Biometrické systémy budoucnosti .....	117
14.1	Atypická biometrika – Tvar ucha .....	117
14.2	Atypická biometrika – Odontologie .....	119
14.3	Atypická biometrika – Otisk dlaně, Přítoky na pero a 3D prst .....	122
14.4	Multimodální biometrický systém .....	122
14.5	Další aplikace budoucnosti .....	123
15.	Literatura .....	128
16.	Akronypy .....	130

# 1. Úvod

## 1.1 Úvod

Předmět **Biometrické systémy** (BIO) je vyučován v zimním semestru na Vysokém učení technickém v Brně, Fakultě informačních technologií. Předmět se skládá z přednášek, laboratorních cvičení a projektů. Struktura přednášek je následující:

1. Úvod do biometrických systémů
2. Teorie zpracování zvukových a obrazových informací
3. Hodnocení spolehlivosti a kvality biometrických systémů
4. Rozpoznávání podle otisků prstů
5. Rozpoznávání podle geometrie ruky, žil ruky a nehtu
6. Rozpoznávání podle obličeje a termogramu obličeje
7. Rozpoznávání podle duhovky a sítnice
8. Rozpoznávání podle hlasu
9. Rozpoznávání podle písma a podpisu
10. Dynamické biometrické vlastnosti
11. DNA a její využití v biometrii
12. Biometrické standardy
13. Biometrické systémy budoucnosti

a odpovídá i struktuře této studijní opory, zejména z důvodu snadné orientace. V jednotlivých kapitolách se nachází i příklady k laboratorním cvičením a příp. ukázky zařízení, používaných během cvičení apod.

Laboratorní cvičení jsou celkem tři:

1. Rozpoznávání podle otisků prstů, práce s termokamerou
2. Rozpoznávání podle hlasu
3. Praktická ukázka průmyslových biometrických systémů

Jejich začátek je v průběhu semestru, až po probrání patřičných částí v rámci přednášek.

V rámci tohoto předmětu se dozvítě něco o lidských vlastnostech (jak fyzických, tak i lidského jednání), jak můžeme tyto vlastnosti získat pro následné počítačové zpracování, které rysy jsou významné a jak pomocí nich rozpoznáme dva jedince od sebe. Navíc budou zmíněny i metodiky hodnocení biometrických systémů a jaké standardy jsou v této oblasti k nalezení. V závěru naleznete vyhlídku do budoucnosti, tj. jakým směrem se biometrické systémy mohou ubírat.

## 1.2 Značení, symboly, konvence

V celém textu je použita základní jednotná konvence vztahující se k řezu písma a jeho konkrétnímu významu:

(Výrazy psané v závorce kurzívou jsou původní anglické výrazy vztahující se k určitému výrazu).

**Tučně psané výrazy v textu jsou významné pojmy, které je nutné znát a zcela určitě se mohou vyskytnout na zkoušce.**

*Části psané kurzívou jsou významné pojmy, ale méně jak tučné.*

Příklady, ukázky výpočtů a jiné praktické zvýraznění teorie je označeno takto.

Kromě zvýraznění textu jsou v levém sloupci použity ikony usnadňující studium tohoto materiálu. Jednotlivé ikony se vztahují k části textu, u níž jsou uvedeny. Jejich konkrétní význam shrnuje Tabulka 1.

Ikona	Význam	Ikona	Význam
	Počítačové cvičení, příklad		Správné řešení
	Otzáka, příklad k řešení		Obtížná část
	Námět k zamýšlení		
	Příklad		
	Slovo tutora, komentář		Důležitá část
	Potřebný čas pro studium, (číslice v hodinách; jedná se o pouhý odhad)		Cíl
	Reference		Definice
	Souhrn		Zajímavé místo
			Rozšiřující látka, informace, znalosti. Nejsou předmětem zkoušky.

Tabulka 1: Symboly použité v tomto materiálu a jejich význam.



## 2. Úvod do biometrických systémů

V této kapitole si vysvětlíme základní pojmy z oblasti biometrie, k nimž řadíme **identitu, identifikaci, verifikaci a biometrický systém**.

Nejprve se věnujme ale historii biometrie.

### 2.1 Historie



Používání biometrických vlastností je známo již dávno. V podstatě používáme denně biometrické rozpoznávání – ostatní lidi jsme schopni rozpozнат podle hlasu, obličeje, způsobu chůze atd. Všechny tyto informace jsou biometrickými vlastnostmi lidí, můžeme je zaznamenat a poté zpracovat.

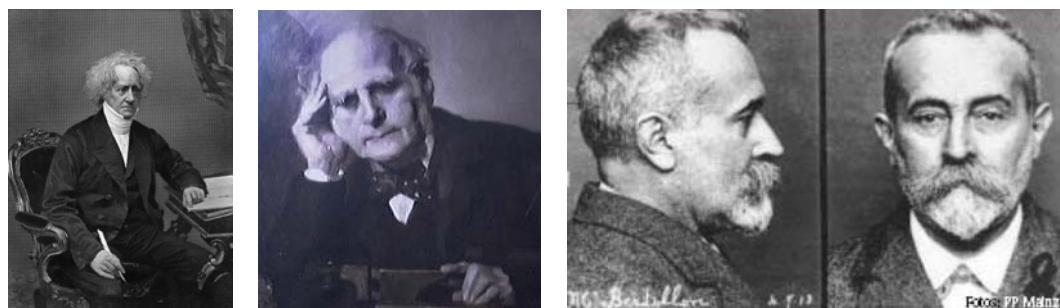


Dochované informace o použití biometrie jsou z Číny ze 14. století. Jedná se ale nepřímo o důkazy biometrie – dochované kresby na skalních stěnách znázorňovaly strukturu podobnou otiskům prstů, nebo se na keramice nacházely otisky prstů autora (možná jako důkaz o autorství).

První průkazné důkazy o použití biometrie pochází z 19. století našeho letopočtu. V tomto období se začaly používat otisky prstů v kriminalistice. Konkrétně:

- 1858 - **W.J. Herschel** (Obr. 2.1.1a) byl koloniálním úředníkem v Indii a začal používat otisky prstů u zaměstnanců dráhy pro stvrzení jejich identity (viz kapitola 2.2). Většina z tamních dělníků neuměla číst a psát a tudíž bylo nemožné od nich očekávat podpis při přebírání výplaty. Pan Herschel nechal každého dělníka otisknout na originál výplatní pásky jeho palec, čímž byla stvrzena identita pracovníka a zároveň i právoplatné převzetí peněz.
- 1865 - **Francis Galton** (Obr. 2.1.1b) přišel se studií o dědičnosti fyzických vlastností (originální název: „*Hereditary talent and character*“), ve které rozebírá skutečnost, že děti dědí od rodičů některé jejich vlastnosti, mezi nimiž mohou být jak fyzické charakteristiky, tak i vlastnosti jednání.
- 1869 - **Francis Galton** je spoluzařadatelem vědy zvané eugenika, což je nauka o dědičných chorobách. Tento obor vychází z jeho předchozí práce.
- 1875 - **Francis Galton** se stává zakladatelem výzkumu dvojčat.
- 1880 - **Francis Galton** přichází s vědním oborem antropometrie (pojem bude vysvětlen v kapitole 2.1.1).
- 1882 - **Alphonse Bertillon** (Obr. 2.1.1c) se zabývá postupem zvaným Bertillonáž [Hau04] (pojem bude vysvětlen v kapitole 2.1.1) již od roku 1879. Jedná se v podstatě o antropometrii.
- 1892 - **Francis Galton** vydává knihu „*Fingerprints*“, z které vychází zavedení daktyloskopie (viz kapitola 5) do praxe v roce 1900. V následujícím roce po 1892 porovnává Galton daktyloskopii s antropometrií. Roku 1894 dochází k závěru, že obě metody jsou dobré a spolehlivé, proto obě doporučuje k praktickému používání.

- 1896 - Dochází k zavedení daktyloskopie (viz kapitola 5) jako identifikačního systému v Argentině.
- 1900 - **Francis Galton** prosazuje daktyloskopii (viz kapitola 5). Prokázal neměnnost a jedinečnost reliéfů kůže na prstech (dnes nazývané papilárními liniemi). Daktyloskopie je zavedena do policejní praxe.
- 1924 - V tomto roce došlo k založení oddělení identifikace otisků prstů u FBI (*Federal Bureau of Investigation*).
- 1965 - Poprvé použit daktyloskopický systém AFIS (*Automated Fingerprint Identification System*, viz kapitola 5) s 810 tisíci otisky prstů.
- 1971 - Byl publikován první článek k rozpoznávání obličeje.
- 2000 - Systém AFIS u FBI obsahuje celkem 47 milionů deseticek otisků prstů (z každé ruky všechny otisky prstů). V průměru dojde k 50 tisícům prohledávání denně. Reakce na vzdálené vyhledání v databázi činí přibližně 2 hodiny.



Obrázek 2.1.1: a) W.J. Herschel ; b) Francis Galton ; c) Alphonse Bertillon

### 2.1.1 Antropometrie



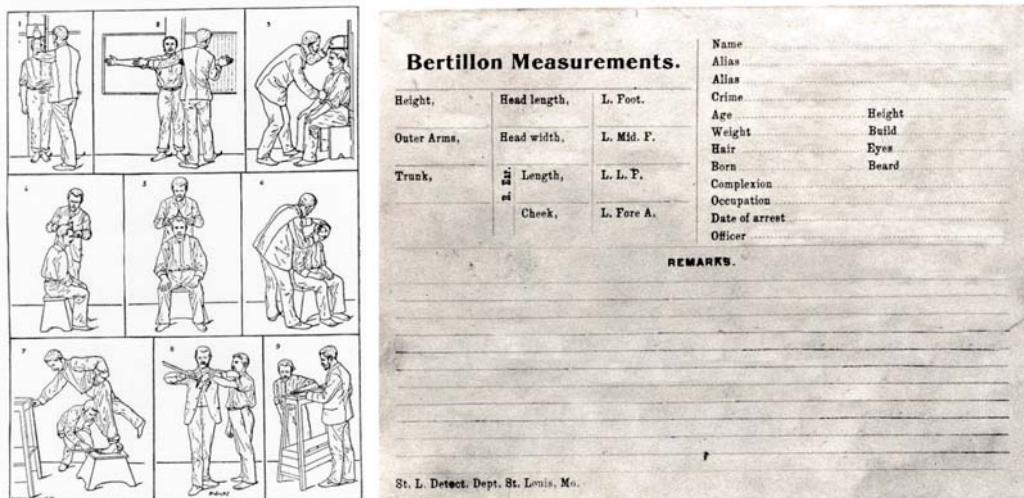
Pojem antropometrie je shodný s pojmem Bertillionáž [Hau04, Ihm05]. Oba pojmy označují metodu záznamu různých lidských rozměrů a jejich následnému použití k identifikaci nebo verifikaci (viz kapitola 2.2) osoby. V rámci antropometrie bylo prokázáno, že

- 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 (příp. verifikovat).

Pro měření bylo použito 11 tělesných rozměrů (Obr. 2.1.2):

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



Obrázek 2.1.2: Měření tělesných rozměrů (antropometrie) + karta pro jejich zápis

## 2.2 Identita, Identifikace, Verifikace

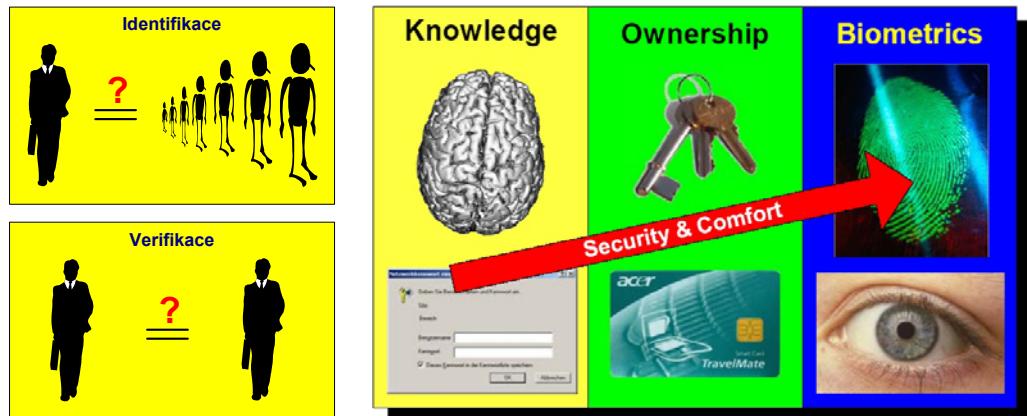
Lidé automaticky rozpoznávají u jiných např. obličej, postavu, rty a jejich pohyby, hlas a jeho intonaci se zabarvením, pohyby (kupř. při chůzi), písmo, podpis atp. Jedná se o automatické rozpoznávání, které probíhá v našem mozku (obdobně je tomu při strojovém rozpoznávání).

Na čem je ale založeno naše rozpoznání jiných? Je založeno na jednoznačné identitě jedince. **Identita** (*identity*) je jednoznačná charakteristika každého z nás. Je ovšem třeba rozlišovat pojem fyzické a elektronické identity. **Fyzickou identitu** máme pouze jednu. Tato identita je definována naším vzhledem a chováním. Na světě by neměl existovat člověk, který má shodnou fyzickou identitu (např. DNA je i u jednovaječných dvojčat odlišná!). U **elektronické identity** to ovšem neplatí. V elektronickém světě si můžeme vytvořit identit kolik chceme (např. účty na free e-mailových portálech).

K pojmu identita se váží další dva pojmy – identifikace vs. verifikace (Obr. 2.2.1a). **Identifikace** (*identification*) slouží ke zjištění identity osoby. Jedná se o situaci, kdy osoba zadá systému svoji biometrickou vlastnost, ale nesdílí mu svoji identitu. Úkolem systému je pak rozpoznání identity uživatele. Dojde k porovnání vzorku ze vstupu s celou databází vzorků, přičemž výstupem je buď nalezená identita a nebo „výsledek nenalezen“. Tento proces je časově relativně náročný, zejména u rozsáhlějších systémů, které obsahují velké množství registrovaných osob (v takových případech se používá rozčlenění databáze na podkategorie – např. databáze otisků prstů je rozdělena podle tříd otisků prstů a teprve v dané podtřídě, ke které otisk prstu na vstupu náleží, proběhne prohledávání). Identifikaci se také říká porovnání 1:N nebo porovnání 1: MANY. Příkladem systému pro



identifikaci mohou být např. daktyloskopické systémy (AFIS), databáze azylantů, registrace nových uživatelů (zde se musí prověřit, zda uživatel s novou elektronickou identitou již není v databázi registrován pod jinou elektronickou identitou – prověření proběhne na základě fyzické identity). Na obrázku 2.2.2a je schematicky znázorněna identifikace – prohledává se celá databáze motýlů (v obrázku).

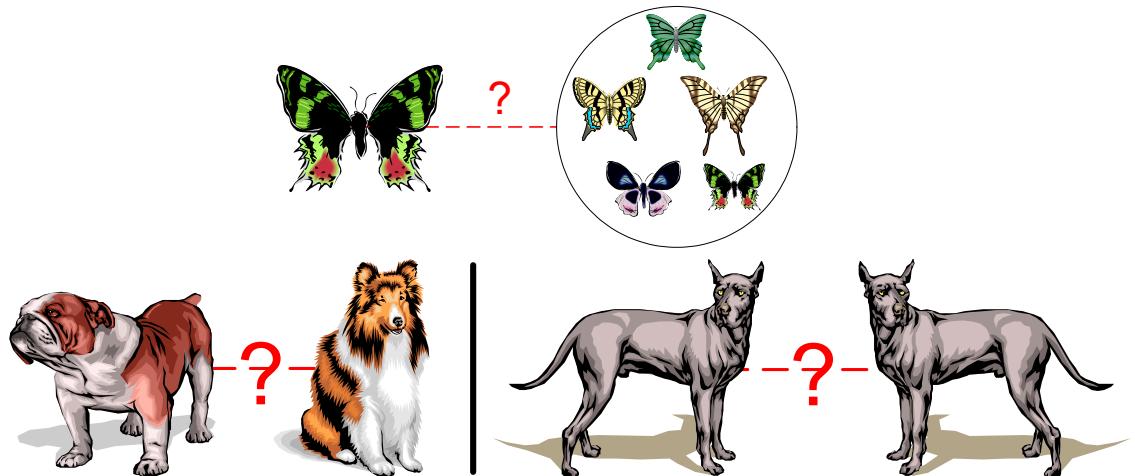


Obrázek 2.2.1: a) Identifikace versus verifikace ; b) Způsoby potvrzení identity



Odlišným přístupem je **verifikace** (*verification*). V tomto případě uživatel (osoba) sdělí systému svoji elektronickou identitu a na základě ní dojde k ověření fyzické identity. Jelikož uživatel sdělil svoji identitu hned na začátku, je v databázi vyhledán jeho záznam obsahující biometrická data. Pokud záznam neexistuje, je přístup uživatele automaticky zamítnut (stejně jako u neexistující e-mailové adresy). Je-li ale záznam úspěšně nalezen, dojde k porovnání dat a v případě shody je výsledkem „Potvrzeno“, jinak „Nepotvrzeno“ – tj. identita potvrzena či nepotvrzena. Verifikaci se také jinak říká porovnání 1:1, protože dochází k porovnání jedných vstupních dat s jedněmi daty z databáze. Příkladem systému, který provádí verifikaci může být např. přístupový systém, databáze azylantů, e-mailové služby. Na obrázku 2.2.2b je schematicky znázorněna verifikace. V levé variantě je výsledkem „nepotvrzeno“, zatímco v pravé variantě je výsledkem „potvrzeno“ (symetrie není na závadu).

Někdy se můžeme setkat s pojmem **autentizace** (*authentication*). S tímto pojmem se setkáváme často u přístupových systémů (jak do počítačového systému, tak i do prostoru). Při autentizaci systém potvrzuje autentičnost (hodnověrnost) dané osoby. O autentizaci se může jednat jak při verifikaci, tak i při identifikaci. Rozhodnutí o hodnověrnosti uživatele proběhne často na základě jakéhosi prahu, který systém vypočte (např. u přihlašování heslem je autentizace jednoduchou úlohou – systém porovná pouze shodu dvou hesel; naopak u biometrických systémů je úloha poněkud složitější). Při zcizení hesla často ani nezjistíme, že se tak stalo – v podstatě nám nic nechybí.



Obrázek 2.2.2: Znázornění principu a) identifikace (nahoře) ; b) verifikace (dole)



Na obrázku 2.2.1b je znázorněna závislost způsobu prokázání identity na komfortu a bezpečí. Identita je založena na

- něčem co víme („*we know*“),
- něčem co máme („*we have*“),
- něčem co jsme („*we are*“).

Nejnižší zajištění komfortu a bezpečí nabízí něco, co víme (např. tajné tlačítko, předepsaný postup, heslo nebo PIN). Ideou tohoto přístupu je náhodná a lehce zapamatovatelná informace, což v sobě ale skrývá úskalí relativně lehkého získání této tajné skutečnosti nepovolanou osobou. Uvedeme si příklad – slovníkový útok na alfanumerické heslo zabere přibližně 5,5 hodiny [Chi03]. Slovníkový útok na libovolné heslo zabere ca 480 hodin [Chi03]. Volme proto hesla co nejsložitější. To ovšem může znamenat, že heslo zapomeneme, což je druhou nevhodou tohoto přístupu.

Střední míru komfortu a bezpečí nám nabízí něco, co vlastníme (např. klíč, čipová karta, token, RFID-tag). Ideou tohoto přístupu je vlastnictví něčeho, co nemá nikdo jiný. Zde opět existuje varianta získání tohoto majetku nepovolanou osobou, a rovněž i varianta zapomenutí (např. doma na stole). Při krádeži trvá kolikrát delší dobu, než si všimneme, že postrádáme náš majetek, pomocí nějž jsme se chtěli právě přihlásit. Samozřejmě tu existuje i varianta nelegálního okopírování (např. vyčtení dat z elektronické karty).

Z jistého pohledu nabízí nejvyšší míru komfortu a bezpečí biometrie, tj. něco co jsme (např. vzhled, pohyby, chování, projevy v různých situacích). Ideou je skutečnost, že jsme sami nositeli identifikačního klíče. Pravdou je, že biometrickou vlastnost doma nejspíš nezapomeneme, ale přesto může dojít k nelegálnímu okopírování a následnému použití falešné biometrické vlastnosti k přihlášení do systému. Naše otisky prstů zanecháváme téměř všude a vyrobí z otisku prstu umělý prst není až takový problém. Kdekoliv se také může stát, že nás někdo vytíká a může použít naši fotografii k přístupu do systému, který řídí vstup na základě rozpoznávání obličeje.

Problematika identity skrývá ale více. V dřívějších dobách se lidé v menších komunitách znali mezi sebou. S růstem populace a nárůstem mobility jsme se začali



spoléhat na dokumenty a tajemství, které nám slouží k určení identity nějaké osoby z naší komunity (není nyní komunitou vlastně celý svět?). Identifikace (verifikace) osob je v současnosti hlavní částí infrastruktury v různých obchodních sektorech, jako např. bankovnictví, hraniční kontrola, právní záležitosti apod. Otázky, které jsou úzce spojené s identitou individua, mohou znít:

- Je tato osoba skutečně tou, za kterou se vydává?
- Byl tento žadatel u nás již někdy dříve?
- Má mít tento uživatel přístup k našemu systému?



Žijeme nyní v globální společnosti, ve které se vyskytují všechnoschopní a nebezpeční jedinci, kterým nemůžeme již věřit na základě předložených osobních dokladů (problematika falešné identity) – to vede k biometrickým cestovním dokladům (viz kapitola 13). **Krádež identity** je v dnešní společnosti celkem častým jevem. Uvedeme si příklad [Kra05]: Zloděj odcizí kreditní kartu a zároveň se mu podaří získat PIN (např. uhodnutím a nebo zcizením). Zcizeným PINem se úspěšně autentizuje (potvrdí sice elektronickou identitu, ale fyzická již není v pořádku) bankovnímu terminálu a podaří se mu vybrat hotovost. Řešením je zavedení biometrie – autentizace je mnohem složitější než u PINu či hesla. Pro představu [Kra05] – v roce 2002 došlo v USA celkem ke 3,3 milionu krádežím identity (nejen podvody s kreditními kartami), přitom ve stejném roce došlo na celém světě k celkovému počtu 6,7 milionu podvodů s kreditními kartami.

## 2.3 Biometrie, Biometrický systém

Slovo **biometrie** (*biometry*) je původem z řečtiny a skládá se ze slov „*bios*“ a „*metron*“, přičemž slovo „*bios*“ znamená život a slovo „*metron*“ znamená měřítko. Jedná se tedy o jakési „měření života“. V oboru IT označujeme tímto výrazem systém či postup k rozpoznávání vzorů. V biomedicínské oblasti však má slovo biometrie poněkud jiný význam – označuje statistické výpočty v biologii (např. pravděpodobnosti vzniku nové generace po mutování, podklady pro genetické obory apod.).



**Biometrie** (IT) je automatické rozpoznávání lidí na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a charakteristického *chování* (např. podpis, chůze).



K výhodám biometrie řadíme:

- Odrazuje od podvodů
- Zvyšuje bezpečnost
- Nemůže být lehce přenesena či zapomenuta
- Nemůže být ztracena či zkopirována
- Eliminuje pokusy o popření identity
- Zvyšuje pohodlí

Biometrie má však i nevýhody:

- Výstupem je skóre porovnání („*matching score*“)
- Nemůže být anulována v případě prozrazení
- Samotný biometrický systém je napadnutelný
- Nezachovává soukromí

- Nutnost rozpoznávání živosti

Proč je ale biometrie složitá? Ve zpracování biometrických informací pracujeme s problémy, jako např. mezitřídní a vnitrotřídní variabilitu (viz Obr. 2.3.1), segmentace, zašuměný vstup, výkonnost systému (chyby, rychlosť, náklady), jednoznačnost biometrické vlastnosti, fúze více biometrických vlastností, rozšiřitelnost, útoky na biometrický systém, otázky privátních dat apod.



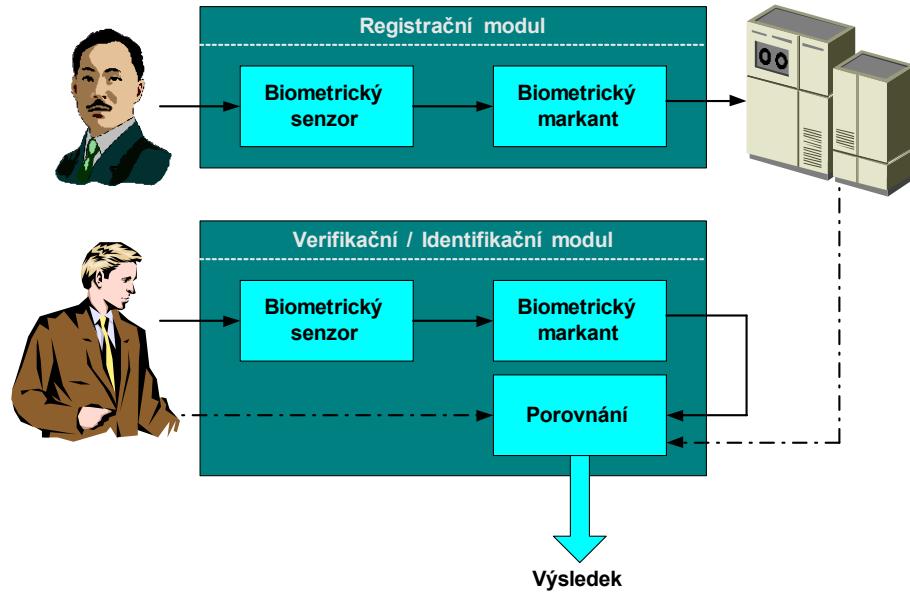
Obrázek 2.3.1: Mezitřídní (nahoře) a vnitrotřídní variabilita (dole)



**Biometrické systém** je znázorněn (zjednodušeně) na obrázku 2.3.2 [Dra01, Pol04]. Skládá se ze dvou modulů (obvykle jsou oba moduly ale integrovány v jednom softwarovém balíku):

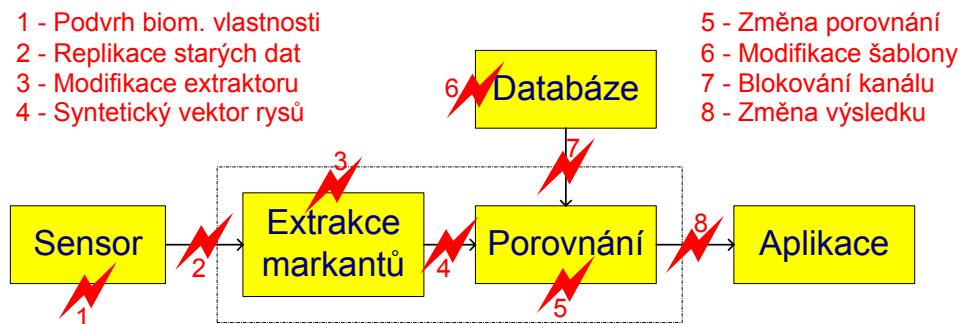
- *Registrační modul*
- *Verifikační / identifikační modul*

V obou modulech se nachází biometrický senzor (viz kapitola 3), který slouží ke získání biometrické informace a jejímu převedení do digitálního světa. V obou modulech se rovněž nachází položka s názvem „biometrický markant“, což jsou vlastně již extrahované rysy z biometrické informace na vstupu (zde pro jednoduchost vynecháváme algoritmické záležitosti). Tento biometrický markant je následně uložen v databázi – to platí pro registrační modul, ve kterém je biometrická informace registrována (jednou před jejím používáním). Verifikační / identifikační modul provede totéž, co registrační modul, pouze neukládá biometrický markant do databáze, ale naopak načítá data z databáze, aby mohl porovnat aktuální biometrický markant s údaji v databázi. Po provedení porovnání obdržíme nějaký výsledek – jeho hodnota závisí na (ne)nalezení shody a příp. operačním módu, tj. verifikace či identifikace.



Obrázek 2.3.2: Biometrický systém [Dra01]

Každý biometrický systém má i svá slabá místa (Obr. 2.3.3). Jak je patrno z obrázku, hned na vstupu může být senzor zmanipulován podvrhem biometrické vlastnosti (např. umělý prst). Komunikace mezi senzorem a extraktorem markantů může být napadena metodou replikace starých dat. Samotný extraktor může být modifikován (jeho funkční princip). Dále komunikace mezi extraktorem markantů a porovnávací jednotkou může být zmanipulována vložením syntetického vektoru rysů, který byl např. odchycen při dřívější komunikaci. Může dojít ke změně dat v databázi (modifikaci šablony). Kanál mezi databází a porovnávací jednotkou může být blokován. Výsledek porovnání může být pozměněn. A v ne- poslední řadě může být podvržen výsledek, který je zasílán aplikaci, která si výsledek porovnání vyžádala.



Obrázek 2.3.3: Slabá místa biometrického systému



Nyní se dostáváme k výčtu **biometrických vlastností (rysů)**, které nám jsou k dispozici. Nejprve musíme provést rozdělení biometrických vlastností do dvou kategorií:



- **Anatomické (fyzické statické) vlastnosti**

- Otisk prstu
- Obličej
- Duhovka oka
- Sítnice oka
- Geometrie ruky
- Dlaň
- Termogram obličeje
- Termogram ruky
- Dentální obraz
- Podpis
- Tvar ucha
- Snímek nehtu
- DNA

- **Dynamické vlastnosti (chování či jednání)**

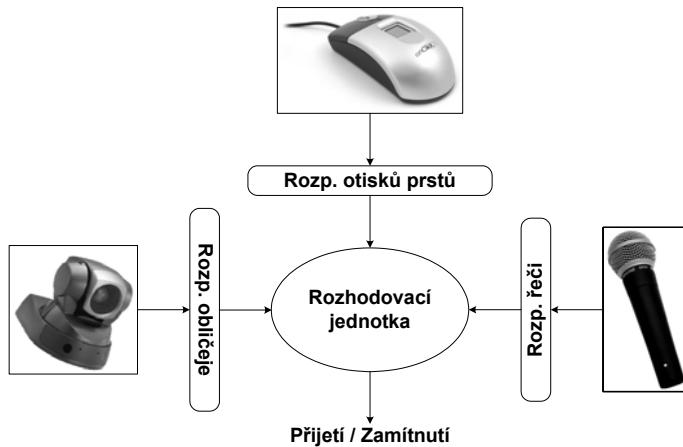
- Hlas / řeč
- Gestikulace obličeje
- Podpis (dynamické vlastnosti)
- Dynamika stisku kláves
- Pohyby rtů
- Chůze

U anatomických vlastností je jeden pevný rys jednou biometrickou vlastností (např. otisk prstu). Tato biometrická vlastnost je vždy přítomna a není lehce ovlivnitelná různými okolnostmi. Metodě analýzy anatomických vlastností se říká *statická metoda*.

Dynamické vlastnosti jsou spojeny s nějakou akcí uživatele. Metodě analýzy dynamických vlastností říkáme *dynamická metoda*. Zde je biometrická vlastnost poměrně lehce ovlivnitelná – každé nasnímání dané biometrické vlastnosti může vést (a často skutečně vede) k naprosto odlišné sadě biometrických vzorků.



V souvislosti s biometrickými vlastnostmi rozlišujeme unimodální a multimodální biometrický systém. **Unimodální biometrický systém** používá pouze jednu biometrickou vlastnost (v praxi se setkáváme téměř výhradně s těmito systémy). Jejich nevýhodou je nižší spolehlivost, ale zároveň také nižší pořizovací náklady. Naopak **multimodální biometrický systém** (viz kapitola 14.4) používá buď více příznaků jedné biometrické vlastnosti (např. statické a dynamické vlastnosti podpisu) a nebo používá více biometrických vlastností (např. rozpoznávání obličeje zároveň s rozpoznáváním duhovky). Tyto systémy mají zvýšenou spolehlivost rozpoznání, ale zároveň vyšší pořizovací náklady, jsou více robustní k falšování a pokusům o útok. Příklad rozhodování u multimodálního biometrického systému je znázorněn na obrázku 2.3.4.



Obrázek 2.3.4: Kombinování biometrických vlastností u multimodálního biometrického systému

**Atributy biometrických vlastností** [Bol04] patří většinou k velmi důležitým kritériím při rozhodování o použití konkrétního systému. Mezi základní atributy biometrických vlastností řadíme tyto:

- **Univerzalita** (každá osoba by měla mít tuto biometrickou vlastnost)
- **Jedinečnost** (žádné dvě osoby nesmí vlastnit stejnou biometrickou vlastnost)
- **Konstantnost** (daná biometrická vlastnost zůstává neměnná s časem)
- **Získatelnost** (biometrická vlastnost je kvantitativně měřitelná)
- **Výkonnost** (biometrická vlastnost se nesmí změnit a ani zestárnout)
- **Akceptace** (ochota lidí pro nasnímání dané biometrické vlastnosti)
- **Bezpečnost proti falšování** (snadnost vytvoření falsifikátu dané biometrické vlastnosti)
- **Finanční náklady na pořízení** (cenové náklady na pořízení systému)

K dalším aspektům můžeme zařadit: použitelnost, údržbu, dostupnost, provedení, anonymitu apod. Velmi důležitým faktorem je spolehlivost – co se stane při změně osvětlení, teploty, make-upu, po zranění či operaci, při použití brýlí nebo čepice, změnou sestřihu, nárůstem vousů či zestánutím.

V níže uvedené Tabulce 2.3.1 je souhrn jednotlivých atributů biometrických vlastností ve vztahu k jednotlivým biometrickým vlastnostem.

Tabulka 2.3.1: Atributy u jednotlivých biometrických vlastností

	Univerzalita	Jedinečnost	Konstantnost	Získatelnost	Výkonnost	Akceptace	Bezpečnost	Finance
<b>Obličej</b>	vysoká	nízká	střední	vysoká	nízká	vysoká	nízká	nízké
<b>Otisk prstu</b>	střední	vysoká	vysoká	střední	vysoká	střední	vysoká	nízké
<b>Geometrie ruky</b>	střední	střední	střední	vysoká	střední	střední	střední	střední
<b>Žily ruky</b>	střední	střední	střední	střední	střední	střední	vysoká	střední
<b>Duhovka</b>	vysoká	vysoká	vysoká	střední	vysoká	nízká	vysoká	vysoké
<b>Sítnice</b>	vysoká	vysoká	střední	nízká	vysoká	nízká	vysoká	vysoké
<b>Podpis</b>	nízká	nízká	nízká	vysoká	nízká	vysoká	nízká	nízké
<b>Hlas</b>	střední	nízká	nízká	střední	nízká	vysoká	nízká	nízké
<b>Termogram</b>	vysoká	vysoká	nízká	vysoká	střední	vysoká	vysoká	vysoké

Typy útoků, které lze aplikovat na biometrický systém:

- „*Low-Force-Attack*“, např. napodobení podpisu, hlasu
- „*Brute-Force-Attack*“, např. použitím speciálních technik



Spolehlivá a automatická identifikace / verifikace osob se stává nutností (příklady: národní identifikační karty, hraniční kontrola, přístupové systémy, e-shopping a další).

Za biometrii neexistuje žádná náhrada – ve smyslu spolehlivé identifikace / verifikace osob.

Biometrické senzory jsou lacné a některé z nich jsou i velmi kompaktní (pro mobilní telefony a laptopy).

Většina biometrických systémů bohužel stále ještě nesplňuje požadovanou přesnost a spolehlivost. Je třeba testování biometrických systémů na rozsáhlých databázích.

Biometrie může vylepšit ochranu našeho soukromí, ale jsou nutné vládní předpisy a směrnice (viz kapitola 13).

Nutný výzkum především v následujících oblastech: nové reprezentace, porovnávací algoritmy, efektivní indexování v databázi, multimodální biometrické systémy, detekce živosti, ochrana šablon, vylepšení chybových hranic, nutné další investice a mnoho práce.



Příklady otázek:

1. Jaký je rozdíl mezi identifikací, verifikací a autentizací?
2. Definujte pojem biometrie.
3. Co je to biometrický systém a z jakých částí se skládá?
4. Jaké biometrické vlastnosti znáte? Uveďte příklady.
5. Jaké atributy biometrických vlastností znáte?



Odpovědi:

1. Strana 5 – 7.
2. Strana 8.
3. Strana 9 – 10.
4. Strana 11.
5. Strana 12.



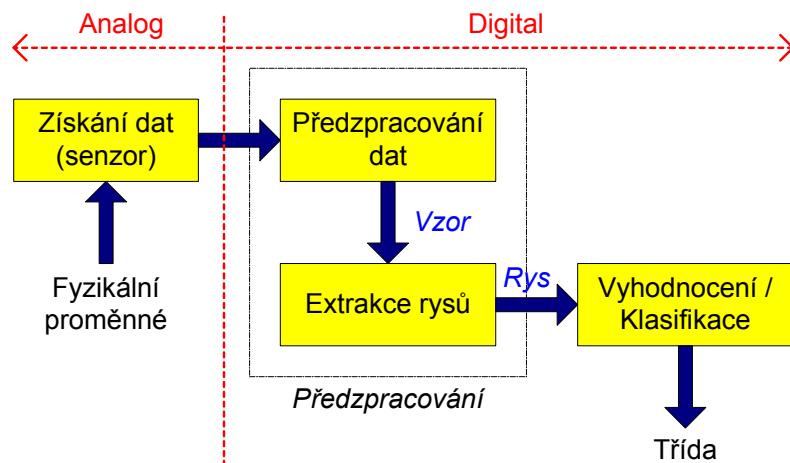
# 3. Teorie zpracování zvukových a obrazových informací

V této kapitole se seznámíme se základními postupy a zařízeními pro získávání biometrických dat a dále s matematickými a statistickými základy, které budeme používat v následujících kapitolách.

## 3.1 Senzory a měření



Nejprve si definujme, co je to senzor. **Senzor** je zařízení, které konvertuje fyzikální jev na elektrický signál. Příklad je uveden na obrázku 3.1.1 – zde je uvedeno rozdelení biometrického systému na analogovou a digitální část, přičemž senzor v podstatě digitalizuje analogová data ze vstupu. Další kroky v digitální části budou osvětleny v následujícím textu.



Obrázek 3.1.1: Rozdelení biometrického systému na analogovu a digitální část

Jaké mají ale senzory detekční schopnosti? Uveďme si relevantní kategorie pro biometrické senzory:

- Biologické
  - Biochemická transformace
  - Spektroskopie
- Chemické
  - Chemické reakce
  - Elektrochemický proces
- Fyzikální
  - Elektromagnetické vlnění
  - Teplota
  - Radioaktivita

**DEF**

Když již máme definován senzor, přejděme k definici dvou pojmu, které se týkají zpracování. **Snímání** (*capturing*) je A/D konverze diskrétní fyzikální charakteristiky, zatímco **vzorkování** (*sampling*) je A/D konverze spojité fyzikální charakteristiky. Příkladem je např. audio (spojitá sekvence skalárních hodnot akustického tlaku), obraz (2D sekvence diskrétních hodnot barev plochy) a nebo video (sekvence audia a obrazu s časovou proměnnou). Snímání můžeme rovněž popsat jako generování počítačové reprezentace fyzikální charakteristiky bez analýzy časových údajů. U vzorkování můžeme rozlišit dvě základní počítačové reprezentace:

- ADC (*Analog-Digital-Converter*), jde o mechanizmus konverze spojitého signálu na sekvenci digitálních vzorků (= vzorkování).
- DAC (*Digital-Analog-Converter*), jde o mechanizmus konverze sekvence digitálních vzorků na spojity signál.

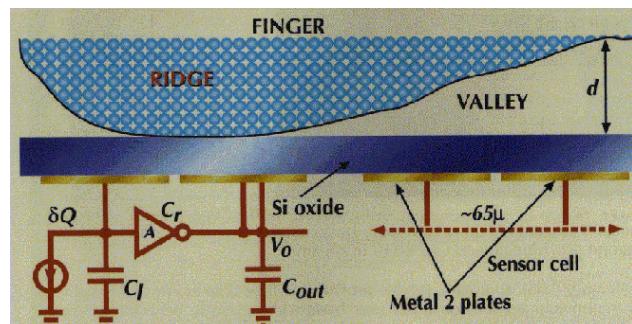
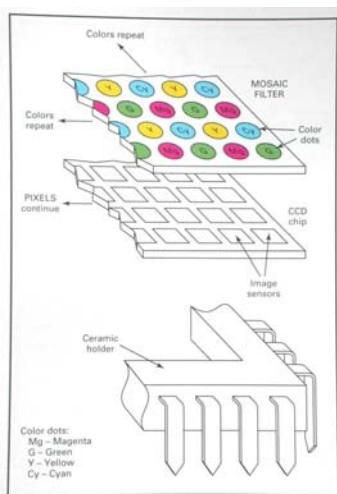
**DEF**

**Vzorek** je sekvence zaznamenaných hodnot amplitudy signálu v konkrétních diskrétních časech.

Při transformaci fyzikální veličiny ze vstupu na její digitální reprezentaci sehrává velmi významnou úlohu **přenosová funkce**, což je specifická charakteristika, kterou vykazuje senzor na výstupu při konverzi A/D. Tato charakteristika bývá většinou nelineární!

U biometrických senzorů existuje mnoho relevantních vlastností, které musíme při jejich výběru zohlednit. Kromě výše zmíněné přenosové funkce k nim patří např. rozlišení (DPI), vzorkovací frekvence (prodleva mezi dvěma vzorky), provozní podmínky (teplota, vlhkost, světlo), reprezentace dat na výstupu (formát) apod.

V různých kategoriích biometrie, dle příslušnosti k biometrické vlastnosti, naleznou použití rozličné senzory, založené na různých fyzikálních principech. Mezi velmi často používané patří optické (princip CCD je znázorněn na obrázku 3.1.2a), dále kapacitní (Obr. 3.1.2b), termické, tlakové, 3D scannery, mikrofony, specializované digitální tablety (složené z aktivního pera, aktivní psací plochy a aktivního displeje) atd.



Obrázek 3.1.2: a) Princip CCD – optické biometrické senzory (vlevo) ; b) Princip kapacitních biometrických senzorů (vpravo)

Při měření (jedná se v podstatě o A/D konverzi) dochází k redukci vstupní informace. Musíme si ale uvědomit, že jak samotná vstupní fyzikální charakteristika, tak i konverzní jednotka a veškeré vedení, jsou ovlivňovány vlivy okolí, což se projevuje jako šum. Zdroje šumu mohou být:

- šum samotného prostředí
- šum senzoru (teplota, elektromagnetické záření)
- kvantizační šum (systematická chyba)
- přenosový šum (analogový kanál)

**DEF**

Při vzorkování provádíme v podstatě kvantizaci analogového signálu, abychom správně reprezentovali ve stanovených intervalech (vzorkovací frekvence) úrovňě daného signálu digitálními hodnotami. Příklad kvantizace je uveden na obrázku 3.1.3. V oblasti biometrie (IT) se setkáváme nejčastěji s **uniformní kvantizací** [Wik06]:

$$Q(x) = \frac{\lfloor 2^{M-1} x \rfloor}{2^{M-1}} \quad (3.1)$$

Hodnota  $2^{M-1}$  se nazývá velikost kvantizačního kroku (*Quantization step size*). Hodnota  $x$  je vstupní analogovou hodnotou (červený průběh v Obr. 3.1.3) a  $Q(x)$  odpovídá výslednému kvantizovanému signálu (v Obr. 3.1.3 modrý průběh).

Dále existuje tzv. **skalární kvantizace** [Wik06]:

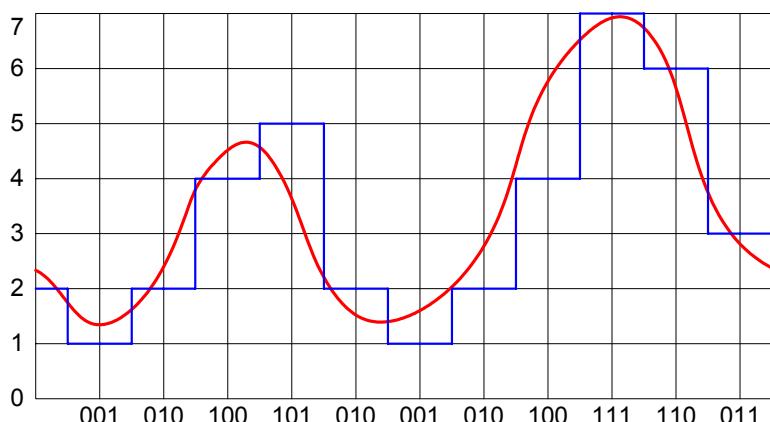
$$Q(x) = g(\lfloor f(x) \rfloor) \quad (3.2)$$

kde  $x \in \mathbb{R}$  a  $f(x)$  a  $g(\cdot)$  jsou partikulárními funkcemi v oboru  $\mathbb{R}$ .

**DEF**

Po spočtení kvantizace (at' už uniformní či skalární) jsme schopni určit pro nás velmi zajímavou hodnotu, a to **poměr signál k šumu** (*Signal-to-Noise-Ratio, SNR*), což nám určuje v jakém poměru stojí šum k signálu. Tuto hodnotu můžeme spočítat následovně [Wik06]:

$$\frac{S}{N_q} \approx 20 \cdot \log_{10}(2^M) = 6,0206 \cdot M \text{ [dB].} \quad (3.3)$$



Obrázek 3.1.3: Průběh kvantizace

Při kvantizaci se pokoušíme korektně rozlišit diskrétní hodnoty. Důležitou roli přitom hraje počet bitů pro uložení jedné hodnoty dat (např. 3 bity odpovídají 8 hodnotám průběhu, 8 bitů odpovídá 256 hodnotám průběhu, a 16 bitů odpovídá 65.536 hodnotám průběhu).



Posledním zajímavým údajem, který se týká výběru vhodného senzoru je jeho rozhraní, tj. jakým způsobem jsme schopni s tímto senzorem komunikovat a získávat od něj data. Mezi typické představitele rozhraní patří: sériová komunikace (např. USB), paralelní komunikace (např. LPT), TCP/IP (nejčastěji pro digitální video), smart karty (nejčastěji pro otisky prstů, v současnosti ale rovněž v biometrických pasech), FireWire (nejčastěji kamery pro rozpoznávání obličeje a rysů oka), BlueTooth. Existují samozřejmě i speciální rozhraní, ale jejich výskyt je řidký.

## 3.2 Matematické a statistické základy

Biometrii můžeme obecně definovat jako metodu pro rozpoznávání vzorů (*pattern recognition*). Biometrické vlastnosti musí splňovat několik kritérií (kromě již dříve zmíněných), a to měřitelnost, variabilitu a musí být rozpoznatelné na základě „biometrického vzoru“ (*biometric pattern*). Chceme-li k biometrii přistupovat jako k metodě rozpoznávání vzorů, je nutné postupovat následovně:

- Definovat model systému rozpoznávání vzorů
- Definovat metody předzpracování (filtrování)
- Vybrat markantní informace
- Klasifikovat tyto informace
- Použít měřítka vzdálenosti pro umístění do správné třídy (vzoru)

Měření slouží k extrakci správného biometrického vzoru, uchování opakovatelných informací k rozlišení a ignorování informací, které takové nejsou. Adekvátní biometrické vlastnosti vyžadují pro automatické zpracování:

- Automatické kvantitativní zaznamenání („*capture*“)
- Časovou efektivnost
- Dostatečný prostor hodnot
- Rozlišovací schopnost
- Cenovou efektivnost

Pro účely měřitelnosti si nyní definujme následující tři pojmy:

**Diskrétní médium** – informace skládající se ze sekvencí jednotlivých elementů bez časové složky (např. text, obraz).

**Spojité médium** – informace nespočívá pouze v jednotlivých hodnotách, ale i v čase jejich výskytu (např. video, hlas, pohyby ruky při psaní).

**Variabilita** – změřené biometrické markanty se budou odlišovat při každém novém nasnímání, i u autentické osoby. Tato variabilita nastává jak změnou používání samotným uživatelem, tak i systematickými chybami (např. vzorkováním). Základními požadavky na variabilitu jsou:

- Nízká vnitrotřídní (*intra-class*) variabilita
- Vysoká meziklasse (inter-class) variabilita

Nízká vnitrotřídní variabilita znamená, že nebude docházet k výrazným změnám mezi jednotlivými vzorky stejného uživatele. Naopak meziklasse variabilita má být vysoká, a znamená, že změny mezi jednotlivými uživateli u dané biometrické informace má být hodně, aby bychom byli schopni jednotlivé uživatele navzájem od sebe odlišit.



Pro rozpoznávání vzorů existují dvě kategorie: *abstraktní* a *konkrétní*. Biometrie spadá do oblasti konkrétního rozpoznávání vzorů, příkladem může být rozpoznávání znaků písma.



Obecný systém pro rozpoznávání vzorů se skládá ze čtyř kroků (Obr. 3.1.1):

- **Získání dat** (transformace fyzikální veličiny pomocí senzoru na digitální reprezentaci)
- **Předzpracování dat** (úprava dat pro extrakci rysů)
- **Extrakce rysů** (nalezení významných vlastností v datech)
- **Klasifikace** (přiřazení do odpovídající kategorie)

Získání dat jsme se věnovali na začátku této kapitoly. K němu se používají senzory, které nám transformují nějakou vstupní veličinu na námi požadovaný signál (nejlépe již digitální). S takovým signálem můžeme pracovat v následujících krocích.

**Předzpracování dat** se používá v případech, kdy je signál zašuměný, data obsahují elementy, které narušují proces klasifikace / rozpoznání apod. Jedná se v podstatě o takové úpravy vstupních dat, které potlačují irrelevantní informace a naopak námi žádané vyzdvihují do popředí. Příkladem předzpracování dat je např. předzpracování obrazu při rozpoznávání otisků prstů. Extrakce markantů z otisku prstu je relativně triviální úlohou pokud je obraz kvalitně prahován a papilární linie jsou ztenčené. Jiným příkladem může být filtrování hluku z pozadí při detekci hlasu.



**Digitální filtr** je zařízení, které přenáší pouze část příchozí energie a může tím změnit spektrální rozložení energie [Dit04]. Ve filtru je implementována filtrovací funkce. Filtrovací funkce je závislá od účelu – příklady:



- Otisk prstu: chtěným výstupem jsou papilární linie, filtr musí potlačit všechno ostatní.
- Detekce řeči: filtr musí potlačit veškerý hluk z pozadí, chtěným výstupem je hlas řečníka.



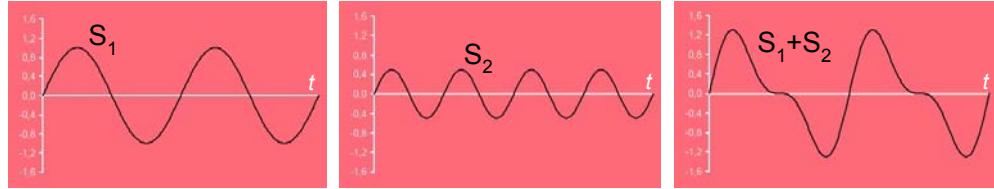
V multimedialní oblasti existuje velké množství filtrů, záleží na cílu jejich uplatnění. Velmi často používanými filtry jsou filtry pro úpravu histogramu obrazu. Vzhledem k tomu, že světlo a zvuk jsou elektromagnetickými oscilacemi (barevné spektrum leží v průměru kolem 380 – 760 THz a zvukové spektrum mezi 20 – 20.000 Hz), provádí filtr takové změny, které stále leží v uvedených rozsazích, ale relevantní informace jsou vyzdvihnuté. Digitální filtry u diskrétního média provádějí spektrální distribuci, zatímco u spojitého média je spektrální distribuce funkcí času. V některých případech je třeba zjednodušit a nebo převzorkovat signál, potom se používají např. lineární splinová interpolace, kubická splinová interpolace, bikuadratická splinová interpolace, Bézierovy křivky a B-spliny.

Hlavní uplatnění v doméně filtrování nachází filtry ve frekvenčním spektru, které jsou založeny především na **Fourierově analýze**. Příkladem vhodného použití je nejen audio (harmonická analýza), ale i zpracování obrazu. Cílem Fourierovy analýzy je transformace signálu z časové reprezentace do frekvenční reprezentace a naopak, přičemž ve frekvenční reprezentaci lze aplikovat celou řadu speciálních filtrů. Dle ideje Fourierovy analýzy je každý signál superimpozicí signálů (Obr. 3.2.1) s proměnnou frekvencí (tzv. Fourierova série) [Dit04]:

$$s(t) = \frac{a_0}{2} + a_1 \cdot \cos(\omega t) + \dots + a_n \cdot \cos(n\omega t) + b_1 \cdot \sin(\omega t) + \dots + b_n \cdot \sin(n\omega t) \quad (3.4)$$

kde  $a_i$  a  $b_i$  jsou Fourierovy koeficienty. Použijeme-li  $A_i = \sqrt{a_i^2 + b_i^2}$  a  $\tan \varphi = \frac{a_i}{b_i}$ , potom:

$$s(t) = \frac{a_0}{2} + A_1 \cdot \sin(\omega t + \varphi) + A_2 \cdot \sin(2\omega t + \varphi) + \dots + A_n \cdot \sin(n\omega t + \varphi) \quad (3.5)$$



Obrázek 3.2.1: Superimpozice signálů (Fourierova analýza)

**DEF**

Definujme si nyní tři formy Fourierovy transformace. Základní formou je **spojitá Fourierova transformace (CFT)**, která je definována takto:

$$f(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F(\omega) \cdot e^{i\omega t} d\omega \quad (3.6)$$

$$f(t) = \frac{1}{\pi} \int_0^{\infty} (a(\omega) \cdot \cos(\omega t) + b(\omega) \cdot \sin(\omega t)) d\omega \quad (3.7)$$



Dále můžeme definovat **diskrétní Fourierovu transformaci (DFT)**:

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) \cdot e^{-\frac{2\pi i kn}{N}} \quad (3.8)$$

$$f(n) = \sum_{k=0}^{N-1} f(k) \cdot e^{\frac{2\pi i kn}{N}}, \quad n = 0 \dots (N-1) \quad (3.9)$$

Na konec si definujme často používanou **rychlou Fourierovu transformaci (FFT)**:

$$x_1(n) = x(2n), x_2 = x(2n+1), \dots, \text{kde } n = 0, 1, 2, \dots, \frac{N}{2} - 1 \quad (3.10)$$

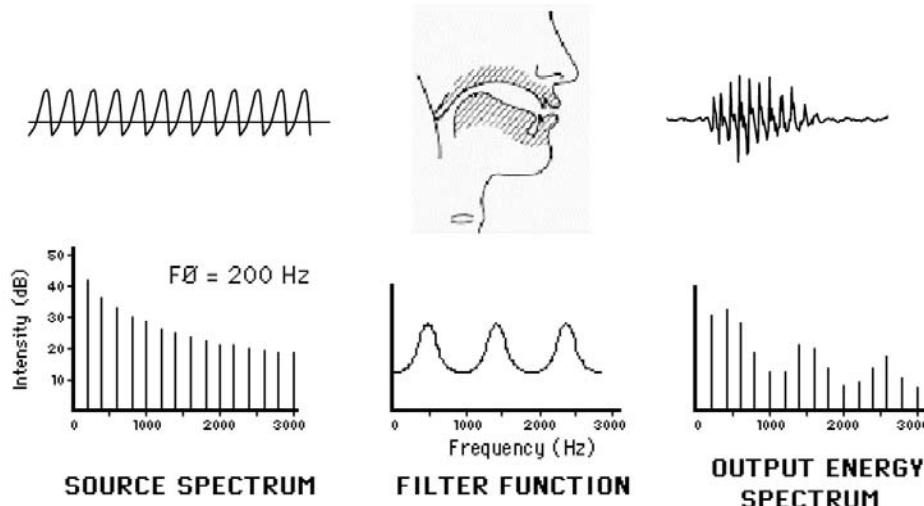
$$X(k) = X_1(k) + W^k \cdot X_2(k), \quad 0 \leq k \leq \frac{N}{2}$$

$$X(k + \frac{N}{2}) = X_1(k) - W^k \cdot X_2(k), \quad 0 \leq k \leq \frac{N}{2}, \quad W = e^{-\frac{2\pi i}{N}} \quad (3.11)$$

Nejen ve frekvenční doméně se dále setkáme s pojmem **histogram**, což je dekompozice diskrétních funkcí do frekvenčního rozložení (např. řeč).

Příklad aplikace filtru ve frekvenční doméně je uveden na obrázku 3.2.2 (zcela vlevo jsou hlasivkové pulsy; uprostřed je filtrová funkce vokálního traktu a zcela vpravo je filtrovaný řečový signál). Řeč je v podstatě spojitým průběhem vokálního traktu.

Filtry pro frekvenční oblast zmíníme vždy v jednotlivých kapitolách – pro různé biometrické vlastnosti se pochopitelně liší i filtry.



Obrázek 3.2.2: Příklad filtru ve frekvenční doméně

**DEF**

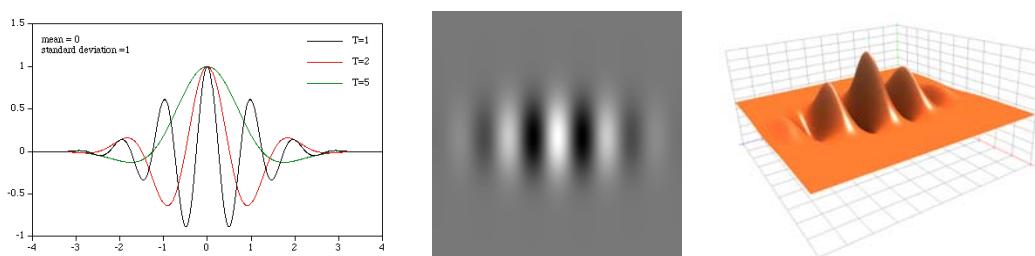
2

Zajímavým filtrem, který nachází v oblasti biometrie uplatnění celkem často, je tzv. **Gaborův filtr**, který je založen na Gaborově funkci. **Gaborova funkce** [Bou02] je založena na pozorování, že jednoduché části v pozorovací rovině jsou modelově popsatelné pomocí Gaborových funkcí. Dále může být obraz dekomponován do orientačních komponent ležících v určitém frekvenčním rozsahu. Gaborova funkce může být interpretována jako kaskádní Gaussovská Fourierova transformace (v časové rovině). 2D Gaborovu funkci můžeme definovat takto:

$$g(x) = \frac{1}{2\pi\sigma_x\sigma_y} \cdot e^{\left(\frac{1}{2}(t_x A x + j \cdot t_y(k_0 x))\right)} \quad (3.12)$$

$$\text{kde } A = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \cdot \begin{pmatrix} \sigma_x^{-2} & 0 \\ 0 & \sigma_y^{-2} \end{pmatrix} \cdot \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \quad (3.13)$$

kde  $k_0$  je modulační funkce. Tato funkce je založena na frekvenci a orientaci  $\Delta\phi$ . Příklad Gaborova filtru je uveden na obrázku 3.2.3, kde je reprezentace od 1D až po 3D. Pomocí těchto funkcí se dají dobře určovat pole orientací – např. při zpracování otisků prstů se aplikuje tento filtr pro zjištění směru papilárních linek a vzájemné se tato informace využívá ke klasifikaci, tj. do které třídy daný otisk prstu náleží (více bude k tomuto tématu popsáno v kapitole 5).



Obrázek 3.2.3: Gaborova funkce pro 1D (vlevo), 2D (uprostřed) a 3D (vpravo)



Nyní se dostáváme k významné oblasti – extrakci a klasifikaci rysů. Extrahujeme-li rysy, očekáváme od nich, že budou mít následující čtyři vlastnosti:

- *Diskriminace* – signifikantně odlišné hodnoty pro objekty patřící do jiné třídy.
- *Spolehlivost* – podobné hodnoty pro objekty stejné třídy.
- *Nezávislost* – žádná korekční závislost.
- *Malý počet* (dimenze) – důvodem je komplexita systémů na rozpoznávání vzorů; učení klasifikátorů narůstá exponenciálně; rušivé rysy mohou degradovat celkovou schopnost systému.

Rysy mohou být determinovány (klasifikovány) např. na základě reprezentace dat (signály, obrazy, struktury, ...) nebo účelu (globální / lokální analýza). Jako příklady rysů si uvedeme frekvenční spektrum (charakteristiky hlasu), waveletové koeficinenty (kód duhovky oka), metriku (geometrické vlastnosti písma) a strukturu (markanty otisků prstů).



Abychom byli schopni určit kategorie (třídu), do které daná biometrická vlastnost (její rysy) patří, musíme provést proces klasifikace. **Klasifikace** je proces, kdy se pro daný vzor hledá jeho obraz v prostoru. Formálně můžeme definovat klasifikaci takto: nechť máme  $N$  rysů získaných z každého vstupního vzoru, je to každá množina rysů  $\Omega$ , referovaná jako vektor rysů  $X$  uvnitř prostoru rysů  $\Omega$ . Rozdělení prostoru rysů  $\Omega$  na vzájemně disjunktní oblasti provedeme tak, že každá oblast odpovídá patřičné třídě vzoru. V biometrii se můžeme setkat s následujícími třemi druhy klasifikátorů:

- *Neparametrické klasifikátory*
  - Klasifikátor minimální vzdálenosti (*minimum distance*)
  - Klasifikátor nejbližšího souseda (*nearest neighbour*)
- *Parametrické klasifikátory*
  - Bayesův klasifikátor

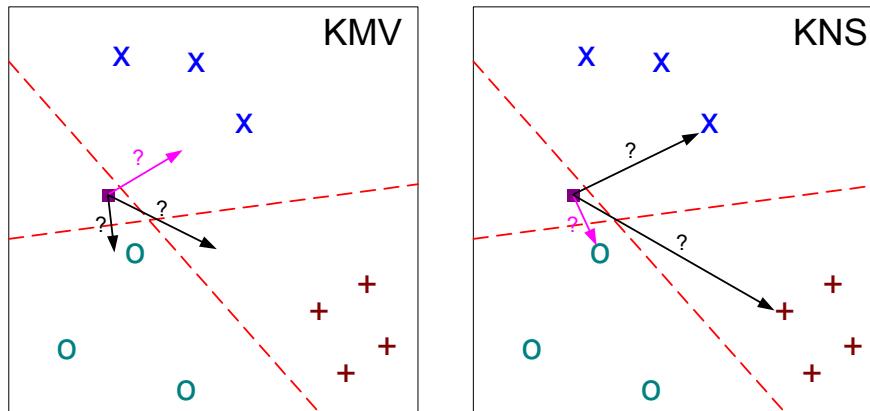


**Klasifikátor minimální vzdálenosti (KMV)** (obrázek 3.2.4a): máme jeden referenční vektor  $R_i$  pro každou třídu  $\omega_i$ :

$$X \sim \omega_i \quad \text{if} \quad |X - R_i| = \min_{1 \leq k \leq N} |X - R_k| \quad (3.14)$$



kde  $|X - R_k|$  je definovaná vzdálenost mezi  $X$  a  $R_k$ .



Obrázek 3.2.4: a) Klasifikátor minimální vzdálenosti (vlevo); b) Klasifikátor nejbližšího souseda (vpravo)

**DEF**

**Klasifikátor nejbližšího souseda (KNS)** (obrázek 3.2.4b): pro každou třídu  $\omega_i$  máme jednu množinu referenčních vektorů  $R_i$ . Nechť  $R_1, \dots, R_N$  jsou (v tomto pořadí) množiny referenčních vektorů asociované k třídám  $\omega_1, \dots, \omega_N$  a nechť referenční vektory v  $R_j$  jsou označeny jako  $R_j(k)$ , potom můžeme definovat vzdálenost mezi  $X$  a  $R_j$  takto:

$$d(X, R_j) = \min_{k=1 \dots u_j} |X - R_j^{(k)}| \quad (3.15)$$

kde  $u_j$  je číslo referenčního vektoru v množině  $R_j$ .

**DEF**

**Bayesův parametrický klasifikátor** [Maj99] je založen na Bayesově teorému:

$$P[X_i | Y] = \frac{P[Y | X_i] \cdot P[X_i]}{\sum_j P[Y | X_j] \cdot P[X_j]} \quad (3.16)$$

kde  $P[X_i]$  je apriorní pravděpodobnost třídy  $X_i$ ,  $P[Y | X_i]$  je pravděpodobnostní funkce  $X_i$  v závislosti na  $Y$  a  $P[X_i | Y]$  je výsledná pravděpodobnost, že  $Y$  patří do  $X_i$ . Největší pravděpodobnost poskytuje *naivní Bayesův teorém* [Maj99]:

$$P[X_i | Y] > P[X_j | Y], \forall i \neq j \quad (3.17)$$

**Vzdálenost** slouží jako metrika k rozlišování rysů / charakteristik. Důležité metriky pro biometrii:



- *Minkowského metrika*:  $d_{ij} = \left[ \sum_k |x_{ik} - x_{jk}|^r \right]^{\frac{1}{r}}$  (3.18)

o pro  $r = 1$  se jedná o „*City-Block-Metric*“

o pro  $r = 2$  se jedná o Eukleidovskou vzdálenost

- *Mahanalobisova metrika*:  $r^2 = (x - m_x)' \cdot C_x^{-1} \cdot (x - m_x)$  (3.19)

o kde  $m_x$  je vlastní vektor všech referenčních vektorů a  $C_x$  je kovariacioní matice pro  $x$ .

o Tato metrika normalizuje vzdálenosti.

o Pro jednotkovou matici  $C_x \sim$  Eukleidovské vzdálenost.

 **$\Sigma$** 

V této kapitole jsme se dozvěděli jakým způsobem fungují senzory a co vlastně můžeme měřit. Následoval popis procesu úpravy vzorků ze senzoru (snímkování / vzorkování). Dnešní inteligentní senzory dávají na výstupu často již digitální signál. Ovšem u samotného senzoru je třeba dbát na jeho přenosovou funkci, která může velmi silně ovlivnit výsledek – pro některé oblasti (např. frekvenční závislost) je vhodné použít jiný typ senzoru, než který jsme zvolili – to rozeznáme právě na základě přenosové funkce.

V matematických a statistických základech jsme se věnovali fázi předzpracování dat, tj. aplikaci různých filtrů. Mezi nejčastěji používané filtry patří ty, které fungují ve frekvenčním spektru, jsou tedy spojené s Fourierovou transformací.

Na závěr jsme se věnovali klasifikátorům, což jsou obecně základy každého biometrického systému – nový vzorek (biometrickou informaci) se snažíme zařadit do prostoru předchozích vzorků, tj. definovat skupinu sobě podobných vzorků, které opravdu patří k sobě (tj. pocházejí od stejné osoby).



Příklady otázek:

1. Jaký je rozdíl mezi snímkováním a vzorkováním?
2. Co je to spojité a diskrétní médium?
3. Definujte digitální filtr.
4. K čemu slouží Gaborův filtr?
5. Jaký je rozdíl mezi KMV a KNS?



Odpovědi:

1. Strana 15.
2. Strana 17.
3. Strana 18.
4. Strana 20.
5. Strana 21 – 22.



## 4. Hodnocení spolehlivosti a kvality biometrických systémů

V předchozí kapitole jsme si definovali významné pojmy, které se týkají jak verifičních / identifikačních procesů, tak i jejich pozadí, tzn. jakým způsobem se vlastně porovnání provádí (klasifikace / rozpoznání vzorů) a jak vlastně můžeme provést rozhodnutí – na základě metrik. V této kapitole si malíčko doplníme statistické základy a dostaneme se k velmi významné části – hodnocení spolehlivosti a kvality biometrických systémů.

### 4.1 Statistické základy pro hodnocení

V biometrii rozlišujeme následující typy klasifikace:

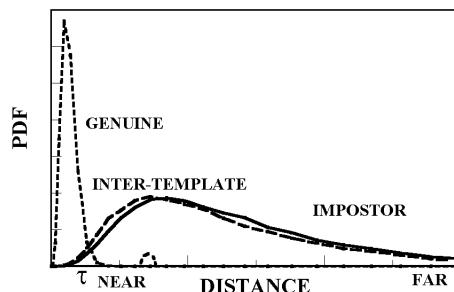
- *Verifikace* – patří množina rysů  $R$  k osobě  $O$  z celkového počtu osob  $N$ ?
- *Identifikace* – která množina rysů  $R$  z celkového počtu osob  $N$  patří k osobě  $O$ ?
- *Rozpoznávání* – které třídě patří sémantický obsah rysů  $R$ ?



Ideálním stavem je žádná chyba, což je prakticky nemožné. Problémem je změření přesnosti, tedy distribuce vzdáleností rysů (viz obrázek 4.1.1):



- *Genuine Distribution* – Rozložení právoplatných rysů
- *Impostor Distribution* – Rozložení neprávoplatných rysů
- *Inter-Template Distribution* – Rozložení vzdáleností rysů mezi šablonami různých osob



Obrázek 4.1.1: Distribuce vzdáleností rysů



Při testování biometrických systémů se ptáme, kolik testů musí být provedeno, aby mohly být vysloveny signifikantní závěry? Ke zjištění množství dat se používá (krom jiného, viz strana 32) binomické rozložení pravděpodobnosti. **Binomické rozložení** udává diskrétní rozdělení pravděpodobnosti  $P_p(n, N)$  pro dosažení přesně  $n$  úspěchů z  $N$  Bernoulliho pokusů (*true* je s pravděpodobností  $p$  a *false* s  $(1-p)$ ). Výpočet [Wei05]:

$$P_p(n, N) = \binom{N}{n} \cdot p^n \cdot q^{N-n} \quad (4.1)$$

kde  $\binom{N}{n}$  je binomický koeficient.

U rozsáhlých databází může být binomické rozložení nahrazeno **standardním normálním rozložením** [Wei05]:

$$f_z(z) = \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{z^2}{2}}, \text{ kde } z = \frac{x - \hat{x}}{\sigma} \quad (4.2)$$

K zajištění specifické úrovně důvěrnosti (chybovost menší než  $\tau$ ) se specifickou odchylkou  $\sigma$  pro hypotézu  $h$  (chyba  $\leq h$ ) lze psát:

$$n_\tau = \frac{Z_\tau^2}{\sigma^2} \cdot h \cdot (1 - h) \quad (4.3)$$

V tabulce 4.1 lze nalézt příklady parametrů pro výše zmíněné výpočty u různých bezpečnostních tříd.

Tabulka 4.1: Parametry  $\sigma$ , **FAR** a  $n_\tau$  pro různé bezpečnostní třídy



Bezpečnostní třída	Horní hranice ( $\sigma + \text{FAR}$ ) [%]	$\sigma$ [%]	<b>FAR</b> [%]	$n_\tau$
Nízká	15,0	5,0	10,0	138
	10,0	2,0	8,0	707
	5,0	1,0	4,0	1475
Střední	4,9	0,9	4,0	1821
	3,6	0,6	3,0	3105
	2,5	0,5	2,0	3012
Vysoká	1,9	0,4	1,5	3547
	1,5	0,5	1,0	1521
Velmi vysoká	1,0	0,3	0,7	2967
	1,0	0,2	0,8	7622
	0,5	0,1	0,4	15305
	0,3	0,1	0,2	30671



Velmi důležitým pojmem je **entropie**, což je množství informace v konkrétní biometrické vlastnosti. Čím větší entropii daná biometrická vlastnost nabízí, tím je lépe předurčena k využití v praxi. Vždy je třeba ale nalézt jakési optimum, tj. máme-li příliš málo entropie, nejsme schopni rozlišit od sebe dva jedince, a naopak, máme-li silně entropickou biometrickou vlastnost, může se nám stát, že její variabilita zapříčiní občasné nerozpoznání právoplatného uživatele. Uvedeme si nějaké příklady – např. kód duhovky (Daugmanův algoritmus) vykazuje 2048 bitů, otisk prstu přibližně 243 – 8075 bitů (teoreticky  $3,23 \cdot 10^{616}$  /  $6,57 \cdot 10^{2430}$ , ovšem jaká je realita?). Dalším příkladem může být pravděpodobnost shody dvou různých duhovek  $\sim 10^{-52}$  či otisků prstů  $\sim 10^{-7}$  až  $10^{-59}$  (závislé na modelu).



**Variabilita** je měřítkem rozptylu statistické distribuce. Je-li  $\mu$  střední hodnotou distribuce náhodné proměnné  $X$ , potom  $I(X) = E[(X-\mu)^2]$ . Tato hodnota může udávat jak blízko je odhadovaný výsledek skutečné hodnotě.

**Interval důvěrnosti** (např. 95%) pro parametr  $x$  se skládá z dolní hranice  $L$  a horní hranice  $U$  tak, že pravděpodobnost skutečné hodnoty leží v tomto intervalu, tj.  $P(x \in [L, U]) = 95\%$ .

Rozlišujeme dva typy chyb:

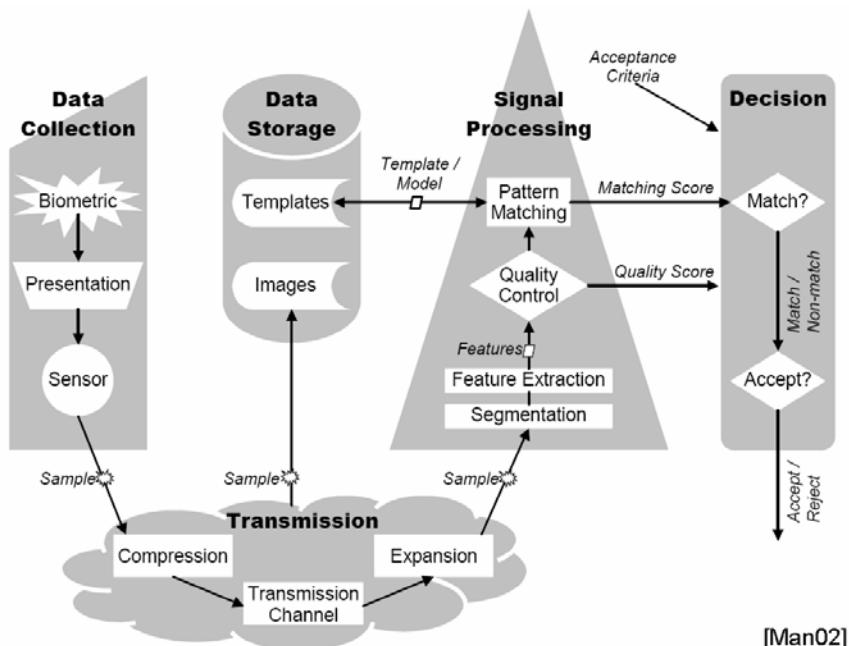
- **Chyba typu I:** Odmítnutí správné hypotézy.
- **Chyba typu II:** Přijetí chybné hypotézy



Celková výkonnost biometrického systému je dána vlastnostmi jako univerzálnost, přesnost, rychlosť a paměťové možnosti. Faktory jako cena a lehkost použití také samozřejmě ovlivňují celkovou výkonnost systému. Biometrické systémy nejsou perfektní – mohou chybně přijmout útočníka jako platného uživatele (chybné přijetí) a nebo odmítat platného uživatele jako útočníka (chybné odmítnutí).

## 4.2 Porovnání a jeho chyby

Nejprve se podívejme na strukturu obecného biometrického systému (Obr. 4.2.1). Základními jednotkami, z nichž se takovýto systém skládá jsou: sběr dat, uložení dat, zpracování signálů, rozhodnutí a přenosy mezi jednotlivými částmi. Kromě již zmíněných útoků na biometrický systém (viz kapitola 3) musíme brát v potaz i nedokonalost samotných biometrických vlastností. Když sečteme tuto nedokonalost s pokusy o průnik do systému, přicházíme k chybám, které si probereme v této kapitole.



Obrázek 4.2.1: Struktura obecného biometrického systému

Nejprve se ale podívejme na různé formy **tvrzení o identitě**, tj. co tvrdí uživatel, co je pravda a jak na to reaguje systém:

- *Pozitivní tvrzení o identitě* – uživatel tvrdí, že je již registrován v daném biometrickém systému. Např. se jedná o běžné přístupové systémy.
- *Negativní tvrzení o identitě* – uživatel tvrdí, že ještě není registrován v daném biometrickém systému. Např. se jedná o systémy sociální podpory / uprchlíků.
- *Explicitní tvrzení o identitě* – uživatel musí zadat svoji identitu (např. smart kartou) a ta je bud' potvrzena a nebo vyvrácena. Porovnání 1:1.
- *Implicitní tvrzení o identitě* – identita uživatele je vyhledána a předložena. Porovnání 1:N.

- Tvrzení o identitě právoplatným uživatelem.
- Tvrzení o identitě útočníkem.



Po zpracování dat (např. filtraci a úpravě vstupních dat) přecházíme do kroku extrakce, kdy jsou ze vstupních biometrických dat extrahovány významné rysy. Tento extrahovaný vzorek (množina rysů) je porovnán se šablonou (uloženou např. v databázi či na čipové kartě) – výsledkem je **skóre porovnání** („*Matching Score*“), tj. míra shody. Skóre porovnání udává kvantifikovanou podobnost mezi vzorkem a šablonou. Označujeme ho jako  $s$ . Skóre porovnání je v podstatě metrikou (leží v nějakém intervalu), přičemž můžeme definovat různé metriky, např.  $<0,1> \sim <0\%, 100\%>$ , tedy  $<\text{neshoda}, \text{shoda}>$ .

Porovnání uvnitř biometrického systému je založeno na prahu  $T$ :

- If  $(s) < (T)$  then Reject
- If  $(s) \geq (T)$  then Accept

Výsledkem je buď přijetí (*accept*) či odmítnutí (*reject*), což odpovídá procesu autorizace. Ukázka oblastí pro přijetí a odmítnutí, s nastaveným prahem, je uvedena na obrázku 4.2.2.



Obrázek 4.2.2: Oblast přijetí (*accept*) a odmítnutí (*reject*) v závislosti na prahu  $T$

Možné chybové stavy při porovnání:

- Dva vzory od dvou odlišných osob jsou rozpoznány (klasifikovány) jako shodné  $\Rightarrow$  **chybná shoda** (*False Match*).
- Dva vzory (nasnímané ve dvou různých okamžicích) od stejné osoby jsou rozpoznány (klasifikovány) jako odlišné  $\Rightarrow$  **chybná neshoda** (*False Non-Match*).

V literatuře, týkající se biometrických systémů, se ujaly pojmy:

- „*False Match*“  $\sim$  „*False Acceptance*“
- „*False Non-Match*“  $\sim$  „*False Rejection*“
- Projev na verifikaci (identifikaci):
  - Osoba A je přijata jako A  $\Rightarrow$  **správné přijetí** („*True Acceptance*“)
  - Osoba A je odmítnuta jako B  $\Rightarrow$  **správné odmítnutí** („*True Rejection*“)
  - Osoba A je přijata jako B  $\Rightarrow$  **chybné přijetí** („*False Acceptance*“)
  - Osoba A je odmítnuta jako A  $\Rightarrow$  **chybné odmítnutí** („*False Rejection*“)

Z výše uvedených variant odvozujeme následující chybové míry, které jsou velmi významné pro hodnocení biometrických systémů:



### Míra chybného přijetí – FAR

**FAR (False Acceptance Rate)** je pravděpodobnost, že biometrický systém klasifikuje chybně dva odlišné biometrické vzory jako shodné a tím selže při odmítání možného útočníka. **FAR** (Obr. 4.2.3) můžeme spočítat následovně:

**FAR** = Počet shodných porovnání rozdílných vzorů / Celkový počet porovnání rozdílných vzorů



Příklad: Porovnali jsme 5000 duhovek, přičemž byly vždy porovnávány páry, které nepochází od stejné osoby. Přesto jsme obdrželi 67 výsledků, které ležely v oblasti přijetí, tj. vykazovaly shodu. Výpočet **FAR** =  $67 / 5000 = 1,34\%$ .



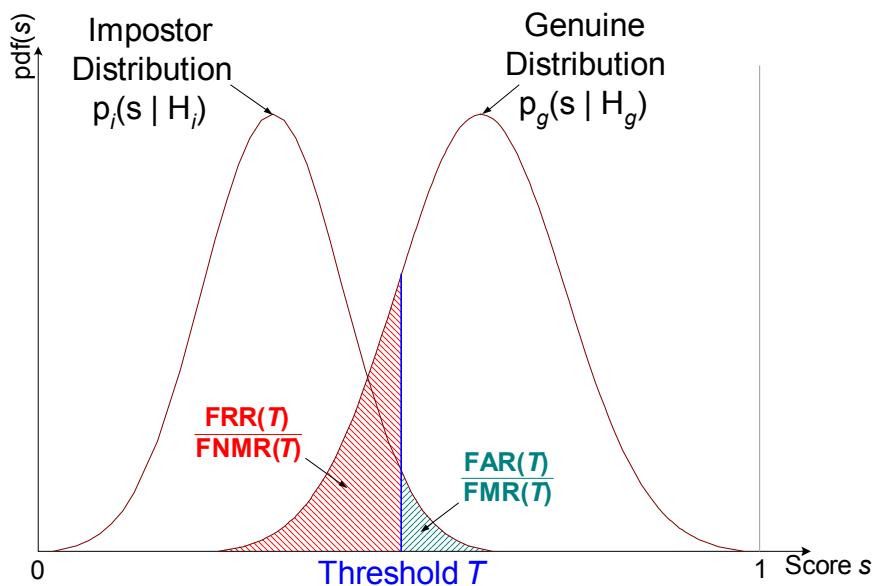
### Míra chybného odmítnutí – FRR

**FRR (False Rejection Rate)** je pravděpodobnost, že biometrický systém klasifikuje chybně dva biometrické vzory od stejné osoby jako odlišné a tím selže při přijetí oprávněného uživatele. **FRR** (Obr. 4.2.3) můžeme spočítat následovně:

**FRR** = Počet porovnání vzorů osoby  $A$  vedoucích k neshodě / Celkový počet porovnání vzorů osoby  $A$



Příklad: Porovnali jsme 200 otisků prstů, přičemž byly vždy porovnávány páry, které pochází od stejného uživatele. Přesto jsme obdrželi 53 výsledků, které ležely v oblasti odmítnutí, tj. vykazovaly neshodu. Výpočet **FRR** =  $53 / 200 = 26,5\%$ .



Obrázek 4.2.3: Chyby **FMR** vs. **FNRM** / **FAR** vs. **FRR**



### **Míra chybné shody – FMR**

**FMR (False Match Rate)** udává podíl chybně akceptovaných osob. Na rozdíl od **FAR** nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (tj. **FTA**, **FTE**). Výpočet **FMR** (Obr. 4.2.3) je definován takto:

$$FMR(T) = \int_0^T p_i(s | H_i) ds \quad (4.4)$$

kde  $T$  je rozhodovací práh,  $H_i$  je výrok „rozdílné“ (vzor a šablona pochází od různých osob),  $p$  je pravděpodobnostní hustota, že výrok v závorce je pravdivý a  $s$  je skóre porovnání.



### **Míra chybné neshody – FNMR**

**FNMR (False Non-Match Rate)** udává podíl chybně neakceptovaných osob. Na rozdíl od **FRR** nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (tj. **FTA**, **FTE**). Výpočet **FNMR** (Obr. 4.2.3) je definován takto:

$$FNMR(T) = \int_0^T p_g(s | H_g) ds \quad (4.5)$$

kde  $T$  je rozhodovací práh,  $H_g$  je výrok „shodné“ (vzor a šablona pochází od stejné osoby),  $p$  je pravděpodobnostní hustota, že výrok v závorce je pravdivý a  $s$  je skóre porovnání.



### **Míra vyrovnaní chyb – EER**

**EER (Equal Error Rate)** je definována podmínkou  $\mathbf{FMR}(T) = \mathbf{FNMR}(T)$ . V praxi se u **FMR** a **FNMR** křivek jedná o diskrétní funkce, tj. přesné určení **EER** není možné. Je tedy možné udat oblast, ve které se obě chybové míry shodují. Při nastavení porovnávacího prahu  $T$  na **EER** bude chybně akceptován stejně jako chybně odmítnut stejný počet osob. Tím je tedy možné nastavit práh tak, aby hodnoty **FMR** / **FNMR** odpovídaly požadavkům (dle způsobu použití systému). K pojmu **EER** se váží další dvě charakteristiky (Obr. 4.2.4):

- **ZeroFMR** je dolní hranice **FNMR**, tj.  $\mathbf{FMR} = 0$ .
- **ZeroFNMR** je dolní hranice **FMR**, tj.  $\mathbf{FNMR} = 0$ .



### **Míra neschopnosti nasnímat – FTA**

**FTA (Failure To Acquire)** udává podíl chybných záznamů v automatickém módu záznamu daného senzoru. Tj. zaznamenání biometrické charakteristiky je odmítnuto, ačkoliv je biometrická charakteristika přítomna. Čím vyšší je tato hodnota, tím méně je daný senzor vhodný pro záznam uvedené biometrické charakteristiky. Tím pádem slouží tato míra k hodnocení kvality senzorů.



Příklad: Z celkového počtu 50 pokusů o nasnímání sítnice oka se nepodařilo získat data ze senzoru celkem 3x. Tedy **FTA** = 3 / 50 = 6%.





### Míra neschopnosti zaregistrovat – FTE

**FTE (Failure To Enroll)** udává procentuální podíl uživatelů, které není systém schopen se naučit. Míry **FTE** se často vyskytují u systémů, které mají kontrolu kvality biometrické charakteristiky, tj. biometrické charakteristiky s nedostatečnou kvalitou nejsou systémem naučeny. V tomto smyslu představuje **FTE** údaj, který ohodnocuje schopnost algoritmu pracovat i s nekvalitními biometrickými charakteristikami.



Příklad: Z celkového počtu 200 pokusů o nasnímání hlasu se nepodařilo z důvodu velkého hluku v pozadí rozpoznat řečový signál z mikrofonu celkem 9x. Tedy **FTE** =  $9 / 200 = 4,5\%$ .

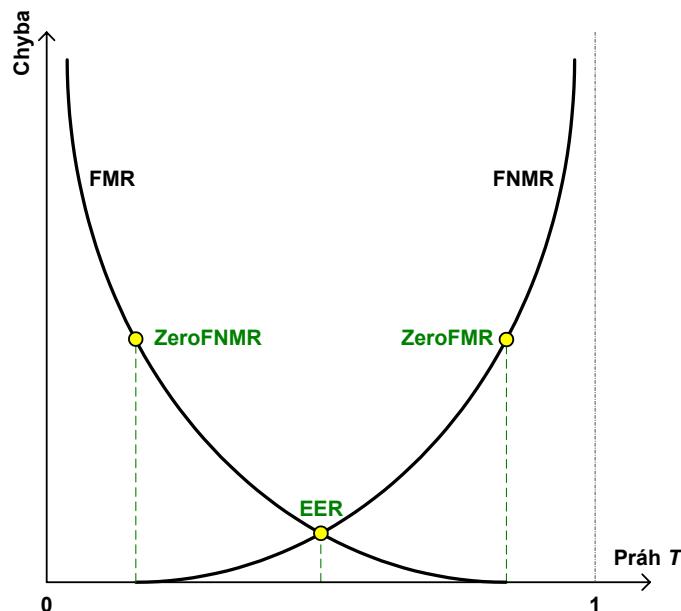


### Míra neschopnosti porovnat – FTM

**FTM (Failure To Match)** udává procentuální podíl biometrických charakteristik, které nemohly být porovnány se šablonou a nebo jakkoliv jinak zpracovány (po procesu zaregistrování). Tato míra poukazuje na neschopnost systému učinit rozhodnutí, tj. porovnání neprinese žádný výsledek.



Příklad: Z celkového počtu 3000 pokusů o porovnání zaregistrovaných otisků prstů se nepodařilo z důvodu nedostatečného počtu markantů srovnat celkem 25 z nich. Tedy **FTM** =  $25 / 3000 = 0,83\%$ .



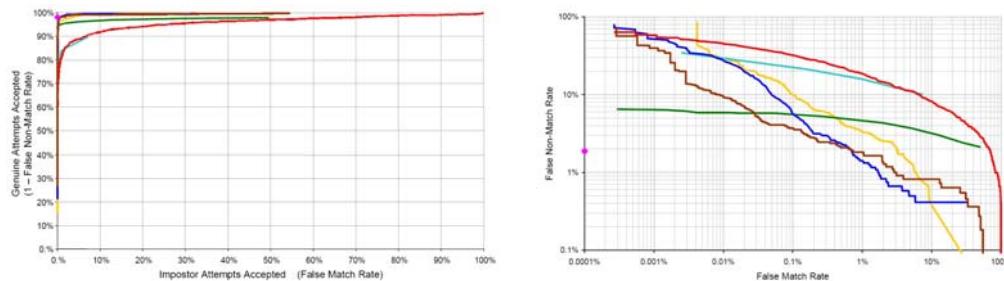
Obrázek 4.2.4: Závislosti **EER**, **ZeroFMR** a **ZeroFNMR**



### ROC křivka

**FMR** i **FNMR** jsou závislé na hodnotě prahu  $T$ . Se změnou hodnoty prahu  $T$  se zvyšuje či zmenšuje hodnota **FMR** a **FNMR** (vždy obě hodnoty naráz opačnými směry). Výkonnost systému se proto udává pomocí tzv. **ROC** křivky (**ROC** = **Receiever Operating Curve**). **ROC** křivky představují v současné době standard při popisu vlastností daného systému; někdy se setkáme s pojmem **DET** (*Detection*

*Error Trade-off*), což je ekvivalent **ROC** křivky, pouze se odlišuje reprezentace zanášení hodnot do grafu. **ROC** křivky představují detekční schopnost funkce **FMR** vzhledem k **FNMR** (příp. **FAR** / **FRR**), tj. **FNMR** =  $f(FMR)$ . Příklad křivek **ROC** a **DET** je uveden na obrázku 4.2.5.



Obrázek 4.2.5: Ukázka **ROC** (vlevo) a **DET** (vpravo) křivky [Man02]

Mezi jednotlivými mírami existují následující souvislosti a vztahy:

- **FTA** udává počet biometrických vlastností, které nemohly být nasnímány. Vyšší **FTA** zvyšuje **FRR** a snižuje naopak **FAR**. Počet biometrických vlastností, které nasnímány být mohly je  $(1 - \text{FTA})$ .
- **FTE** udává počet biometrických vlastností, které nemohly být daným algoritmem registrovány / naučeny. Vyšší **FTE** zvyšuje **FRR** a naopak snižuje **FAR**. Počet biometrických vlastností, které mohly být naučeny / zaregistrovány je  $(1 - \text{FTE})$ .
- $(1 - \text{FTA}) \times \text{FTE}$ : odpovídá podílu biometrických vlastností, které byly nasnímány, ale nemohly být naučeny / zaregistrovány.
- $(1 - \text{FTA}) \times (1 - \text{FTE})$ : odpovídá podílu biometrických vlastností, které byly nasnímány a zároveň naučeny / zaregistrovány.
- Jako hraniční podmínky lze psát:
  - $\text{FMR}(0) = 1, \text{ FMR}(1) = 0$
  - $\text{FNMR}(0) = 0, \text{ FNMR}(1) = 1$



Pro vytvoření **FMR** křivky (*Impostor Distribution*) je třeba provést následující počet porovnání [BIF04]:

$$N_{FMR} = \sum_{i=1}^{N_{DB}-1} (N_{DB} - i) = \frac{N_{DB} \cdot (N_{DB} - 1)}{2} \quad (4.6)$$

kde  $N_{DB}$  představuje celkový počet vzorů dané biometrické vlastnosti v databázi.

Pro vytvoření **FNMR** křivky (*Genuine Distribution*) je třeba provést následující počet porovnání [BIF04]:

$$N_{FNMR} = \sum_{i=1}^{N_p} (N_p - i) \cdot N_{DB} = \frac{N_p \cdot (N_p - 1)}{2} \cdot N_{DB} \quad (4.7)$$

kde  $N_{DB}$  představuje celkový počet vzorů biometrické vlastnosti a  $N_p$  je počet záznámů od stejného nosiče biometrické vlastnosti (např. z téhož prstu).

Následně se dostáváme ke scénářům chyb, tj. pro které hodnoty je kde vhodné použití. Je-li **FRR** > **FAR** (**FAR**  $\geq 0$ ), biometrických systémů se používají ke kont-

role identity – verifikaci (1:1). Např. hraniční kontrola. Je-li **FRR < FAR**, pak se biometrické systémy používají ke zjištění identity – identifikaci (1:N). Např. automatické rozpoznávání obličejů a jejich porovnání s databází pachatelů, mobilní použití scannerů otisků prstů a vyhledání v databázi otisků prstů trestanců, identifikace již trestaných pachatelů na základě jejich hlasu, chůze...

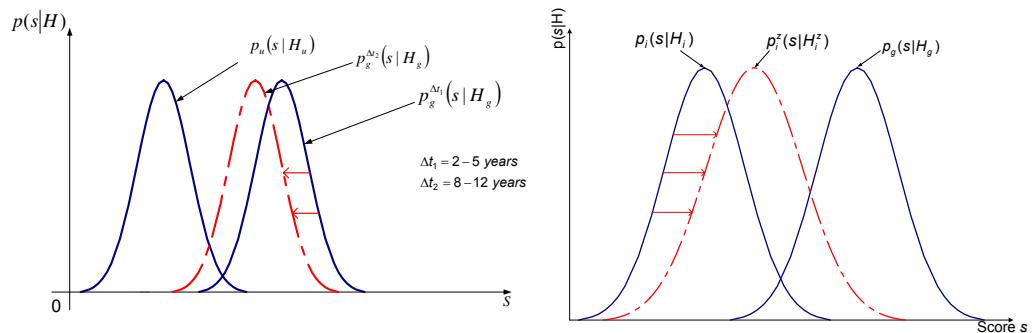


Dle normy ISO/IEC 15480 můžeme definovat *bezpečnostní sílu* biometrického systému dle FAR takto:

- Základní: **FAR**  $\leq 10^{-2}$
- Střední: **FAR**  $\leq 10^{-4}$
- Vysoká: **FAR**  $\leq 10^{-6}$



Na biometrické vlastnosti působí kromě výše zmíněných okolností také další vlivy, a těmi je stárnutí a působení podobnosti dvojčat. Změny v rozložení křivek právoplatných (*Genuine*) a neprávoplatných (*Impostor*) uživatelů jsou znázorněny na obrázcích 4.2.6a a 4.2.6b (v tomto pořadí). Stárnutí má vliv především na křivku právoplatných uživatelů (Obr. 4.2.6a, modrá křivka vpravo), kdy dochází vlivem stárnutí ke změnám takovým, že právoplatný uživatel je klasifikován sice stále ve správné množině, ale s nižším skóre porovnání. U dvojčat (Obr. 4.2.6b) naopak dochází k posunu levé modré křivky doprava. Jedná se o rozložení neprávoplatných uživatelů. Systém by měl stále rozlišit obě dvojčata, ale skóre porovnání bude vyšší. Jak je patrné z obrázků, je nutné správně zvolit práh pro přijetí či ne-přijetí. Jeho hodnota má totiž přímý vliv na to, zda uživatel se zestárlými biometrickými informacemi projde či nikoliv, a rovněž platí toto rozhodovací dilema i pro dvojčata.



Obrázek 4.2.6: a) Změna rozložení vlivem stárnutí; b) Změna rozložení u dvojčat



Pro testování máme k dispozici základní tři druhy evaluačních možností:

- **Evaluace technologie** spočívá v testování vybraných algoritmů, které používá daný biometrický systém a jsou obvykle provedeny v laboratorních systémech či prototypech budoucích systémů.
- **Evaluace scénáře** testuje celkovou výkonnost a spolehlivost daného biometrického systému v prototypových situacích. Tato evaluace obsahuje snímání biometrické vlastnosti, provedení registrace a porovnání, vč. generování a předání výsledku.
- **Provozní evaluace** spočívá v testování zvoleného biometrického systému pro nějakou konkrétní specifickou aplikaci. Tím pomáhá určit, zda daný systém bude pracovat v reálném světě v daném konkrétním prostředí.

Při plánování provedení testů se musíme nejprve zeptat, co chceme testováním vlastně dokázat a který typ scénáře evaluace máme použít. Dále musíme zjistit informace o systému (log soubory, šablony, SDK, kvalita vstupu, ...). Podstatnou částí je i kontrola faktorů ovlivňujících výkonnost (vlivy prostředí, chybná volba dobrovolníků, ...). Pro zjištění potřebné velikost testových dat můžeme použít buď vzorce (4.6) a (4.7), nebo následující dvě pravidla:

- Pravidlo „Rule of 3“
- Pravidlo „Rule of 30“

Pro získání opravdu dobrých výsledků se doporučují opakované testy se stejnými daty za jiných podmínek.

### Pravidlo „Rule of 3“

Otázka – Jaká je nejmenší chybová míra, která může být statisticky určena na základě určitého počtu  $N$  porovnání?

Odpověď – Touto hodnotou je chybová míra  $p$ , pro kterou je pravděpodobnost žádné chyby v  $N$  pokusech (zcela náhodných), 5%. Potom  $p \approx 3 / N$  pro 95% úroveň jistoty.

 Příklad: O testu 300 nezávislých vzorků nevykazujících chyby může být vyřčeno s 95% jistotou, že chybová míra  $p$  leží pod 1%.

### Pravidlo „Rule of 30“

Toto pravidlo slouží k určení velikosti dat. Abychom si byli jisti na 90%, že skutečná chybová míra leží v rozsahu  $\pm 30\%$  zjištěné chybové míry, musí se vyskytnout nejméně 30 chyb.

 Příklad: Máme-li 30 chybných Non-Match výsledků ve 3000 nezávislých pokusech oprávněných uživatelů, můžeme říct s 90% jistotou, že skutečná chybová míra leží v rozsahu  $<0,7\%; 1,3\%>$ .

Při sběru dat je nutné zamezení vzniku chyb! Ke každému snímání je třeba ukládat záznamy a dále ukládat log-soubory pro registraci uživatelů do systému a veškeré provedené transakce. Zvolit evaluační různé scénáře pro transakce právoplatných uživatelů (*Genuine*) a transakce útočníků (*Impostor*). Musíme také myslet na rozdíl mezi on-line a off-line systémy. Po provedení testů je nutné vyjádřit **FTA**, **FTE**, **FTM**, dále **FMR+FNR** / **FAR+FRR** a **ROC** křivky.

 Příklady provedených testů:

- CESG - Best Practices  
[www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf](http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf)
- Face Recognition Vendor Test  
[www.frvt.org](http://www.frvt.org)
- FVC 2004  
[bias.csr.unibo.it/fvc2004](http://bias.csr.unibo.it/fvc2004)
- BioFinger  
[www.bsi.de/literat/studien/BioFinger](http://www.bsi.de/literat/studien/BioFinger)

- BioFace

[www.bsi.de/literat/studien/BioFace](http://www.bsi.de/literat/studien/BioFace)



V této kapitole jsme probrali velmi důležitou část, která patří neúprosně k biometrickým systémům – testování jejich kvality. Součástí kapitoly byly i statistické základy, tj. kolik pokusů musíme provést pro testování s určitým počtem vzorků, abychom docílili určené vypovídací hodnoty. S tím úzce souvisí množství vzorků, které bychom měli nasbírat, aby byla opět vypovídací hodnota našeho testování patřičně vysoká.

Výsledek porovnání vstupního vzorku se šablonou je skóre porovnání, jehož výsledek používáme pro vytvoření hodnot **FAR/FRR**, příp. **FMR/FNMR**. Z těchto hodnot lze potom odvodit **ROC** křivku. S těmito chybami mírami souvisí i jiné hodnoty, jejichž význam není sice malý, ale tyto výše zmíněné údaje se používají nejčastěji pro vyhodnocení kvality daného biometrického systému.

Příklady otázek:

1. Co je to entropie?
2. Jaký je rozdíl mezi **FMR+FNMR** a **FAR+FRR**?
3. Definujte **FTA**, **FTE**, **FTM**.
4. Co je to **ROC** křivka?
5. Jaká znáte pravidla pro zjištění potřebné velikosti dat?



Odpovědi:

1. Strana 24.
2. Strana 27 – 28.
3. Strana 29.
4. Strana 30.
5. Strana 32.





## 5. Rozpoznávání podle otisků prstů

V této kapitole se budeme věnovat biometrickému rozpoznávání, které je založeno na otiscích našich prstů. Projdeme strukturu kůže na prstech, principy snímání, úpravy obrazu, až po samotné metody porovnávání otisků prstů.

Před samotným začátkem si uveďme nějaké motivační informace. Papilární linie (bude vysvětleno dále) mají grafickou reprezentaci = otisk prstu. Papilární linie se formují během embryonálního vývoje. Markanty (bude vysvětleno dále) jsou neměnné s časem. Každý prst je unikátním vzorkem, tj. neexistují na světě dva stejné prsty. Vše je historicky podloženo.

Trocha historie – prvními pozůstatky jsou archeologické artefakty a malby v jeskyních. Jména spojená s historií otisků prstů:

- Nehemiah Grew (1864)
- Mayer (1788)
- Thomas Bewick (1809)
- J.E. Purkyně (1823)
- Henry Fauld (1880)
- W.J. Herschel (1900) – Scotland Yard
- Francis Galton (1900) – Scotland Yard



### Daktyloskopické zákony [Joz72]:

- Na světě neexistují žádní dva lidé, jejichž papilární linie by měly stejnou strukturu.
- Vzor tvořený papilárními liniemi zůstává po celý život jedince relativně neměnný.
- Papilární linie jsou obnovovány dorůstáním kůže na povrchu prstů. Tyto linie nemohou být pozměněny či odstraněny, není-li poškozena epidermální vrstva kůže. Potom již nedojde na tomto místě k obnově papilárních linií.
- Konfigurační typy se individuálně mění, ale změny jsou natolik malé, že leží v tolerančních limitech a tím umožňují systematickou klasifikaci.

### 5.1 Základy



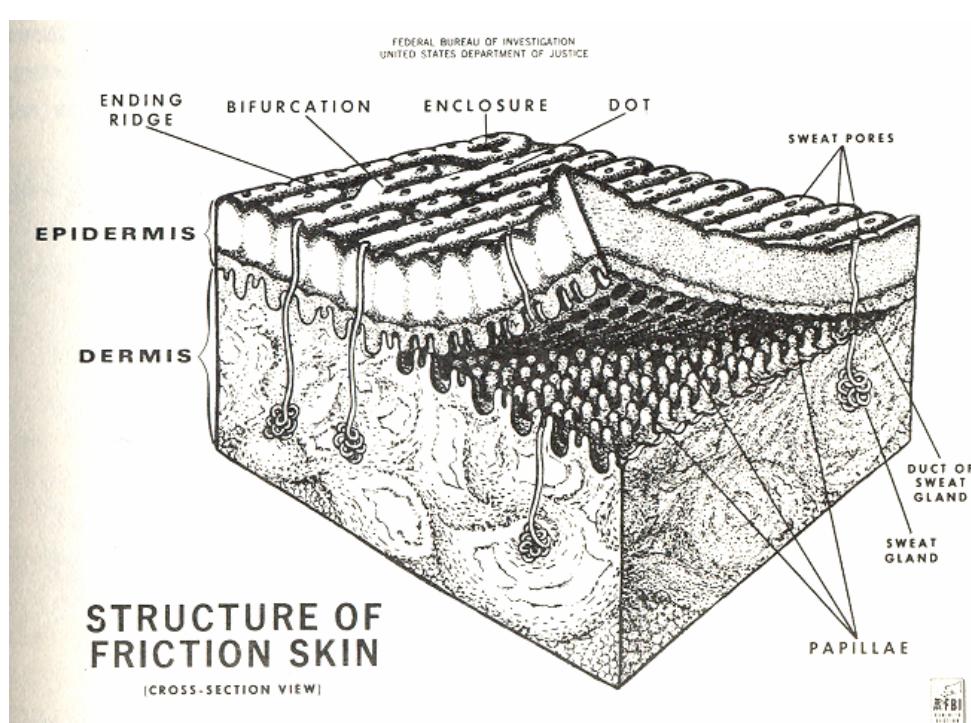
Rozlišujeme tři druhy otisků prstů:

- **Válený** (též barvený, rolovaný; Obr. 5.1.1a)
- **Píchaný** (též živý; Obr. 5.1.1b)
- **Latentní** (též skrytý; Obr. 5.1.1c)



Existují ovšem otisky prstů (prsty), které jsou naprosto nevhodné pro automatické rozpoznání či pro porovnání založené na markantech.

K pojmu otisků prstů se váže základní termín – **papilární linií** (Obr. 5.1.2). Otisk prstu je vzor tvořený obrazem papilárních linií. Výška papilárních linií leží v rozmezí 0,1 – 0,4 mm a šířka papilárních linií v rozmezí 0,2 – 0,5 mm.

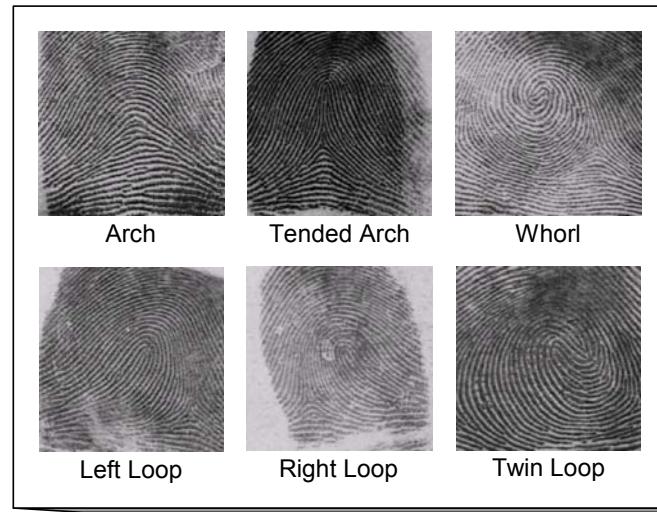


Obrázek 5.1.2: Řez kůží a zobrazení průběhu papilárních linií

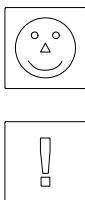
Existují následující **třídy otisků prstů** (*fingerprint classes*) – Obr. 5.1.3:

- **Oblouk** (*Arch*)
- **Klenutý oblouk** (*Tended Arch*)
- **Spirála / Závit** (*Whorl*)
- **Levá smyčka** (*Left Loop*)
- **Pravá smyčka** (*Right Loop*)
- **Dvojitá smyčka** (*Twin Loop*)



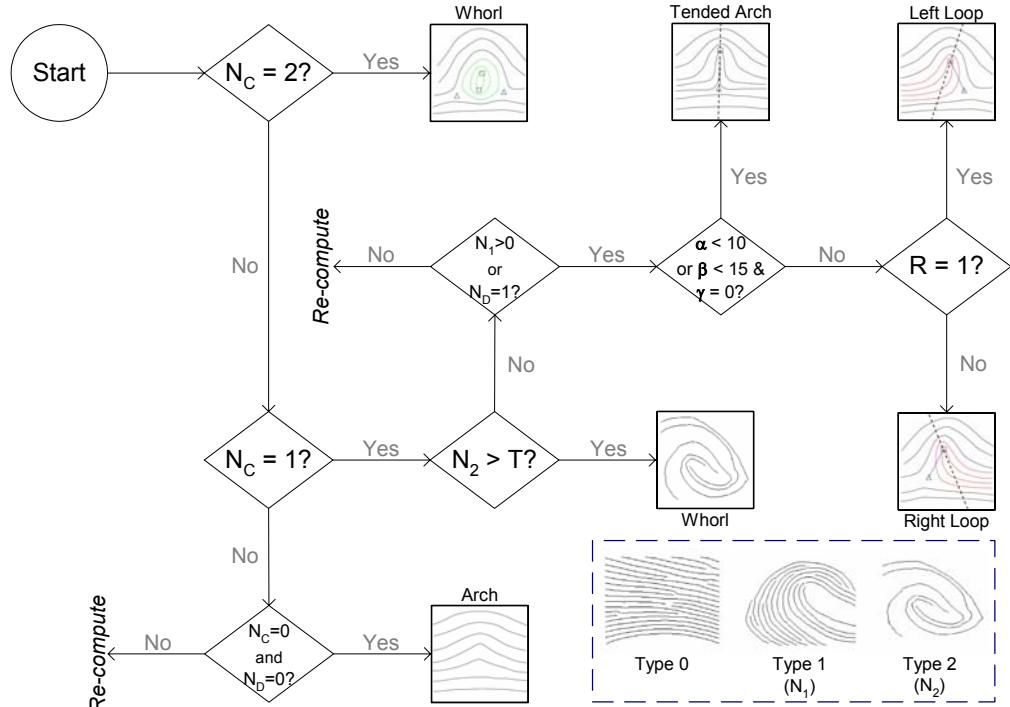


Obrázek 5.1.3: Třídy otisků prstů [Dra05]



V daktyloskopických systémech (pro kriminalistické účely) se používají většinou všechny třídy, kromě poslední (dvojitá smyčka). Algoritmus pro klasifikaci otisků prstů je znázorněn na obrázku 5.1.4 a vychází z informací obsažených v prstu. Pojmy, které se váží ke klasifikaci (Obr. 5.1.5b) [Dra01]:

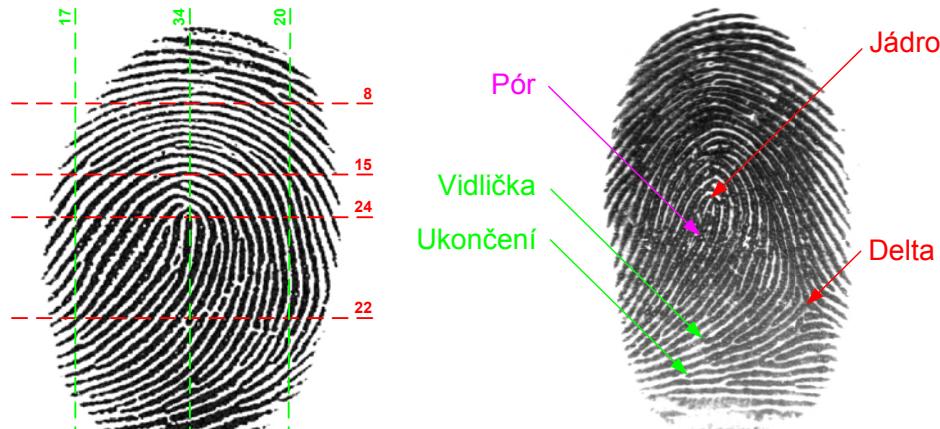
- **Delta** – místo v otisku prstu, kde probíhají papilární linie do tří směrů (většinou je na okraji; mohou existovat i 2 delty).
- **Jádro (Core)** – střed otisku prstu, nachází se na nejspodnějším vyklenutí v průběhu papilárních linií.
- **Typové linie (Type Lines)** – vytýčují prostor mezi nejsvrchnější papilární linií patřící ke středu, a nejspodnější patřící k deltě.



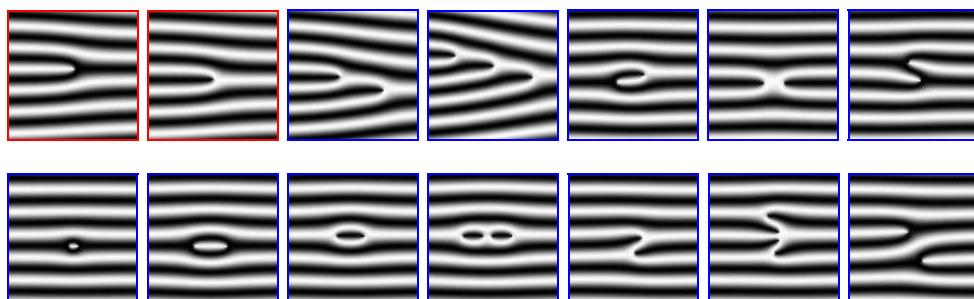
Obrázek 5.1.4: Algoritmus klasifikace otisků prstů



**RIP Count** je počet papilárních linií mezi dvěma definovanými body v otisku prstu (nejčastěji mezi jádrem a deltu). Příklad počtu papilárních linií ve vertikálním a horizontálním směru je znázorněn na obrázku 5.1.5a (směrem k jádru otisku prstu se počet papilárních linií zvětšuje).

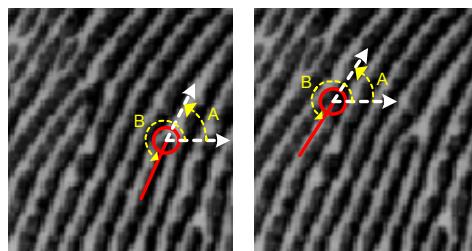


Otisky prstů rozlišujeme ovšem na základě speciálních útvarů, které tvoří papilární linie. Tyto útvary nazýváme **markanty**. K základním markantům patří (Obr. 5.1.6, v tomto pořadí): **ukončení** (*Line Ending*), **jednoduchá vidlička / rozdvojení** (*Simple Bifurcation*), **dvojitá vidlička** (*Double Bifurcation*), **trojítá vidlička** (*Triple Bifurcation*), **hák** (*Hook*), **křížení** (*Crossing*), **boční kontakt** (*Side Contact*); (dolní řádek obrázku 5.1.6): **bod** (*Point*), **interval** (*Interval*), **jednoduchá smyčka** (*Single Whorl*), **dvojitá smyčka** (*Double Whorl*), **jednoduchý most** (*Single Bridge*), **dvojitý most** (*Twin Bridge*) a **průsečná linie** (*Through Line*). V daktyloskopických systémech se používá mnohem více markantů, než jsou zde uvedeny. Naopak u přístupových systémů se používají pouze dva: **ukončení** (*Line Ending*) a **vidlička** (*Bifurcation*).



**Orientace markantu** je směr, ve kterém by pokračovala papilární linie v markantu. Rozlišujeme dvě notace (Obr. 5.1.7; levý obrázek = ukončení; pravý obrázek = vidlička):

- Označení A: **Standardní notace**
- Označení B: **FBI / AFIS notace** (opačná ke standardní notaci)



Obrázek 5.1.7: Standardní (vlevo) a FBI (vpravo) notace orientace markantu

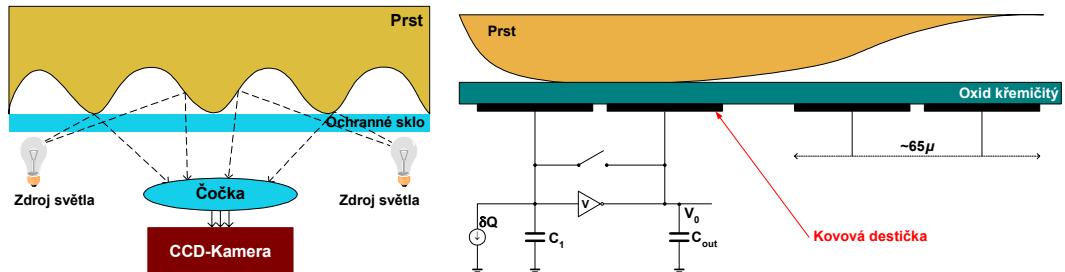
## 5.2 Technologie senzorů

V biometrických systémech pro rozpoznávání otisků prstů rozlišujeme následující technologie senzorů [Bon04]: optická, kapacitní, ultrazvuková, e-field, elektrooptická, tlaková a termická.



**Optická technologie** (Obr. 5.2.1a): Jedná se o relativně jednoduchý optický princip, tj. zdroj světla (LED) osvětlí plochu prstu, který je přiložen na skleněnou plochu senzoru (existují i bezkontaktní 3D optické senzory, tzn. ne vždy musí být prst přiložen na plochu) a kamera (CCD) nasnímá obraz.

**Kapacitní technologie** (Obr. 5.2.1b): Senzor je složen z maticy malých vodičových plošek, na nichž je napařená vrstva nevodivého oxidu křemičitého. Jemnost těchto vodičových plošek je vyšší než jemnost papilárních linií. Přiložením prstu vzniknou nad plochami těchto plošek kondenzátory, jejichž výstupem je hodnota odpovídající překryvu plochy plošky (viz princip kondenzátoru).



Obrázek 5.2.1: a) Optická technologie; b) Kapacitní technologie

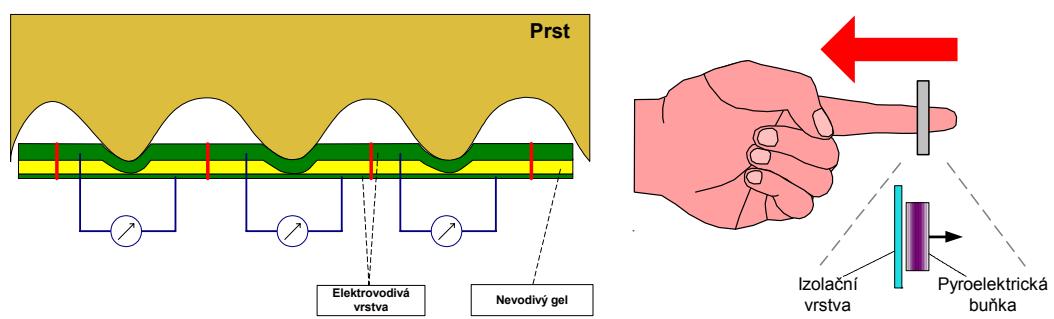
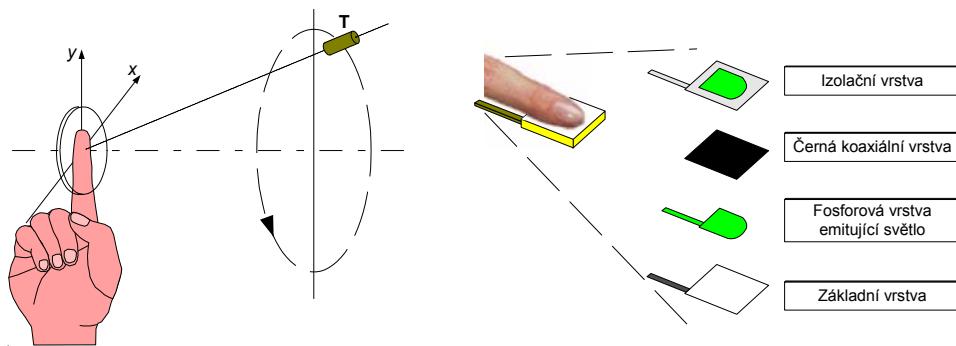


**Ultrazvuková technologie** (Obr. 5.2.2a): Zde je princip založen na rotujícím ultrazvukovém vysílači, v němž je zabudován i přijímač. Tento rotuje po kruhové dráze a snímá otisk prstu. Ultrazvukové vlny proniknou i pod povrch kůže, tzn. tato technologie může lehce odhalit falešné prsty.

**Elektrooptická technologie** (Obr. 5.2.2b): Senzor se skládá ze 4 vrstev, přičemž přítlačem prstu vybudí styk černé koaxiální vrstvy emitování světla ve fosforevné vrstvě. Toto záření projde základní vrstvou do senzoru.

**Tlaková technologie** (Obr. 5.2.3a): Senzor je 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.

**Termická technologie** (Obr. 5.2.3b): 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.



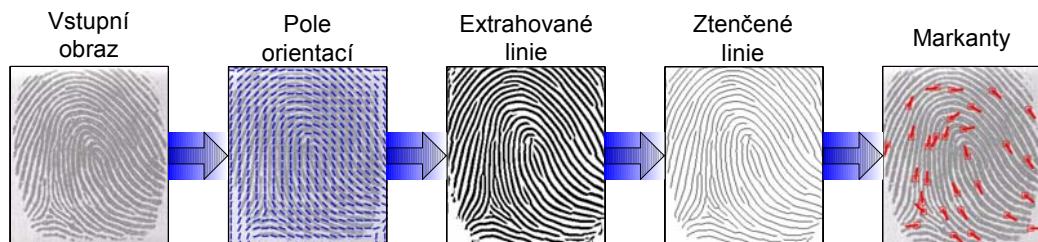
### 5.3 Funkce systému

Obecně máme dvě fáze biometrického systému (viz Obr. 2.3.2):

- Registrace = *Enroll*
- Porovnání = *Authenticate*

Registrace probíhá způsobem popsáným v kapitole 2.3. Porovnávání funguje rovněž obdobně, ale odlišnost otisků prstů pocházejících ze stejného prstu může být značná, rovněž jako podobnost otisků prstů, které pochází i od naprostě odlišných jedinců. Proces porovnání není tedy příliš jednoduchý (to platí obecně pro všechny biometrické metody).

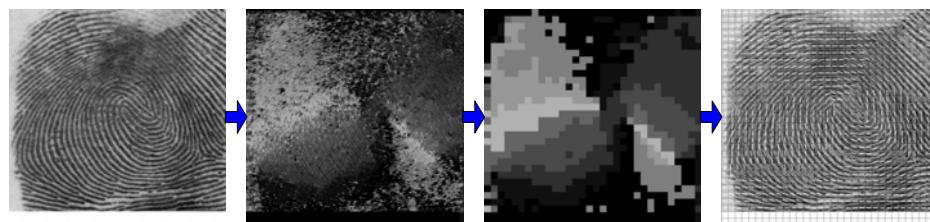
Proces zpracování otisku prstu je znázorněn na obrázku 5.3.1.





Tento proces se skládá z následujících kroků:

- **Vstupní obraz** – získání obrazu otisku prstu ze senzoru (optické, kapacitní...) či z jiné předlohy → digitální otisk prstu. Ve vstupním obrazu je obsaženo velké množství šumu, což vyžaduje následnou úpravu ve třetím kroku zpracování. Při snímání je nutné rozlišovat válené / píchané a příp. latentní otisky prstů. Dále je nutné dbát na vlivy jako např. znečištění povrchu otisku prstu, poranění apod. Nezbytné je kontrolovat živost prstu, resp. zda není na prstu nalepen falešný otisk prstu.
- **Pole orientací** – v každém bodu obrazu se spočte směr papilární linie z okolí (dle tónů šedé barvy). Nachází-li se bod přímo na papilární linii, určuje s maximální pravděpodobností její směr. Nejprve se vypočte pole orientací pro každý bod obrazu. Ve druhém kroku dojde k transformaci na *blokové pole orientací*. Blokové pole orientací je následně namapováno na původní obrázek otisku prstu. Ukázka je uvedena na obrázku 5.3.2.



Obrázek 5.3.2: Postup při výpočtu pole orientací

- **Extrahované linie** – úprava obrazu + Č/B linie. Sem patří úpravy histogramu – např. škálování histogramu. S tím je spjatá kontrola kvality vstupního obrazu. Pro filtrování (často i v předchozím kroku – pole orientací) se používá 2D Gaborova funkce (viz kapitola 3.2). Pro filtrování ve frekvenční doméně (FFT → aplikace filtru → IFFT) se používají následující filtry:

- Dolní propust:  $H(u,v) = \begin{cases} 1 & D(u,v) \leq D_0 \\ 0 & D(u,v) > D_0 \end{cases}$ , kde  $D_0$  je hraniční frekvence a  $D(u,v) = \sqrt{u^2 + v^2}$ .
- Filtr Butterworth:  $H(u,v) = \frac{1}{1 + [D(u,v)/D_0]^{2n}}$
- Filtr Ikonomopoulos:  $H_i = \begin{cases} 1 & \theta_i < \tan^{-1}(v/u) < \theta_{i+1} \& u^2 + v^2 > r_c^2 \\ 0 & jinak \end{cases}$   
kde  $u,v$  jsou frekvenční souřadnice,  $n$  je počet směrů a  $\theta_i = (i-1)\pi/2n$
- Filtr Sherlock – podklady viz Internet.

Pro prahování (*thresholding*) obrazu se využívá (krom jiných metod) tzv. **schéma RAT** (*Regional Average Thresholding*), které nejprve rozdělí obrázek na bloky  $8 \times 8$ , potom spočte průměrnou úroveň šedé v této oblasti, dále nastaví hodnotu levé části  $8 \times 4$  na tuto hodnotu a posune operační okno o 4 body doprava. Je-li dosažen pravý okraj, posune se okno o 8 bodů dolů a začne se opět zleva.



- **Ztenčené linie** – ztenčování papilárních linií na 1 pixel. Pro ztenčování se používá relativně jednoduchý algoritmus, jehož účelem je zredukovat počet pixelů na obrazu papilární linie tak, že její tloušťka je pouze 1 pixel. Mezi nejpoužívanější metody řadíme **Metodu Emyroglu**, která používá dva typy bodů (RMP – *Ridge Meeting Point* a RCP – *Ridge Continuity Point*). Musí platit, že papilární linie nesmí ubývat v žádném směru – problém s polohou markantů.
- **Markanty** – detekce a extrakce markantů. Zde se používá (opět krom jiných možných metod) metoda detekce papilárních linií dle Honga, tzv. **Hongova metoda**. Metoda je založena na tom, že papilární linie probíhají paralelně vůči sobě a dosahují maximální úrovni šedé uprostřed samotné linie (černé (tmavé) body). Otisk prstu je násoben se dvěma maskami  $h_t$  a  $h_b$ , které mají navzájem posunutou fází o  $180^\circ$ :

$$h_t(i, j; u, v) = \begin{cases} -\frac{1}{\sqrt{2\pi\delta}} e^{-\frac{u^2}{\delta^2}} & \dots \dots u = (v \cot(O(i, j)) - \frac{H}{2 \cos(O(i, j))}), v \in \Omega \\ \frac{1}{\sqrt{2\pi\delta}} e^{-\frac{u^2}{\delta^2}} & \dots \dots u = (v \cot(O(i, j))), v \in \Omega \\ 0 & \dots \dots \text{anders} \end{cases}$$

$$h_b(i, j; u, v) = \begin{cases} -\frac{1}{\sqrt{2\pi\delta}} e^{-\frac{u^2}{\delta^2}} & \dots \dots u = (v \cot(O(i, j)) + \frac{H}{2 \cos(O(i, j))}), v \in \Omega \\ \frac{1}{\sqrt{2\pi\delta}} e^{-\frac{u^2}{\delta^2}} & \dots \dots u = (v \cot(O(i, j))), v \in \Omega \\ 0 & \dots \dots \text{anders} \end{cases}$$

$$\Omega = \left[ -\frac{|L \sin(O(i, j))|}{2}, \frac{|L \sin(O(i, j))|}{2} \right]$$

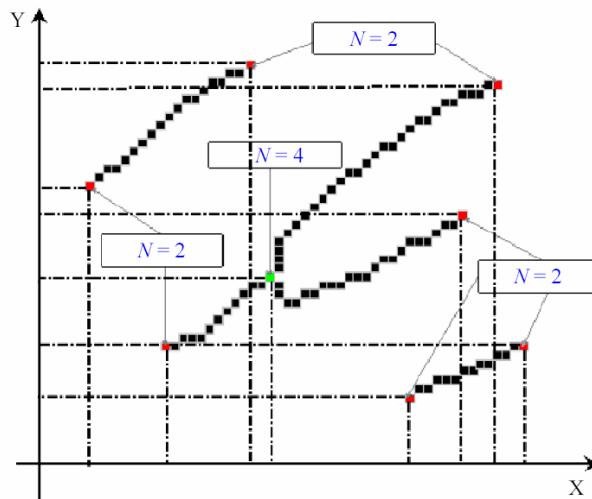
V průměru lze říci, že  $L \times H$  je  $11 \times 7$  [Jai04]. Ideálně by měla být šířka masky rovna šířce lokální linie. Pixel  $(i, j)$  je označen jako pixel papilární linie, pokud jsou obě hodnoty po konvolucích (filtry  $h_t$  a  $h_b$ ) větší jak nastavený práh  $T_R$ . S ohledem na parametr  $\delta$  provádí obě masky i vyhlazování. Ve výsledném obrazu je nutné provést kontrolu a úpravu porušení papilárních linií, příp. zrušení zlomů v průbězích papilárních linií.

Obecně se detekují dva základní typy markantů (ukončení papilární linie a vidlička), přičemž ostatní typy markantů jsou kombinací těchto dvou základních typů, tj. existuje možnost detekce více typů. Rozhodování pro detekci probíhá na základě následujících podmínek:

- $\sum_{u=-1}^1 \sum_{v=-1}^1 T_R(i+u, j+v) = 2$  potom *Ukončení*.
- $\sum_{u=-1}^1 \sum_{v=-1}^1 T_R(i+u, j+v) > 3$  potom *Vidlička*.



Tato situace je schematicky znázorněna na obrázku 5.3.3. Obě podmínky znamenají v podstatě, že se provede součet bodů v okolí a je-li roven 2, jedná se o ukončení a je-li větší jak 3, jedná se o vidličku.



Obrázek 5.3.3: Znázornění detekce markantů na ztenčených pap. liniích

Ke každému markantu se ukládají následující údaje:



- **Pozice X**
- **Pozice Y**
- **Typ** (ukončení / vidlička)
- **Gradient** (orientace pokračování papilární linie)

Výsledek extrakce markantů je porovnán s uloženou šablonou (z databáze / smart karty apod.). Metody pro porovnávání otisků prstů:

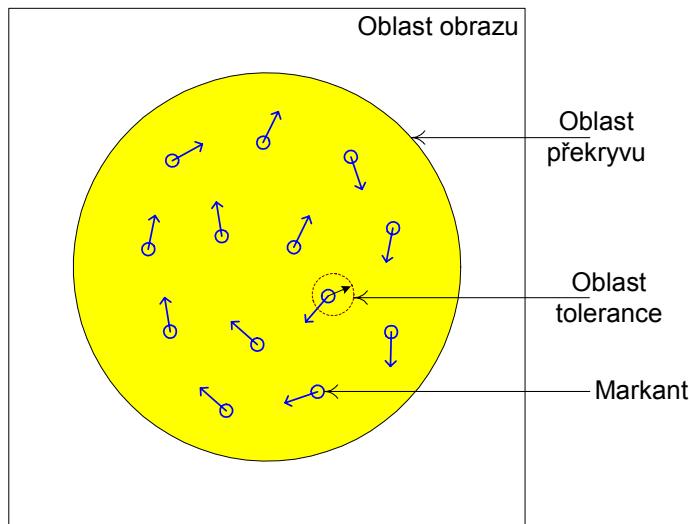
- *Metody založené na markantech*
  - Používají pozici, typ a gradient (směr)
  - Obecně problematika porovnání vzorů
- *Metody založené na korelace*
  - 2D korelace mezi vstupem a šablonou
  - Výpočetně náročné
- *Metody založené na vlastnostech papilárních linií*
  - Orientace a frekvence papilárních linií, tvar linie, texturní informace atd.
  - Nízká rozlišovací schopnost

**Metoda založená na markantech** je nejčastěji se vyskytující metodou, jedná se prakticky o problém porovnání vzorů (dvou množin markantů).

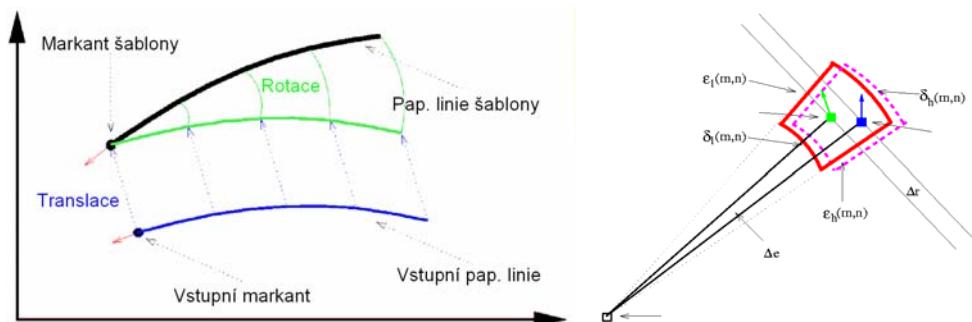
Dvě metody pro porovnávání (používající markanty):

- **Hongova metoda**
- **Rathova metoda**

Obě metody založeny na dvou hlavních krocích: generování globálního překryvu (Zarovnání) a hledání lokálního překryvu (Porovnání) – viz Obr. 5.3.4. Schématické znázornění průběhu metod je uvedeno v obrázku 5.3.5.

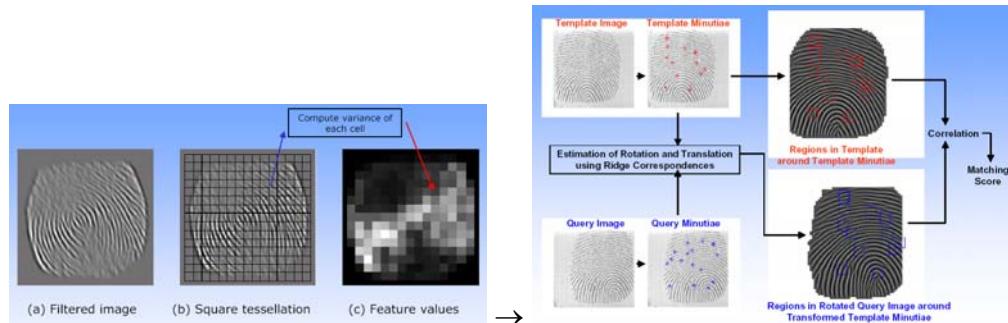


Obrázek 5.3.4: Oblast překryvu a oblast tolerance



Obrázek 5.3.5: Schematické znázornění porovnání založeném na markantech

Postup při rozpoznávání **metody založené na vlastnostech papilárních linií** je znázorněn na obrázku 5.3.6.



Obrázek 5.3.6: Rozpoznávání metody zal. na vlast. pap. linií [Jai04A]



Informace z otisku prstu lze využít i ke generování klíče, který je možné použít pro kryptografické účely. Takovému systému říkáme biometrický bezpečnostní systém (*Biometric Security System*). Na obrázku 5.3.7 je znázorněn průběh. Nejprve je načten otisk prstu. Poté dojde k procesu generování klíče, kde se využívají výše zmíněné metody a následně jsou tyto informace transformovány do podoby klíče, který se předá poslednímu modulu, který tento klíč využije k šifrování.



Obrázek 5.3.7: Biometrický bezpečnostní systém



Na začátku této kapitoly jsme si definovali daktyloskopické zákony, jejichž platnost byla prokázána již po několik desetiletí.

Dále jsme se dozvěděli, z jakých částí se skládá naše kůže a že papilární linie jsou specifikem našich prstů, dlaní a chodidel. V samotném otisku prstu nalezneme deltu a jádro, což jsou používané prvky pro klasifikaci otisků prstů. Následoval popis metod pro úpravu otisků prstů, jejich zpracování a na závěr byl uveden triviální algoritmus pro detekci markantů. Poté jsme se dozvěděli, jak se otisky prstů porovnávají.

Řekli jsme si něco i o technologiích senzorů na snímání otisků prstů, přičemž nejpoužívanější technologií je kapacitní a za ní následuje optická. Třetí nejužívanější je termická (tzv. průtahové senzory).



Motivací na cvičení nechť je obrázek 5.3.8, kde jsou zobrazeny biometrické snímače, se kterými se setkáte v laboratorních cvičeních.



Obrázek 5.3.8: Snímače otisků prstů používané v laboratorních cvičeních



Příklady otázek:

1. Co definují daktyloskopické zákony?
2. Jaké znáte třídy otisků prstů? Stručně popište.

3. Jaké znáte markanty? Stručně popište.
4. Které technologie senzorů znáte? Alespoň dva typy popište.
5. Popište funkci systému pro rozpoznávání otisků prstů?



Odpovědi:

1. Strana 34.
2. Strana 35.
3. Strana 37.
4. Strana 38.
5. Strana 39.



## 6. Rozpoznávání podle geometrie ruky, žil ruky a nehtu

V této kapitole se budeme věnovat biometrickému rozpoznávání tvaru ruky (její geometrie), struktury na hřbetu a dlani ruky, a na závěr kapitoly zjistíme, že i nehod se dá používat k biometrickému rozpoznávání identity osoby.



Kromě papilárních linií na prstech se nachází papilární linie také na dlaních obou rukou (nachází se i na chodidlech obou nohou, ale z celkem zřejmých důvodů se neuvažuje o jejich použití k biometrickým účelům). Tyto se využívají především v oblasti daktyloskopie, kdy jsou na daktyloskopickou kartu zaneseny i otisky dlaní obou rukou. Pro automatické přístupové systémy je to ale příliš mnoho informací a než by byly zpracovány, trvalo by to celkem dlouho. Proto se z ruky používá její tvar (geometrie ruky) a také žily ruky, které jsou někdy pozorovatelné i pouhým okem. Jako poslední věc, která se na ruce nachází, a může být použita k biometrickým účelům, je nehod, který vykazuje speciální a unikátní strukturu. V jednotlivých kapitolách budou popsány zmíněné vlastnosti ruky a popsány metody pro jejich rozpoznání.

### 6.1 Rozpoznávání podle geometrie ruky

Hned na začátku si ukažme, jak takový přístroj pro rozpoznávání geometrie ruky vlastně vypadá – viz obrázek 6.1.1.



Obrázek 6.1.1: Systém pro rozpoznávání geometrie ruky HandKey II.



Jako příklady nasazení těchto systémů mohou být jmenovány:

- Diebold Inc. – vstup k depozitním schránkám banky
- Simkins Industries (2 / 2004)
- U.S. Air Force – zabezpečení základen (3 / 2004)
- Letiště Yeager – kontrolní věž (8 / 2004)
- Letiště San Francisco – pro zaměstnance (9 / 2004)
- Wisconsin Private School (10 / 2004)

Tato technologie je relativně nová a tudíž zatím v začátcích.

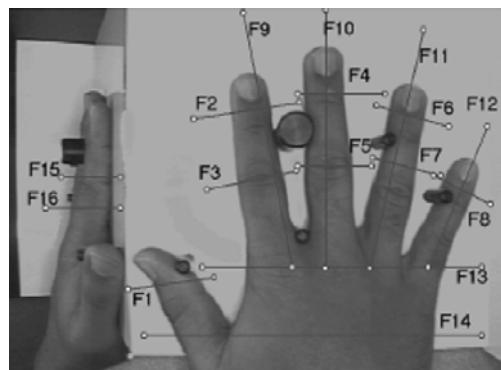
Antropologové se domnívají, že lidstvo přežilo a dále se vyvíjelo díky velkým mozkům a protilehlým palcům. Lidská ruka má mnohostranné použití – uchopovací schopnost, házení a z toho plynoucí výroba nástrojů. V dnešní době má lidská ruka i jiné použití – slouží k verifikaci (identifikaci).

V roce 1971 obdržel pan Robert P. Miller patent na zařízení, které umožňovalo měřit charakteristiky ruky, tyto používat k tvorbě šablon a následnému porovnání; tehdy nabízel toto mechanické zařízení pod názvem *Identimation*. V roce 1988 získal pan Sidlausks patent na zařízení, které již bylo elektronické.

Rozpoznávání je založeno na tvrzení, že lidská ruka je jedinečná. K rozlišení jedinců mezi sebou se používají následující **charakteristiky ruky** (Obr. 6.1.2):

- Délka prstů
- Šířka prstů
- Výška prstů
- Zakřivení a lokální anomálie

Scannery snímají pouze siluetu ruky, informace jako povrchová struktura, prsty, papilární linie apod. se ignorují. Používá se ortografické scannování – shora a z boku (Obr. 6.1.2).



Obrázek 6.1.2: Příklad snímků geometrie ruky, včetně charakteristik

Proč použít právě geometrii ruky? Geometrie ruky je

- dobré akceptovaná uživateli,
- lehce použitelná,
- používá lehce nalezitelné rysy,
- robustní vůči vlivům prostředí,
- relativně nenákladným zařízením.

A proč nepoužít geometrii ruky? Geometrie ruky

- vykazuje celkem nízkou rozlišovací schopnost a
- při identifikaci je nabídnuto příliš mnoho kandidátů.

Průběh registrace / verifikace je následující. Uživatel je systémem vyzván k opakování (obvykle 3x) položení ruky na plochu k tomu určenou. Distanční slouppky slouží k zajištění optimální pozice ruky a prstů pro kvalitní snímek. Systém provede zprůměrování snímků a uloží šablonu. Šablona má velikost 9 bytů –



je tedy vhodná pro uložení na smart kartu. Pro verifikaci zadá uživatel svoji identitu a opět položí ruku na plochu k tomu určenou. Výsledkem je buď přijetí či odmítnutí identity uživatele, tj. klasický průběh verifikačního procesu.

Kvalita snímání ovlivňuje **FRR**:

- Různá výška snímacího zařízení vede k odlišnostem ve snímcích, např. sedící uživatel při registraci by měl používat snímač také v sedě a nikoliv ve stoje.
- Vhodné použít zpětnou vazbu s uživatelem.



Praktické systémy musí provádět tzv. **průměrování šablony**, tj. při každé pozitivní verifikaci je aktuální snímek zprůměrován se šablonou – zanesení změn ve tvaru ruky (např. růst, stárnutí, úraz apod.)



Systémy pracují spolehlivě od věku 8 let. Do tohoto věku dochází k výrazným změnám v geometrii ruky. Extrakce rysů – z obrázku ruky se extrahují rysy, které jsou uvedeny výše (délka prstů, šířka prstů, výška prstů a příp. zakřivení a lokální anomálie) – viz obrázek 6.1.2 a obrázek 6.1.3. Úkolem je spočítat hodnoty  $P_s$  a  $P_e$  z následujícího profilu, přičemž  $G(x)$  je profil úrovní šedé podél osy  $x$  a platí  $0 \leq x < \text{Délka}$ . Metoda postupuje takto: začátek je v levém horním rohu. Posouvej okno přes profil směrem k pravému pixelu. Spočítej následující parametry pro každou pozici okna  $W_i$ :

$$\text{Max\_Val}(i) = \max_{j \in W_i} G(j), \quad \text{Max\_Index}(i) = \arg \max_{j \in W_i} G(j) \quad (6.1)$$

$$\text{Min\_Val}(i) = \min_{j \in W_i} G(j), \quad \text{Min\_Index}(i) = \arg \min_{j \in W_i} G(j) \quad (6.2)$$

Z předchozích údajů se spočtou hodnoty  $P_s$  a  $P_e$  takto:

$$P_s = \text{Max\_Index}(k), \quad \text{Min\_Index}(k) > \text{Max\_Index}(k) \quad (6.3)$$

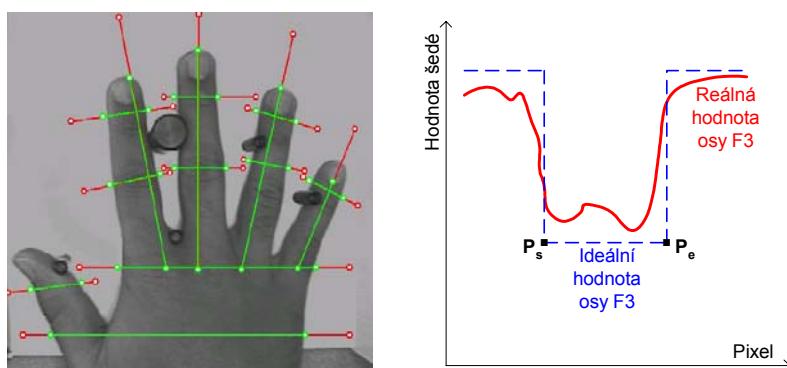
$$P_e = \text{Max\_Index}(k), \quad \text{Max\_Index}(k) > \text{Min\_Index}(k) \quad (6.4)$$

$$(\text{Max\_Val}(k) - \text{Min\_Val}(k)) > (\text{Max\_Val}(i) - \text{Min\_Val}(i)), \quad \forall i \neq k, 0 \leq i, k \leq N$$

Pro porovnání existují dva vektory:

- Vstupní vektor rysů:  $(x_1, x_2, \dots, x_{14})$
- Vektor rysů šablony:  $(y_1, y_2, \dots, y_{14})$

Skóre porovnání  $s = \text{Euklidovská vzdálenost: } \sum_{u=1}^{14} (x_u - y_u)^2$ .



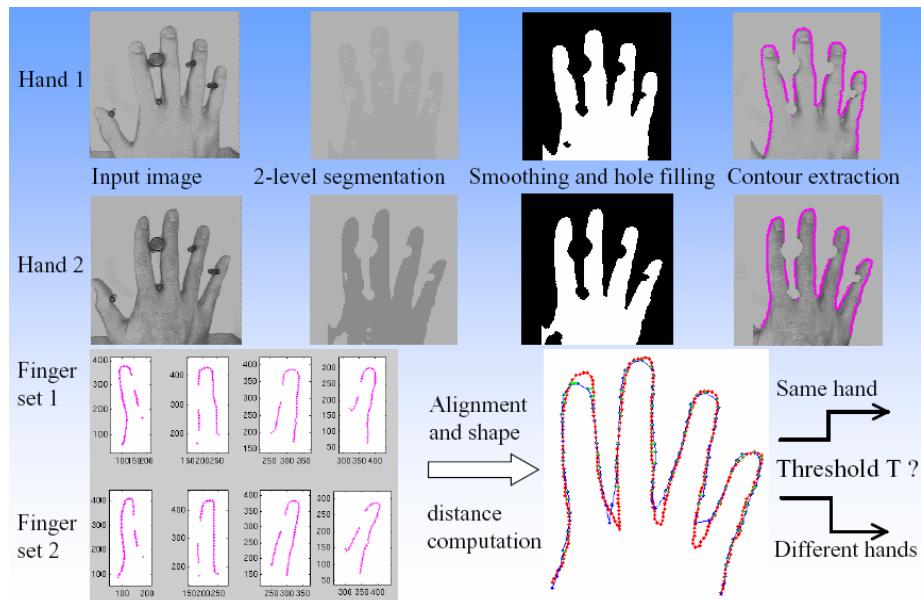
Obrázek 6.1.3: Rysy geometrie ruky a jejich extrakce z grafického průběhu



**Chernoffovy obličeje** [Wei05] se používají k popisu objektů dle různých charakteristik (např. velikost očí, nosu, ...) – ilustrují variace v hodnotách. U geometrie ruky odpovídají rysy Chernoffových obličejů následujícím charakteristikám geometrie ruky: F1 = plocha obličeje; F2 = tvar obličeje; F3 = délka nosu; F4 = poloha úst; F5 = zakřivení úsměvu; F6 = šířka úsměvu; F7 = poloha očí; F8 = vzdálenost očí; F9 = úhel očí; F10 = tvar očí; F11 = šířka očí; F12 = poloha dušovky; F13 = poloha obočí; F14 = úhel obočí.

Verifikace (obrázek 6.1.4) založená na zarovnávání rukou se skládá z následujících kroků:

- *Odstranění distančních sloupků (čepů)* – k eliminaci distančních sloupků se používá maska, která obsahuje známé pozice všech pěti sloupků, přičemž sloupky jsou nahrazeny barvou pozadí.
- *Extrakce kontury* – pro extrakci tvaru ruky se používá adaptivní prahování (binarizace).
- *Extrakce a zarovnání prstů* – nejprve se extrahuje pozice a směry prstů, které se překryjí se šablonou, s níž je daný snímek porovnáván.
- *Výpočet párových vzdáleností* – každé zarovnání z předchozího kroku produkuje množinu shody bodů. Dojde k výpočtu **MAE** (*Mean Alignment Error*), což je průměrná vzdálenost mezi odpovídajícími si body.
- *Verifikace* – pokud je **MAE**  $< T$ , potom shodné ruce!



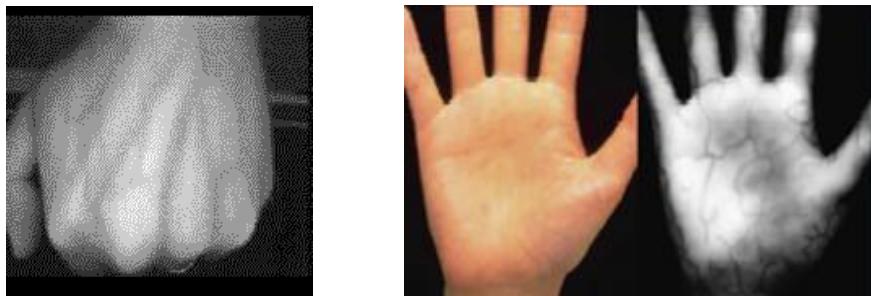
Obrázek 6.1.4: Verifikace založená na zarovnání rukou [Jai04]



Geometrie ruky není příliš signifikantním rysem pro popis osoby – tj. tato technologie je nevhodná pro rozpoznávání velkého počtu osob (velká pravděpodobnost chyby). Informace z ruky nejsou bohužel invariantní během života jedince – problémy se stárnutím / změnami. Použitím prstenů (obecně šperků) se snižuje kvalita rozpoznání, resp. jedinec může být chybně odmítnut. Fyzická velikost samotného systému je příliš velká – limitované použití např. v přenosných zařízeních.

## 6.2 Rozpoznávání podle žil ruky

Pro biometrické účely lze použít buď žíly na hřbetu ruky (Obr. 6.2.1a) a nebo žíly na dlani ruky (6.2.1b).



Obrázek 6.2.1: a) Žíly hřbetu ruky (vlevo); b) Žíly dlaně ruky (vpravo)

### Technologie žil hřbetu ruky



Hlavním příkladem aplikace pro rozpoznávání žil ruky je systém, který byl použit v Singapuru v roce 2004. Tento systém se nachází v mezinárodním finančním institutu, kde nahradil předchozí systém čipových karet. Dalším ukázkou funkčního systému je instalace ve FirstBank Puerto Rico pro kontrolu přístupu zaměstnanců banky.

Vyhídky do budoucnosti:

- Použití např. v nemocnicích (možnost testování vlivů vysokého krevního tlaku, náklonnosti k srdečnímu infarktu a onemocnění žil).
- Uvažuje se o přenosném scanneru, který by umožňoval snímání žil z hřbetu ruky např. přímo u pacientů na lůžku, přičemž data by byla uložena v PDA (PocketPC).

Provedení verifikace (obrázek 6.2.2a) se skládá z:



- Zadání identity (např. pomocí identifikačního čísla)
- Vložení ruky do snímače žil hřbetu ruky
- Extrakce žil z hřbetu ruky + generování jedinečného kódu (Obr. 6.2.2b)
  - Detekce tvaru ruky
  - Získání šedotónového obrazu s oblastí žil
  - Extrakce spletí žil z obrazu
  - Generování jedinečného kódu, podobnému obrazu papilárních linií z otisku prstu
- Porovnání se šablonou

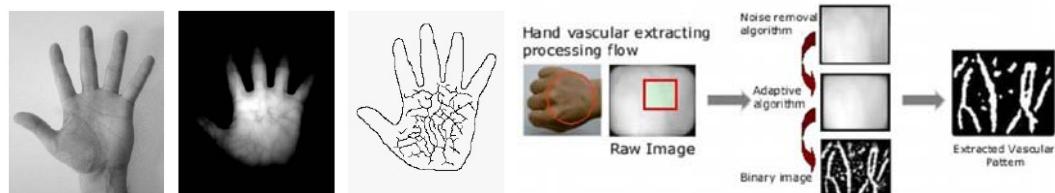
Vybrané vlastnosti [Im01]:



- Provedení nasnímání kratší jak 0,5 sekundy. Vytvoření množiny rysů z obrazku ca 1 sekunda. Velmi rychlé provedení verifikace.
- Velikost množiny rysů v průměru kolem 250 bytů. **FAR** =  $10^{-4}$  %, **FRR** =  $10^{-1}$  %
- Žíly se vytvářejí již před samotným porodem a zůstávají po celý život nemenné. Rozlišovací schopnost vyšší jak u pouhé geometrie ruky, tj. lze

použít i pro více uživatelů (v literatuře lze nalézt systém až s 18 tisíci uživatelů, zatímco u geometrie ruky se jedná řádově o stovky uživatelů).

- Žádný kontakt se snímacím zařízením. Tím není možné použít latentní informace. Prsteny, onemocnění kůže či revma nemají žádný vliv na provedení verifikace. Vlivy stárnutí a náklonnosti k srdečnímu infarktu nebyly doposud testovány. Systém akceptuje pouze žily žijícího jedince – není nutné testovat život! Výborně akceptovaný systém (99,98%).
- Díky fyzické velikosti systému omezené možnosti pro přenosná zařízení.



Obrázek 6.2.2: a) Postup verifikace na základě žil ruky; b) Detaily

### **Technologie žil dlaně ruky**



Obdobná technologie jako technologie rozpoznávání žil hřbetu ruky, pouze jsou nasnímány žily dlaně ruky. S touto technologií proráží v současné době firma Fujitsu<sup>1</sup>.

Scanner je založen na stejném principu jako u technologie rozpoznávání žil ze hřbetu ruky:

- NIR (*Near-InfraRed*) osvětlení
- Hemoglobin v žilách ~ černá barva

Příkladem systémů mohou být dvě instalace:

- Tokyo-Mitsubishi banka (ATM)
- Banka Suruga (přepážkové transakce)

Jedná se o bezkontaktní a tudíž dobře akceptovanou technologii. Je tolerantní vůči osvětlení, pozici ruky a výšce ruky. Chybové míry: **FRR** přibližně 1% a **FAR** přibližně 0,5%.



Obrázek 6.2.3: Technologie žil dlaně ruky

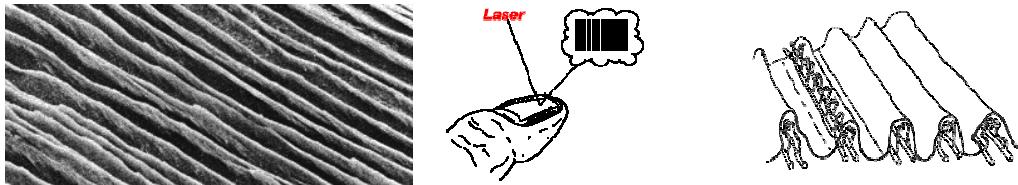
<sup>1</sup> <http://www.fujitsu.com/global/about/rd/200506palm-vein.html>

## 6.3 Rozpoznávání podle nehtu



Nehet má na povrchu čárové nerovnosti, kopírující strukturu lůžka nehtu, která je unikátní u každého člověka, na každém prstu. Při správném nasvícení dostaneme odrazem „čárový kód“ – viz obrázek 6.3.1a.

Lůžko nehtu je prakticky paralelní podkožní struktura nacházející se přímo pod nehtem (obrázek 6.3.1b). Rostoucí nehet se pohybuje po této struktuře a kopíruje její povrch.



Obrázek 6.3.1: a) „Čárový kód“ nehtu (vlevo); b) Podkožní struktura nehtu (vpravo) [Das03]



Mezi nehtem a lůžkem se nachází *keratin*. Tento přírodní polymer mění orientaci dopadajícího polarizovaného světla. Necháme-li pod určitým úhlem dopadat paprsek polarizovaného světla, můžeme analyzovat fázové změny paprsku po odraze. Je to podobné, jako bychom analyzovali strukturu lůžka pod mikroskopem. Po zpracování nasnímaného odrazu dostaneme jednorozměrnou strukturu lůžka nehtu, číselnou sekvenci, která připomíná sekvenci čárového kódu, unikátní pro každého jedince.



V této kapitole jsme probrali přístroje a markantní informace ze struktury ruky, které se používají pro její rozpoznávání. Dále jsme se věnovali žilám, jenž se nachází jak uvnitř hřbetu ruky, tak i uvnitř dlaně ruky. Tyto jsou neměnné a slouží k jednoznačnému určení identity. K tomuto účelu lze využít i struktury nehtu.



Příklady otázek:

1. Jaké charakteristiky ruky znáte?
2. Co je to průměrování šablony?
3. Co jsou Chernoffovy obličeje a k čemu slouží?
4. Popište princip funkčnosti technologie žil ruky.
5. Na čem je založena technologie nehtu?



Odpovědi:

1. Strana 46.
2. Strana 47.
3. Strana 48.
4. Strana 49 – 50.
5. Strana 51.



## 7. Rozpoznávání podle obličeje a termogramu obličeje

V této kapitole zjistíme, jakým způsobem fungují biometrické systémy na rozpoznávání obličeje. Nejprve musíme obličeji detektovat a poté můžeme provést buď 2D a nebo 3D rozpoznávání. Navíc nám mohou posloužit k rozeznání identity osoby i termosnímky obličeje, získané pomocí termokamery.



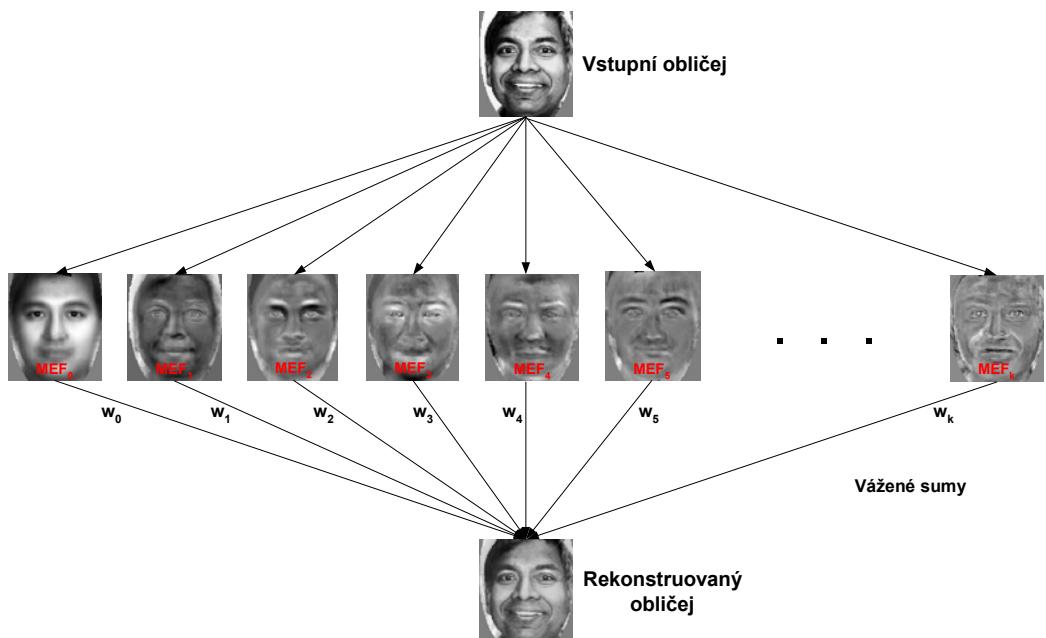
Motivace: Obličeji je nejčastěji používanou biometrickou vlastností. Rozsah aplikací: statické vs. dynamické. Problém při neřízeném rozpoznávání (více obličejů a problematika separace od pozadí)

Výzvy: automatická detekce obličeje; obecné rozpoznání obličeje za různých podmínek; vlivy – různé osvětlení, výrazy obličejů, stárnutí... Příklad změn [Mac04]:

- Stejný den, stejné osvětlení: **FAR** = 2%, **FRR** = 0,4%
- Stejný den, různé osvětlení: **FAR** = 2%, **FRR** = 9%
- Různé dny (> 1 rok): **FAR** = 2%, **FRR** = 11% (43%)

Příklady aplikací:

- Letiště
- Přístupové systémy – Internet
- Přístupové systémy – budovy
- Docházkové systémy
- Policejní využití
- Kontrola návštěvníků akcí s velkým počtem lidí



Obrázek 7.1: Vlastní obličeje (*Eigen-Faces*)



**Vlastní obličeje** (*Eigen-Faces*, MEF) (Obr. 7.1) – jedná se o rozklad snímku obličeje na snímky s různými intenzitami, které se po vahování spojí do výsledného obrázku, který se poté používá k dalším účelům v oblasti rozpoznávání obličeje.

## 7.1 Detekce obličeje

Jedná se o první krok ve zpracování obličejů. Obličeje jsou nasnímány za různých osvětlení. Obličeje se liší v barvě, pozici, rozměrech, orientaci, 3D pozici, výrazu obličeje atd. Problémem je větší množství obličejů s barevným pozadím – ukázka na obrázku 7.1.1.

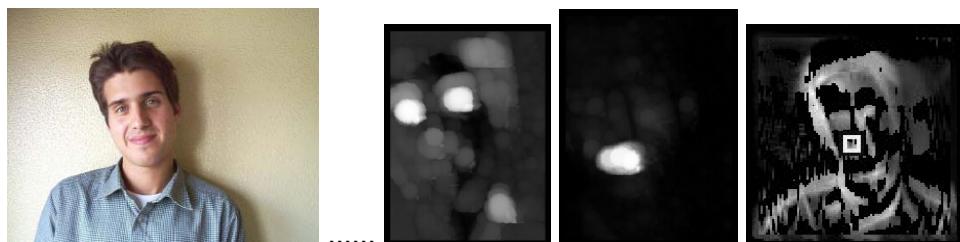


Obrázek 7.1.1: Ukázka složité scény pro detekci obličejů



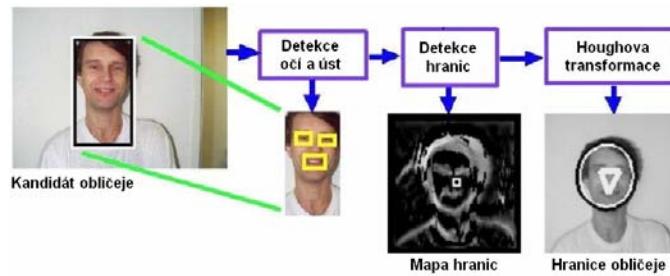
**Algoritmus detekce obličejů** (detekce obličejů nejčastěji v barevných snímcích) – viz obrázek 7.1.2:

1. Kompenzace osvětlení
2. Detekce tónu kůže
3. Detekce rysů obličeje (oči, ústa a ohrazení obličeje)



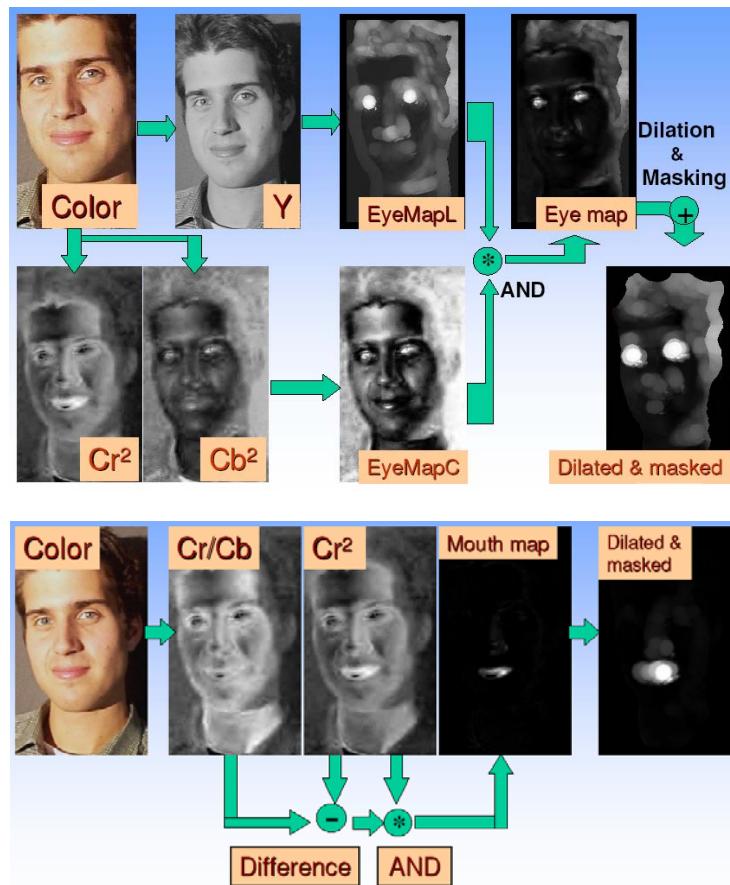
Obrázek 7.1.2: Postup při detekci obličeje

Hranice obličeje (výpočet založen na velikosti samotného obličeje a orientacích gradientů) – viz obrázek 7.1.3.



Obrázek 7.1.3: Zjištění hranic obličeje

Postup detekce očí a úst je založen na převodu barevných prostorů RGB  $\Rightarrow$  YCb-Cr. Postup této detekce je znázorněn na obrázcích 7.1.4a a 7.1.4b.



Obrázek 7.1.4: Postup detekce a) očí (nahoře); b) úst (dole) [Jai04]

## 7.2 2D rozpoznávání obličeje

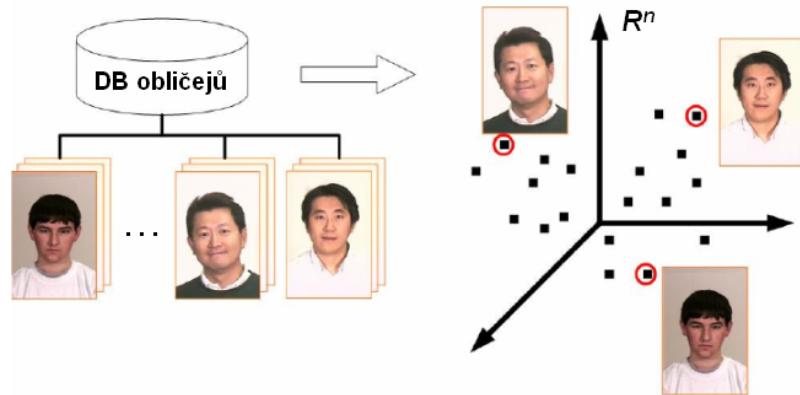


**Vektorová reprezentace** – 2D obrázek je považován za vektor, provedeme-li spojení jednotlivých řádků (sloupců) do jednoho vektoru.

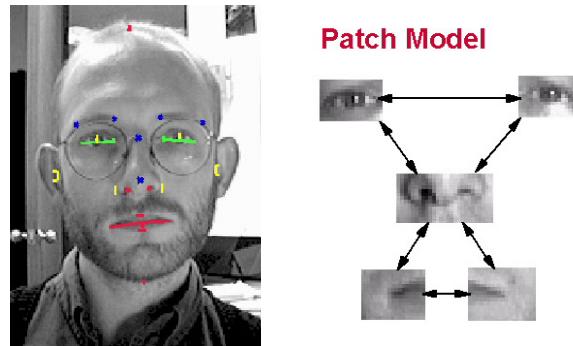
Obrázek obličeje odpovídá bodu v  $n$ -rozměrném prostoru  $R^n$  ( $n = p \times q$ , kde  $p$  je výška a  $q$  je šířka obrázku).

**Prostor obličejů** (Obr. 7.2.1) – množina obličejů rozvrstvených v prostoru  $R^n$  (distribuce obličejů v tomto prostoru).

**Metriky** – v obličeji se hledají (po kroku detekce) hlavní rysy, jako poloha nosu, úst a očí (obrázek 7.2.2). Potom přichází detekce obočí, uší, rtů apod. Porovnání probíhá na základě vzdáleností mezi jednotlivými body, přičemž se opět využívají toleranční limity.



Obrázek 7.2.1: Prostor obličejů  $R^n$



Obrázek 7.2.2: Metriky obličeje – Patch Model

**DEF**

Původní prostor obličejů o rozměrech  $p \times q$  je příliš velký; data obličejů leží ve skutečnosti v prostoru s mnohem nižší rozmanitostí. Identifikací a parametrizací redukovaného prostoru obličejů se zabývá lineární (podprostorová) analýza. **Lineární analýza** – hledání lineární transformace  $W$ , která mapuje originální vektor obličeje  $X$  na vektor projekčních koeficientů  $Y$ , tedy:  $Y = W^T X$ . Je-li  $d$  dimenzí  $Y$  a  $n$  dimenzí  $X$ , pak platí:  $d \ll n$ . Jedná se tedy o srovnávání vektorů příznaků a následné přiřazení do prostoru obličejů (viz klasifikace).



### Metoda PCA = *Principal Component Analysis*

$$\text{Průměr: } \mu = \frac{1}{N} \sum_{i=1}^N x_i \quad (7.1)$$

$$\text{Matice rozptylu: } S_T = \sum_{i=1}^N (x_i - \mu)(x_i - \mu)^T \quad (7.2)$$

$$\text{Vlastní dekompozice: } S_T e = \lambda e \quad (7.3)$$

Jedná se o učení bez učitele. Konstruuje prostor obličejů bez použití třídy (kategorie) obličeje.

Metoda PCA - algoritmus vlastních obličejů (dekompozice) – obrázek 7.1:

1. Kolekce  $x_i$  z  $n$ -dimenzionální množiny dat  $X$ ,  $i=1,\dots,N$ .
2. Centrování (korekce) všech bodů; spočti střední hodnotu  $m_x$  a odečti od každého bodu,  $x_i - m_x$ .
3. Spočti kovariační matici  $C$ .
4. Determinuj vlastní hodnoty a vlastní vektory matice  $C$ .
5. Seřaď vlastní hodnoty (a odpovídající vlastní vektory) ve vzestupném směru.
6. Vyber prvních  $k$  vlastních vektorů a generuj množinu dat v nové reprezentaci.
7. Testový obrázek v dané projekci (po odečtení střední hodnoty  $m_x$ ) je porovnán s trénovacími obrázky za použití měřítka podobnosti. Výsledkem je nejbližší obrázek z trénovací sady, který je nejbližší testovému obrázku.



### Metoda LDA = *Linear Discriminant Analysis*

Učení s učitelem, používá mezi- a vnitro-třídní informaci.



$$\text{Transformační matice: } W_{LDA} = \arg \max_W \frac{|W^T S_B W|}{|W^T S_W W|} = [W_1, W_2, \dots, W_k] \quad (7.4)$$

$$\text{Matice rozptylu „vnitro-třídní“: } S_B = \sum_{i=1}^C N_i (\mu_i - \mu)(\mu_i - \mu)^T \quad (7.5)$$

$$\text{Matice rozptylu „mezi-třídní“: } S_W = \sum_{i=1}^C \sum_{x_k \in X_i} (x_k - \mu_i)(x_k - \mu_i)^T \quad (7.6)$$

Výsledkem je množina generalizovaných vlastních vektorů  $\{w_i \mid i=1,\dots,k\}$  na základě  $S_B$  a  $S_W$ , odpovídající k největším (generalizovaným) vlastním hodnotám  $\{\lambda_i \mid i=1,\dots,k\}$  tak, že:  $S_B w_i = \lambda_i S_W w_i$ .

**FLD (Fisher Linear Discriminant)** – porovnáváním obličejomých částí a částí nenáležícím obličeji se vytvoří kandidáti, ze kterých se potom poskládají Fisherovy obličeje. Slouží k jednoznačné detekci obličeje, přičemž se používají různé prahy.



Obrázek 7.2.3: Fisherovy obličeje



### Metoda AAM = *Active Appearance Model*



Lineární konstrukce modelu, učení s učitelem. Nejprve se do obrazu vloží významné body, které se dle geometrie obličeje extrahují a použijí pro vygenerování textury obličeje bez formy (obrázek 7.2.4).

$$\text{Model tvaru: } s = (x_1, y_1, \dots, x_n, y_n)^T, \quad s = \bar{s} + P_s b_s \quad (7.7)$$

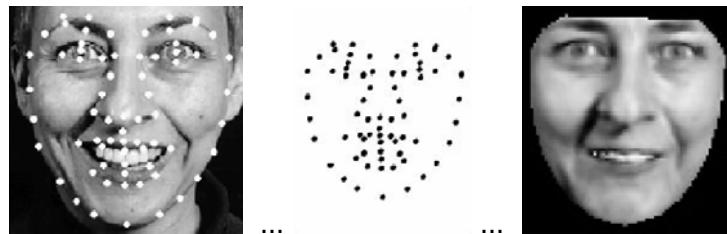
$$\text{Model výskytu: } g = (I_1, \dots, I_M)^T, \quad g = \bar{g} + P_g b_g \quad (7.8)$$

$$\text{Kombinovaný model: } b = \begin{pmatrix} W_s b_s \\ b_g \end{pmatrix} = \begin{pmatrix} W_s P_s^T (s - \bar{s}) \\ P_g^T (g - \bar{g}) \end{pmatrix} \xrightarrow{\text{PCA}} b = Qc \quad (7.9)$$

Nastavení modelu – minimalizace cílové funkce (rozdíl úrovně šedé mezi daným obrazem a uloženou šablonou):  $\Delta = |\delta I|^2$

Jedná se o prohledávání učením, komentovaný model (skutečné parametry).

Relace: známá velikost modelu  $\leftrightarrow$  pozorovaný rozdílový vektor.



Obrázek 7.2.4: Postup metody AAM (*Active Appearance Model*)

Použití vícenásobné regrese k učení poměrů a k predikci velikostí během prohledávání. Příklad použití metody (více iterací) je uveden na obrázku 7.2.5.

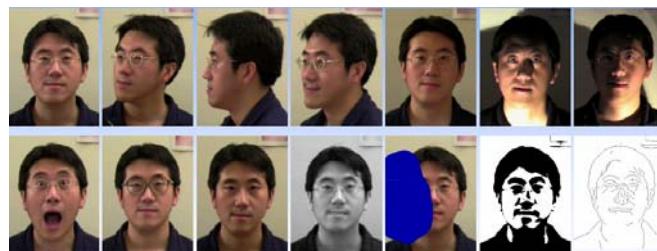


Obrázek 7.2.5: Příklad iterací u metody AAM (*Active Appearance Model*)

### 7.3 3D rozpoznávání obličeje<sup>2</sup>



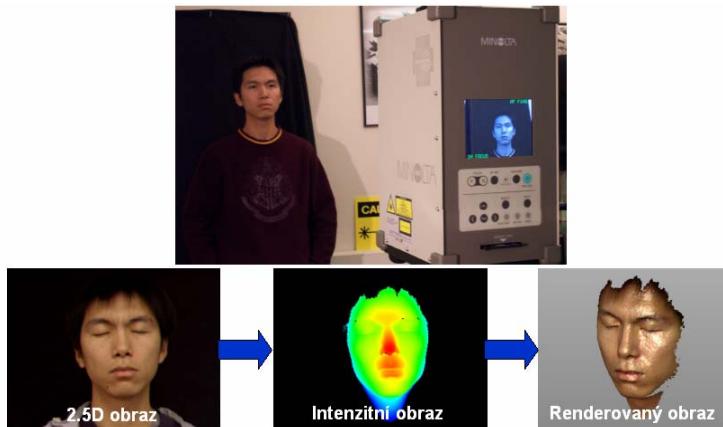
Výzvy: Vnitrotřídní variabilita (obrázek 7.3.1) – změna v osvětlení, výrazu, pozici, doplňcích atd. První výzvou je návrh algoritmu pro rozpoznávání 3D obličeje, který vykazuje **FAR** = 0,1%. Hlavní důraz je ale stále kladen na 2D systémy. Druhá výzva – I komerční systémy se zaměřují na čelní snímky a neutrální výrazy v obličeji. Možnosti?



Obrázek 7.3.1: Vnitrotřídní variabilita – změny v obrazu jedince

Co se aplikací týče, těmito zařízeními se zabývá především firma *a4vision*. Jejich zařízení pro snímání 3D obrázků obličeje obsahují strukturované osvětlení nebo infračervené osvětlení. Existují ale i přenosné snímače (např. pro policii).

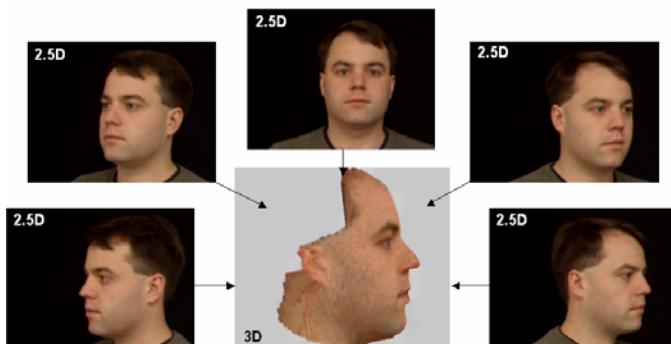
Snímání 3D obrazu obličeje je znázorněno na obrázku 7.3.2. Nejprve se nasnímají 2.5D obrazy obličeje, z nich se odvodí intenzitní obraz a následně se vyrenderuje výstupní obraz obličeje.



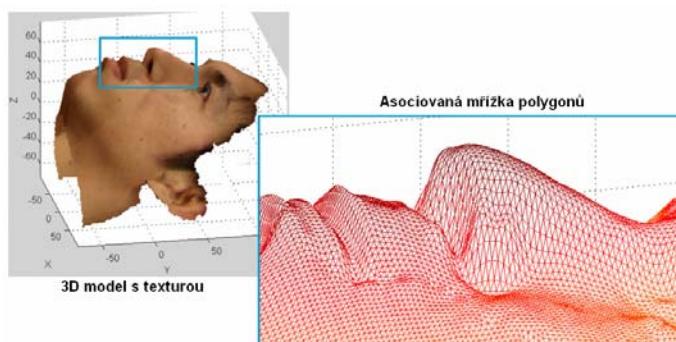
Obrázek 7.3.2: Průběh snímání 3D obrazu obličeje



Na sestavení **3D modelu** z pěti **2.5D** scanů se používá např. *Geomagic Studio* nebo *Rapid Form Software* – příklad je vyobrazen na obrázku 7.3.3 a 7.3.4. Nejprve se musí odstranit šum a vyplnit díry ve 2.5D scanech. Pak se vytvoří 3D model z 50 tisíců polygonů.

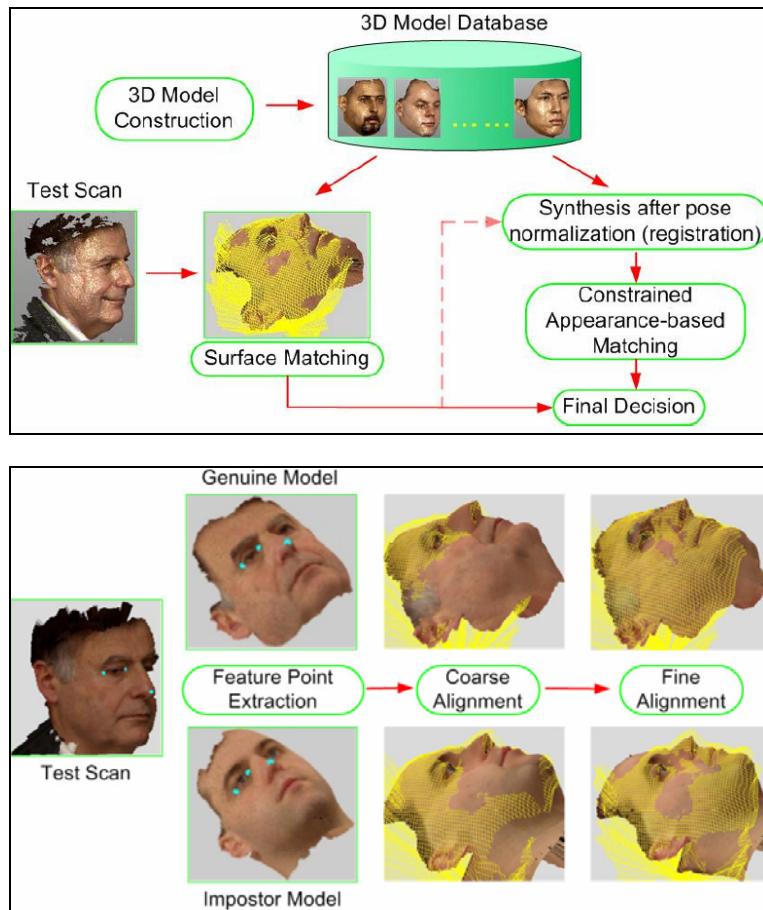


Obrázek 7.3.3: Konstrukce 3D modelu z 2.5D scanů



Obrázek 7.3.4: Reprezentace dat 3D obličeje

Na obrázku 7.3.5 je zobrazen algoritmus pro rozpoznávání 3D obličejů a porovnání povrchů.

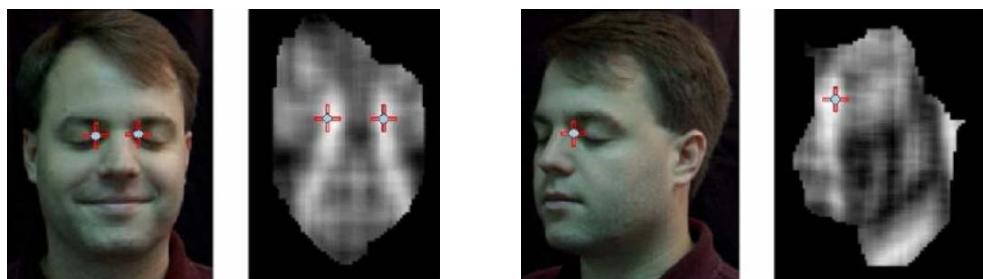


Obrázek 7.3.5: Systém pro rozpoznávání 3D obličejů (nahoře) a porovnání povrchů (dole) [Dit04]

Pro **indexy tvaru** (zakřivení obličeje) platí vztah:

$$S(p) = \frac{1}{2} - \frac{1}{\pi} \tan^{-1} \frac{\kappa_1(p) + \kappa_2(p)}{\kappa_1(p) - \kappa_2(p)} \quad (7.10)$$

**Detekce bodů rysů** spočívá v identifikaci bodů rysů v prostoru indexů tvarů. Na vnitřní a vnější straně očí jsou hodnoty indexů tvarů rovny prakticky nule. Příklad je uveden na obrázku 7.3.6 (varianta A je pohled zepředu a B je semiprofil).



Obrázek 7.3.6: Detekce bodů rysů (A vlevo, B vpravo) [Jai04]



### Hrubé zarovnání

3D rigidní transformace  $T$  je approximována korespondencí 3 bodů:

$$T = T_{C_p} \cdot R_{p'} \cdot \Theta \cdot R_A \cdot T_{C-a} \quad (7.11)$$

$T$  je totální transformace z množiny  $a$  na  $p$ ,  $T_{C-a}$  je translace do středu přes počátek,  $R_A$  je rotace do  $xy$ -roviny,  $\Theta$  je optimální rotace z  $xy$ -roviny do souřadného systému  $p$ ,  $R_{p'}$  je rotace z  $xy$ -roviny do souřadného systému  $p$  a  $T_{C_p}$  je translace za účelem stejného centroidu jako  $p$ .



### Jemné zarovnání

Použití algoritmu **ICP** (*Iterative Closest Point*)

- Chenův algoritmus
- Besleův algoritmus
- Hybridní algoritmus (Chenův + Besleův v cikcak módu)

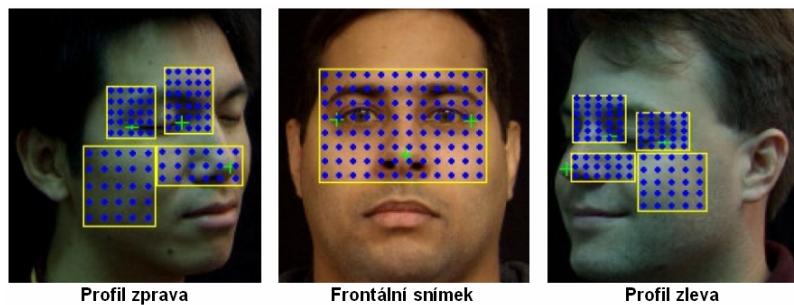
Výběr kontrolních bodů v testovém snímku a transformování testového snímku za účelem minimalizace vzdálenosti mezi kontrolními body a povrchem modelu.

#### **ICP algoritmus:**

1. Vyber kontrolní body v jedné množině.
2. Najdi nejbližší body v množině druhé (korespondence).
3. Vypočti optimální transformaci mezi oběma množinami na základě aktuální korespondence.
4. Transformuj body; opakuj č. 2 až do konvergence.

Výběr kontrolních bodů (obrázek 7.3.7):

- Regiony málo tvárné (malá změna výrazů obličeje)
- Pokrytí co největší plochy obličeje



Obrázek 7.3.7: ICP – Výběr kontrolních bodů



### Porovnání založené na vzhledu

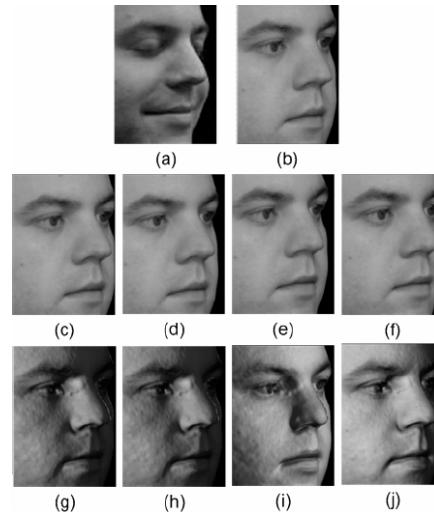
$$\text{Transformační matice: } W_{LDA} = \arg \max_w \frac{|W^T S_B W|}{|W^T S_W W|} \quad (7.12)$$

kde  $c$  je počet tříd obličejů a  $N_i$  je počet vzorků třídy  $i$ .

$$\text{Matice rozptylu mezi třídami: } S_B = \sum_{i=1}^c N_i (\mu_i - \mu)(\mu_i - \mu)^T, \quad \mu = \sum_{i=1}^N x_i \quad (7.13)$$

$$\text{Matice rozptylu uvnitř třídy: } S_W = \sum_{i=1}^c \sum_{x_k \in X_i} (x_k - \mu_i)(x_k - \mu_i)^T \quad (7.14)$$

Vícenásobné vzorky jsou třeba k výpočtu matic rozptylů  $\Rightarrow$  **syntéza obličeje**. Příklad porovnání založeném na vzhledu je na obrázku 7.3.8 ((a) – 2.5D testový snímek; (b) 3D model po provedení normalizace (zarovnání); (c-f) syntetizované obrázky z (b) s posunutím v horizontálních a vertikálních směrech; (g-j) syntetizované obrázky se změnami osvětlení).



Obrázek 7.3.8: Příklad porovnání založeném na vzhledu

### Omezené porovnávání založené na vzhledu

Použití normalizace (nutná pro porovnávání založeném na vzhledu se závislostí na pohledech) je provedeno po registraci tvarů. Použití Phongova stínování k syntéze světelých efektů. Porovnání povrchů nabídne nejlepších  $M$  kandidátů testového snímku; syntéza vzhledu je provedena pouze pro těchto  $M$  modelů. Porovnání na základě vzhledu je provedeno na  $M$  třídách.

$$\text{Vzdálenost porovnání tvarů: } MD_{ICP} = \sqrt{\frac{1}{N_c} \sum_{i=1}^{N_c} d^2(\Psi(p_i), S_i)} \quad (7.15)$$

$$\text{Porovnání na základě vzhledu: } MS_{LDA} = \frac{\langle \vec{V}_1, \vec{V}_2 \rangle}{\|\vec{V}_1\| \cdot \|\vec{V}_2\|} \quad (7.16)$$

$$\text{Akumulace jistoty: } MD_{comb} = MD_{ICP} + \alpha \cdot (1 - MS_{LDA}) / 2 \quad (7.17)$$



Obrázek 7.3.9: Příklady 3D modelů

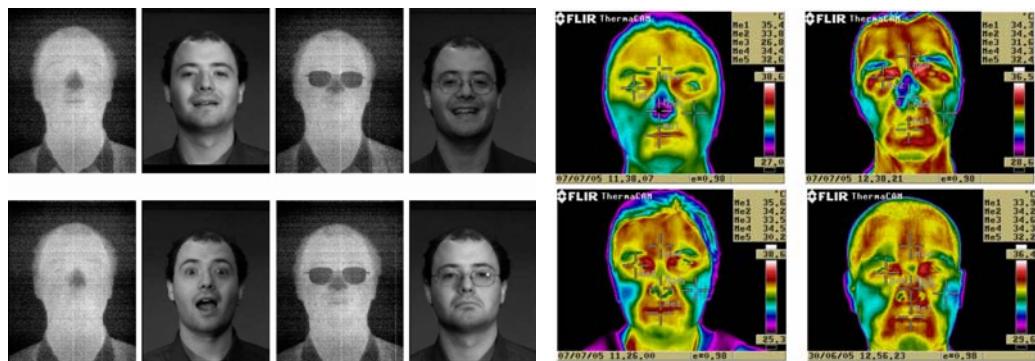
## 7.4 Rozpoznávání termogramu obličeje



Pro záznam snímků se používá termokamera, u které je nutné správně nastavit (dodržet) následující parametry [Soc01, TT02]:

- Emisní koeficient kůže:  $e = 0,98$
- Konstantní vzdálenost (správné zaostření)
- Relativní vlhkost okolí
- Teplota okolí

Záznamem jsou obrázky termomap obličeje (viz obrázky 7.4.1). V nich se hledají opět obdobným způsobem jako u klasického 2D rozpoznávání obličejů pozice očí, úst, nosu a hranice obličeje. Dalším krokem je překryv obou termooibličejů (zahrnání). Možnosti: vlastní obličeje / algoritmus ARENA. Výsledným krokem je zjištění korespondence ploch a přibližného tepelného záření pro jednotlivé plochy.



Obrázek 7.4.1: Černobílé a barevné termosnímky obličeje



Obrázek 7.4.3: Motivace na cvičení – Termokamera AGA Thermovision 110



V této kapitole jsme se nejprve věnovali detekci obličeje, což je v podstatě nejdůležitější proces před samotným rozpoznáním obličeje. Detekce obličeje je relativně složitý proces, zejména v prostředí, kde je příliš pestrobarevné pozadí (vykazující podobnost s prvky obličejů), nebo v obrázcích, kde se nachází velký počet lidí (často i s částečně zakrytými částmi obličejů).

2D rozpoznávání obličejů funguje jen na základě klasických snímků. Předpokladem pro dobré rozpoznání je kvalitní detekce obličeje ve snímku a obličej by neměl být překryt žádnou další částí (jakýkoliv předmět apod.).

3D rozpoznávání obličejů vychází ze 2.5D snímků, z nichž se složí 3D snímek. Zde jsou důležité oblasti zakřivení, kde se počítají koeficienty křivky.

Speciální částí je rozpoznávání termosnímků obličejů. Ke získání snímků je třeba použít termokameru, což zvyšuje pořizovací náklady celého systému, ale zase zvyšuje odolnost oproti některým vlivům prostředí, jako je např. osvětlení.

 Příklady otázek:

1. Jak funguje detekce obličeje?
2. Vyjmenujte metody pro rozpoznávání 2D obličeje. Stručně popište.
3. Popište skládání 3D obličeje ze 2.5D scanů.
4. Co jsou indexy tvarů?
5. Popište funkční princip rozpoznávání termogramu obličeje.

 Odpovědi:

1. Strana 53 – 54.
2. Strana 55 – 57.
3. Strana 58.
4. Strana 59.
5. Strana 62.



## 8. Rozpoznávání podle duhovky a sítnice



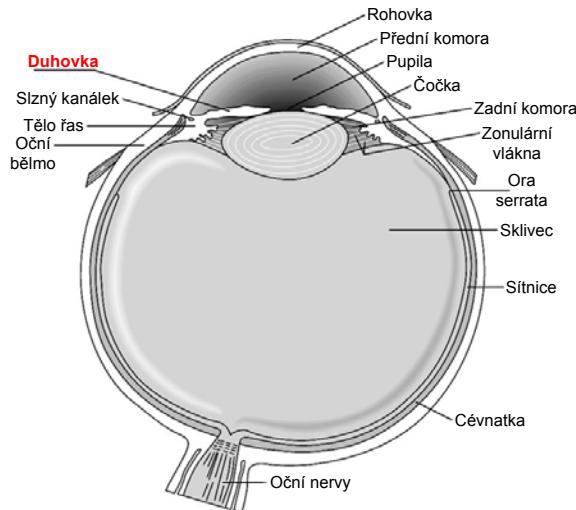
Naše oko je rovněž zcela unikátní a může sloužit k biometrickým účelům. V oku se nachází dvě stejné části, které vykazují dokonce i relativně vysokou entropii. První je *duhovka oka*, zvaná též (nesprávně) panenka a druhou částí je *sítnice*, která leží uvnitř oka a není pozorovatelná pouhým pohledem, oproti duhovce.

### 8.1 Rozpoznávání podle duhovky oka



**Duhovka** je onou barevnou částí oka, kterou u jiných můžeme pozorovat pouhým pohledem. Duhovka kontroluje úroveň světla, které vstupuje do oka – podobnost se clonou. Černý otvor ve středu duhovky se nazývá *pupila* (panenka). Duhovka je spojena s jemnými svaly, které duhovku budou rozšiřovat a nebo zužovat. Barva, textura a vzor duhovky jsou u každé osoby jiné → lze porovnat s rozlišovací schopností otisků prstů.

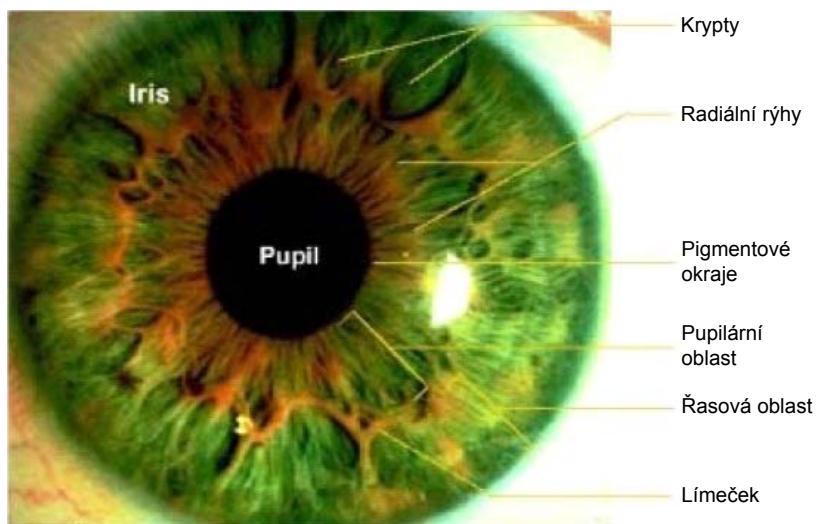
*Svírací sval* leží podél hranice duhovky a stahuje duhovku při silnějším světle. *Roztahovací sval* leží příčně, podobně jako výplet jízdního kola, a roztahuje duhovku při slabším osvětlení. Duhovka je plochá a rozděluje oko na přední a zadní část. Na obrázku 8.1.1 je vyobrazeno složení lidského oka.



Obrázek 8.1.1: Složení lidského oka



Barva duhovky je způsobena barvivem, které se nazývá **melanin**. Duhovka je přední částí oka a je zodpovědná za korekci množství světla vstupujícího do oka. Nachází se mezi pupilou a oční bělmou. Velikost duhovky se pohybuje kolem 11 mm. Vizuální textura se formuje během prvních dvou let života a základní struktura zůstává během života neměnná. Struktura duhovky je znázorněna na obrázku 8.1.2. Duhovka u dvojčat je odlišná!



Obrázek 8.1.2: Struktura duhovky – rysy



*Výhody* použití duhovky pro rozpoznávání:

- Stabilní během života jedince
- Pořízení snímku je neinvazivní
- Velikost šablony je malá
- Vnitřní orgán – malé možnosti změn
- Vysoká náhodnost informace uvnitř duhovky

*Nevýhody* použití duhovky pro rozpoznávání:

- Možnost podvrhu kontaktními čočkami
- Strach uživatelů z poškození oka
- Patentovaný algoritmus (spolehlivý)

**Vliv osvětlení** na snímání duhovky:

- Viditelné světlo
  - Viditelné vrstvy
  - Méně texturní informace
  - Melanin absorbuje viditelné světlo
- Infračervené světlo
  - Melanin reflektuje většinu infračerveného světla
  - Preferovaná technologie pro rozpoznávání duhovky



Nyní si uvedeme nějaké příklady praktických aplikací: nejvíce rozšířené jsou tyto systémy ve Spojených arabských emirátech, kde se nachází na letištích a v přistavech (ca 3,8 miliónů porovnání denně). Dalším příkladem je např. systém na letišti Schiphol v Holandsku, který využívají lidé s vysokou frekvencí letů. V ČR zatím tento systém nebyl nasazen v praktické aplikaci. Dalším příkladem je aplikace ve městě Tokyo. Pracovníci firmy Condominum používají tento systém ke

vstupu a zároveň je přivolán výtah, který je odveze k jejich kanceláři. V Afgánistánu používá UNHC (United Nations High Commission) rozpoznávání duhovky ke kontrole přistěhovalců z okolních zemí.



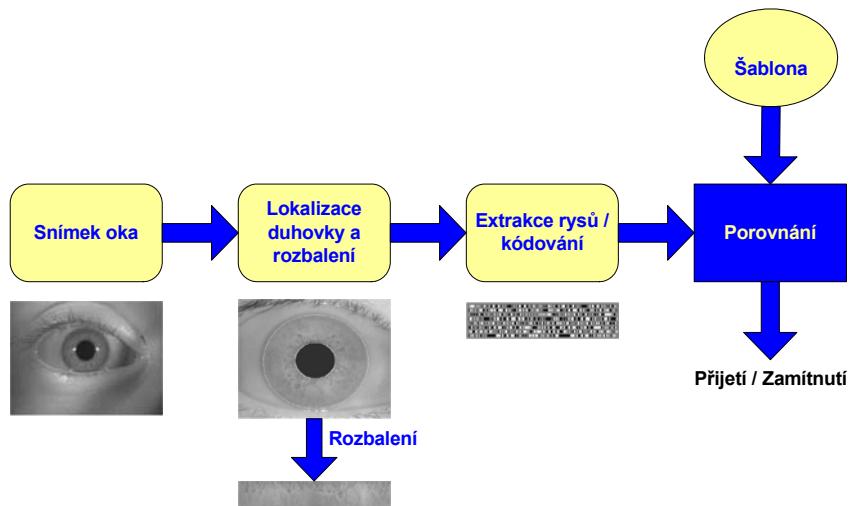
### Schémata rozpoznávání duhovky [Dau00]

- *Gaborova demodulace* (Daugman, PAMI 1993)
- *Waveletové rysy* (Lim, Lee, Byeon, Kim, ETRI J 2001)
- *Analýza nezávislých komponent* (Bae, Noh, Kim, AVBPA 2003)
- *Variace lokálních klíčů* (Ma, Tan, Wang, Zhang, IEEE TIP 2004)



### Gaborova demodulace (Daugmanův algoritmus)

Princip Daugmanova algoritmu je znázorněn na obrázku 8.1.3.



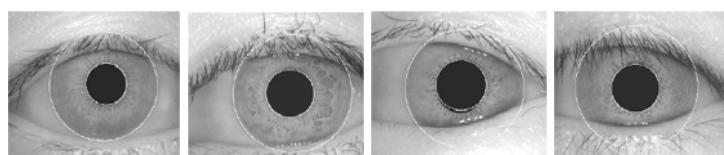
Obrázek 8.1.3: Princip Daugmanova algoritmu



Nejprve se ve snímku oka **lokalizuje duhovka** (hranice křivky). Duhovka je lokalizována pomocí následujícího operátoru:

$$\max_{(r, x_0, y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \int_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} ds \right| \quad (8.1)$$

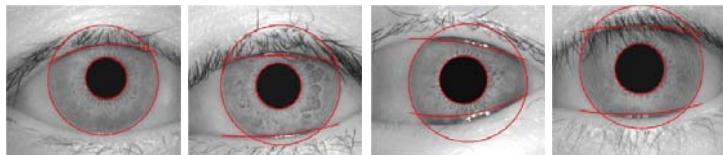
kde  $G_\sigma(r)$  je gaussovská funkce uhlazení (*smooth*) dle  $\sigma$ ,  $I(x, y)$  je hrubý vstupní obrázek a operátor hledá maximum v rozostřené parciální derivaci obrazu s ohledem na poloměr  $r$  a souřadnice středu  $(x_0, y_0)$ . Operátor je v podstatě kruhovým detektorem hran a vrátí maximum, pokud sdílí kandidátská kružnice střed pupily a poloměr. Příklady lokalizovaných duhovek jsou uvedeny v obrázku 8.1.4.



Obrázek 8.1.4: Příklady lokalizovaných duhovek



Dalším krokem je **lokalizace víčka**. Obdobným postupem, jakým se detekovala samotná duhovka, se určí pozice dolního a horní víčka oka. Část z předchozího vzorce, která slouží k detekci kontury se zamění z kruhové za obloukovou, přičemž splinové parametry jsou nastaveny dle standardních statistických metod odhadu, aby optimálně korespondovaly každé hranici očního víčka. Příklad lokalizovaných víček je uveden na obrázku 8.1.5.



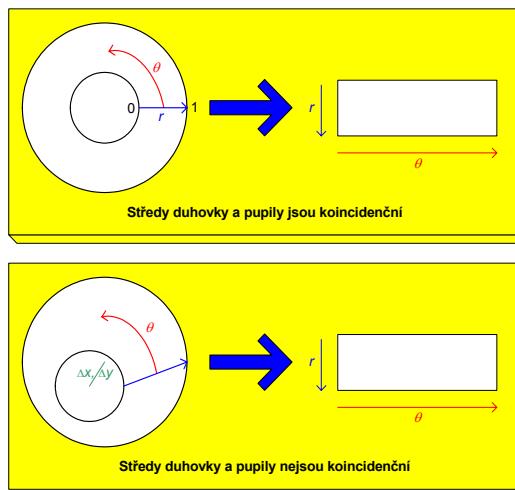
Obrázek 8.1.5: Příklady lokalizovaných víček



### Daugmanův model hrubého zarovnání

Model mapuje každý bod uvnitř duhovky do polárních souřadnic  $(r, \theta)$ , kde  $r$  je z intervalu  $<0,1>$  a  $\theta$  je úhel z intervalu  $<0,2\pi>$ .

Model kompenzuje rozšíření (dilataci) pupily a nekonzistenci ve velikosti díky reprezentaci v polárném souřadném systému, invariantnímu vůči velikosti a translaci. Model však nekompenzuje rotační nekonzistenci, která je řešena posunem šablony duhovky ve směru  $\theta$  ve fázi porovnávání, dokud obě šablony nedosáhnou shody. Zavedení souřadného systému je znázorněno na obrázku 8.1.6.



Obrázek 8.1.6: Zavedení souřadného systému Daugmanova algoritmu



### Kódování rysů duhovky:

- *Gaborovo filtrování v polárním souřadném systému*

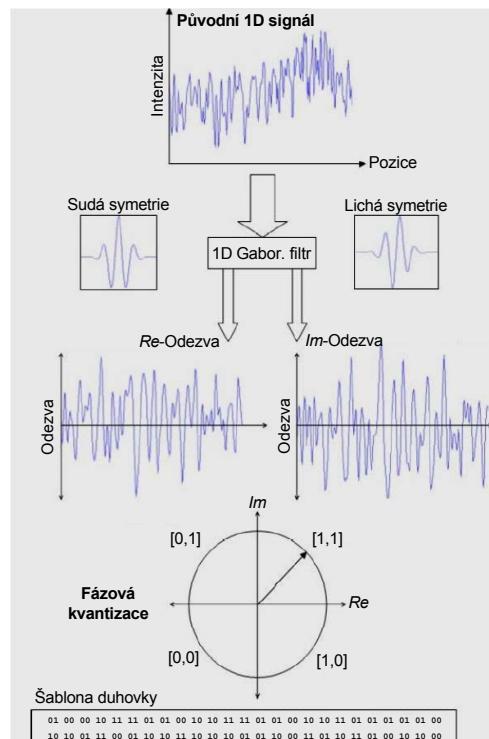
$$\circ \quad G(r, \theta) = e^{j\omega(\theta-\theta_0)} e^{-\frac{(r-r_0)^2}{\alpha^2}} e^{-\frac{j(\theta-\theta_0)^2}{\beta^2}} \quad (8.2)$$

- $(r, \theta)$  udává pozici v obrazu,  $(\alpha, \beta)$  určují efektivní výšku a délku a  $\omega$  je frekvence filtru
- Demodulace a fázová kvantizace

$$\circ \quad g_{\{\text{Re}, \text{Im}\}} = \text{sgn}_{\{\text{Re}, \text{Im}\}} \iint I(\rho, \phi) e^{j\omega(\theta_0 - \phi)} e^{-\frac{(r_0 - \rho)^2}{\alpha^2}} e^{-\frac{(\theta_0 - \phi)^2}{\beta^2}} \rho d\rho d\phi \quad (8.3)$$

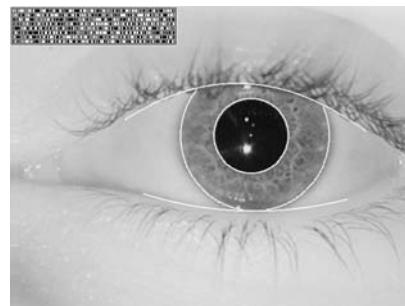
- $I(r, \phi)$  je hrubý obrázek duhovky v polárním souřadném systému a  $g_{\{\text{Re}, \text{Im}\}}$  je bit v komplexní rovině odpovídající znaménku reálné a imaginární části odezvy filtru.

Na obrázku 8.1.7 je znázorněn průběh kódování duhovky.



Obrázek 8.1.7: Ilustrace kódovacího procesu

Kód duhovky obsahuje 2.048 bitů, tj. 256 bytů. Velikost vstupního obrázku je  $64 \times 256$  bytů, velikost kódu duhovky je  $8 \times 32$  bytů a rozměr Gaborova filtru je  $8 \times 8$ . Příklad kódu duhovky je na obrázku 8.1.8.



Obrázek 8.1.8: Příklad kódu duhovky

### **Porovnávání kódů duhovky**

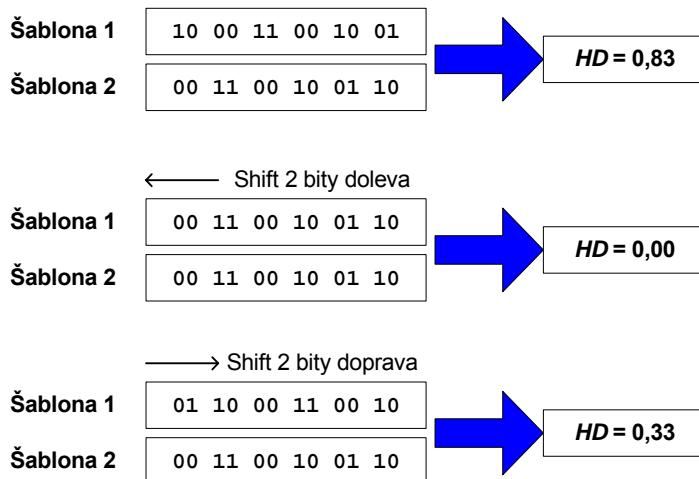
Porovnání je provedeno výpočtem Hammingovy vzdálenosti mezi oběma 256ti bytovými kódy duhovek. Hammingova vzdálenost mezi kódem duhovky  $A$  a  $B$  je dána (suma XOR mezi jednotlivými bity):



$$HD = \frac{1}{N} \sum_{j=1}^N A_j \otimes B_j \quad (8.4)$$

kde  $N=2.048$  ( $8 \times 256$ ), není-li duhovka zastíněna víčkem. V opačném případě jsou použity pro výpočet Hammingovy vzdálenosti pouze platné regiony.

Pokud jsou oba vzorky získány ze stejné duhovky, je Hammingova vzdálenost mezi nimi rovna či blízka nule (díky vysoké korelací obou vzorků). K zajištění rotační konzistence je jeden ze vzorů shiftován doprava/doleva a vždy je spočtena odpovídající Hammingova vzdálenost. Nejnižší hodnota Hammingovy vzdálenosti je potom brána jako výsledné skóre porovnání  $s$ . Příklad porovnání kódů duhovek za použití shiftování je uveden na obrázku 8.1.9.



Obrázek 8.1.9: Příklad porovnání kódů duhovek za použití shiftování



### Limitace duhovky

- Pořízení snímku duhovky vyžaduje spolupráci uživatele; uživatel musí stát v předdefinované vzdálenosti a pozici před kamerou.
- Náklady na systém s vysokou výkonností jsou nemalé.
- Obrázky duhovky mohou mít nízkou kvalitu, což vede k chybám při registraci / verifikaci / identifikaci.
- Bylo zjištěno [NN], že až 7% snímků duhovek je nevhodných k rozpoznávání, díky anomáliím očí (slzy v očích, dlouhé rásy nebo tvrdé kontaktní čočky).
- Duhovka se může změnit s přibývajícím časem:
  - Operace šedého zákalu
  - Nemoc *nystagmus* (třás oka)
  - Nemoc *anaridia* (zcela chybí duhovka)
- Slepí lidé jsou diskriminováni!
- Použití kontaktních čoček (k podvedení systému může být použita buď kontaktní čočka a nebo fotografie duhovky).
- Jednotlivé části duhovky se váží k různým vnitřním orgánům lidského těla → možnost zneužití ke zjištění zdravotního stavu osoby.



### Detekce živosti

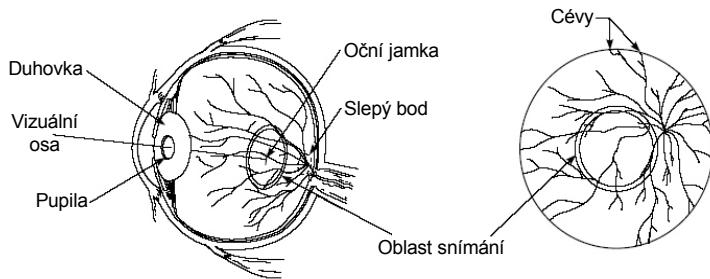
- Fotonická a spektrografická protiopatření:
  - Spektrografické vlastnosti tkání, tuků a krve
  - Spektrografické vlastnosti barviva melanin
  - Koaxiální zadní reflexe duhovky („červené oči“)
  - 4 Purkyňovy reflexe z povrchu rohovky a čočky
- Protiopatření pomocí reakcí (chování):
  - Nekontrolovatelné:
    - Pohyby pupily
    - Reflex pupily na světlo
  - Kontrolovatelné:
    - Pohyby oka / mrkání dle povelů

## 8.2 Rozpoznávání podle sítnice oka

Roku 1935 zjistili lékaři C. Simon a I. Goldstein, že žíly oka jsou u různých jedinců odlišné. Oko vykazuje podobný aparát jako mozek – struktura a žilní spletě zůstávají neměnné. Díky pozici uvnitř oka je sítnice chráněna před vlivy prostředí a tím je velmi vhodná k biometrickým účelům.



**Sítnice** detekuje obraz (Obr. 8.2.1), obdobně jako fotoaparát. Čočkou se upraví vstupní obraz a sítnici je zachycen, podobně jako na film. Sítnice je zásobována krví, která je přiváděna cévami. Tyto cévy jsou připojeny k očnímu nervu.



Obrázek 8.2.1: Funkční princip sítnice oka



K průmyslovým systémům můžeme řadit následující: Použití rozpoznávání duhovky je v oblastech s vysokými nároky na bezpečnost, jako např. nukleární vývoj, firmy vyvíjející a vyrábějící zbraně, vládní a armádní základny, tajné organizace. Systémy: *EyeDentify*, *Retinal Technologies*, *TPI* (Trans Pacific Int.), *RaycoSecurity*.

K osvětlení sítnice se používá infračerveného světla, protože sítnice je u této vlnové délky průhledná, zatímco cévy sítnice infračervené světlo reflektují. První funkční systém byl vytvořen v roce 1975, firmou *EyeDentify*.



Dvě možné **reprezentace sítnice** [Hil04]:

- Původní reprezentace má 40 bytů. Jedná se o informace o kontrastu za-kódované pomocí reálných a imaginárních souřadnic frekvenčního spekt-ra (FFT).
- Nová reprezentace má 48 bytů. Obsahuje informace o kontrastu v časo-vé doméně. Je rychlejší a efektivnější.



Šablona sítnice obsahuje pole 96ti čtyřbitových čísel kontrastů z 96ti scanů sou-středních kruhů v časové oblasti, tj.  $96 \times 4 = 48$  bytů. Intenzity v časové oblasti mohou nabývat hodnot v intervalu  $<-8,7>$ , přičemž se provádí normalizace na toto rozložení – úprava na 4 bity intenzitního rozložení.

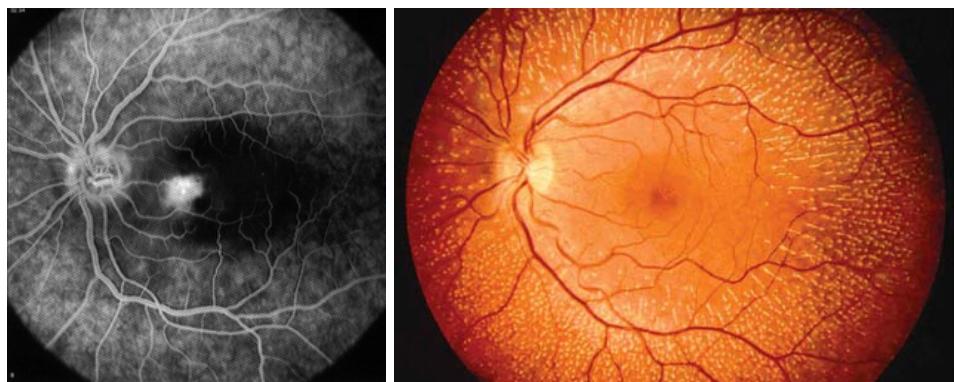
Pro porovnání dvou šablon se musí provést tyto kroky:

- Zarovnání (zajištění překryvu).
- Normalizace obou šablon (intenzit).
- Korelace obou šablon v časové oblasti (příp. Fourierova korelace).



### Limitace sítnice oka:

- Strach uživatelů z poškození oka.
- Zjištění zdravotního stavu – kórnatění cév apod.
- Omezené možnosti pro venkovní použití.
- Vysoká cena zařízení.
- Lidé s poruchou zraku (astigmatismus) nejsou schopni zaostřit oko na bod (funkčnost srovnatelná s měřením zaostřovací schopnosti oka u očního lé-kaře) a tím nedojde ke správnému vygenerování šablony.
- Možné zdroje chyb: nedostatečná fixace oka, chybná vzdálenost oka od snímače, nedostatečně rozšířená pupila, špinavý okulár, kontaktní čočky, interference světla...



Obrázek 8.2.2: Příklady scanů sítnice oka



V této kapitole jsme se dozvěděli podrobnosti o složení lidského oka. Zjistili jsme, že v oku se krom mnoha důležitých částí nachází dvě stěžejní ve smyslu biometrickém a těmi jsou duhovka a sítnice. Obě tyto oční součásti vykazují vhodnou strukturu (obraz duhovky a žilní síť sítnice) pro biometrické rozpoznávání.



Příklady otázek:

1. Jaký vliv má osvětlení na duhovku a sítnici oka?
2. Jak funguje Daugmanův algoritmus?
3. Vyjměte limitace duhovky oka.
4. Jak je reprezentována sítnice oka?
5. Vyjměte limitace sítnice oka.



Odpovědi:

1. Strana 65 a 70.
2. Strana 66 – 67.
3. Strana 69.
4. Strana 70.
5. Strana 71.



## 9. Rozpoznávání podle hlasu

Hlas patří do dynamických biometrických vlastností. Podstatnou složkou při záznamu hlasu je čas. V této kapitole si nejprve uvedeme základní pojmy a poté se dostaneme k metodám zpracování hlasu / řeči.

### 9.1 Základní pojmy



Složení hlasového traktu a mluvních orgánů je následující (Obr. 9.1.1):

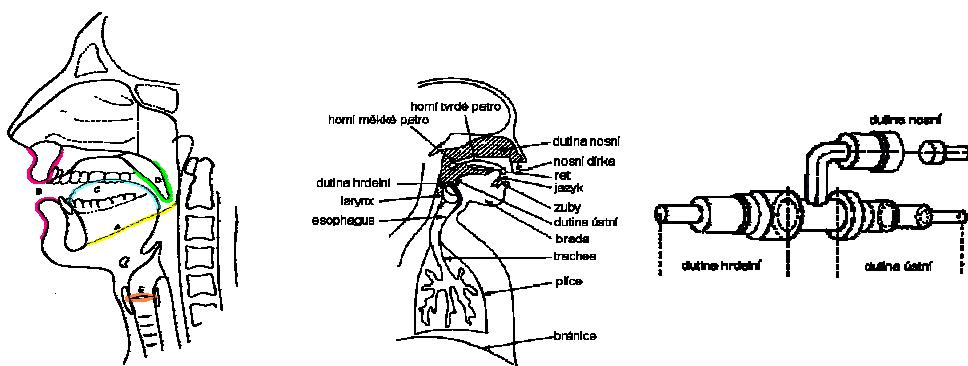
#### Vokální (hlasový) trakt

- A – dutina ústní – orální
- B – dutina nosní – nasální
- C – dutina hrdelní – laryngální
- D – velum, měkké patro



#### Aktivní mluvní orgány

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

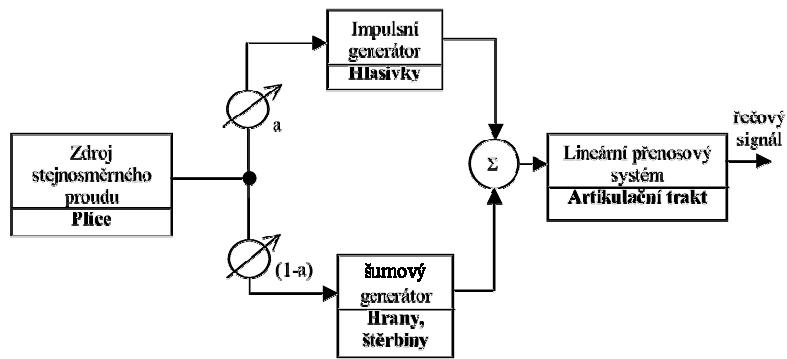


Obrázek 9.1.1: Složení hlasového traktu a mluvních orgánů



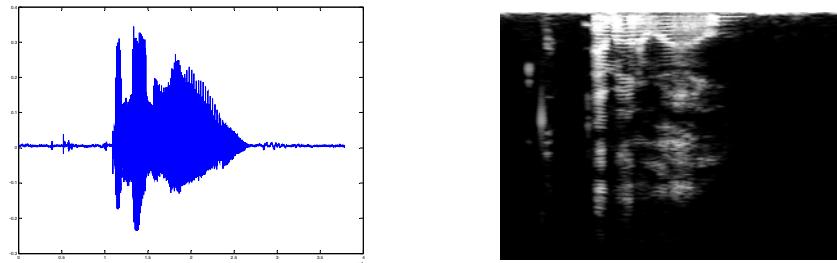
#### Generování řeči

- se skládá z (Obr. 9.1.2):
- Plíce (zdroj stejnosměrného proudu)
  - Hlasivky (impulsní generátor)
  - Hrany, štěrbiny (šumový generátor)
  - Artikulační trakt (lineární přenosový systém)



Obrázek 9.1.2: Generování řeči

Ukázka průběhu akustického tlaku a odpovídající spektrogram je uveden na obrázku 9.1.3.



Obrázek 9.1.3: Průběh akustického tlaku a jeho spektrogram

Tabulka 9.1.1: Typy hlásek podle tvoření

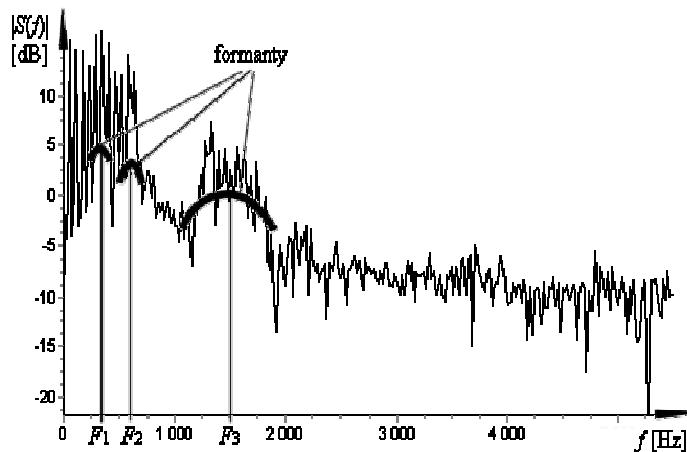
apertura (otevřenosť mluvidel)	strukturna (překážka v mluvidlech)			
	Konsonant			
vokál	Aproximanta	sonora	(pravý, vlastní) konsonant	
		lilkvida	nasála	znělý
např: [a] [e]	[j]	[l] [r]	[m] [n]	[b] [z]
				[f] [k]

vertikální posun jazyka	horizontální posun jazyka				
	anteriorní (přední)		centrální (střední)		posteriorní (zadní)
zavřené (=vysoké)	i				u
středové zavřenější	e				o
středové otevřenější		přednější a a		zadnější a a	
otevřené (=nízké)			a		

**Formanty** a jejich význam (Obr. 9.1.4):



- dobře charakterizují samohlásky
- jedinečné, ale dobře modifikovatelné
- vyšší formanty se hodí pro rozpoznávání mluvčích



Obrázek 9.1.4: Formanty [Ors05]

Průběh akustického tlaku – srovnání:



Pouhým okem lze někdy poznat rozdíly mezi mluvčími buď přímo z průběhu akustického tlaku nebo přímo ze spektrogramů. Ale pozor! Nemůžeme na to spoléhat! Za týden už může být vzorek naprostě jiný, ačkoliv byl od téhož člověka. Musíme tedy nalézt parametry vhodné pro rozpoznávání mluvčích.

## 9.2 Zpracování hlasu a jeho příznaky



Cyklus zpracování hlasového signálu je znázorněn na obrázku 9.2.1.



Obrázek 9.2.1: Cyklus zpracování hlasového signálu [Ors05]



**Digitální záznam řeči:** hlas (analogový signál)  $s_a(t) \rightarrow$  mikrofon  $\rightarrow$  A/D převodník – vzorkovací perioda  $T_s \rightarrow$  digitální signál  $s(n)$ :

$$s(n) = s_a(nT_s) \quad (9.1)$$

Na kvalitu záznamu mají vliv následující faktory:

- Různé typy mikrofonů (kvalita). Odstup signálu a šumu (SNR).
- Různé druhy prostředí (laboratoř × kancelář).

Typické hodnoty A/D převodu:  $f_s = 1/T_s \dots 8 \text{ kHz} - 22 \text{ kHz}$ , přesnost 8 – 16 bitů.



### Preemfáze

Zpracování signálu horní propustí nízkého rádu:

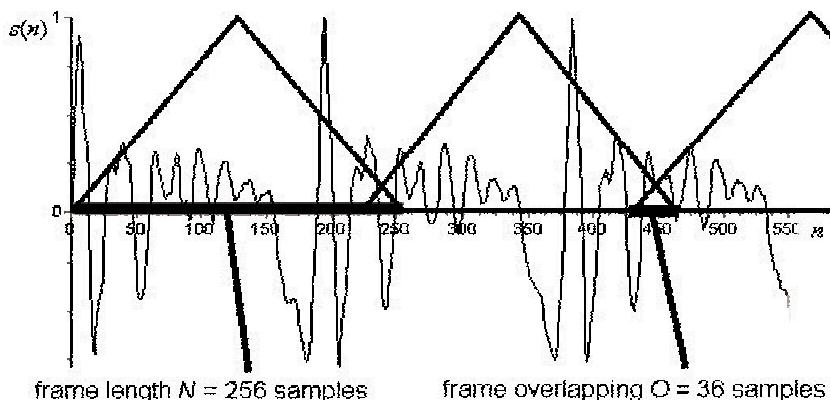
$$s_p(n) = s(n) - \lambda s(n-1) \quad (9.2)$$



Hodnota  $\lambda$  je typicky z intervalu  $<0,9;1>$ .

Důležitým krokem je **rozdělení signálu na okna** (rámce, tzv. rámcování) – viz Obr. 9.2.2. Typicky pracujeme jen s jednotlivými částmi signálu. Rámec: délka  $\sim 20 \text{ ms} \Rightarrow N$  vzorků. Často definujeme překrytí rámců  $O$ . Celkový počet rámců:

$$J = \int \left( \frac{N_{\text{total}}}{N - O} \right) \quad (9.2)$$



Obrázek 9.2.2: Rámcování (rozdělení signálu na okna) [Ors05]



Dalším krokem je **násobení digitálního signálu oknem**:

$$s_w(n) = s(n) \cdot w(n) \quad (9.3)$$



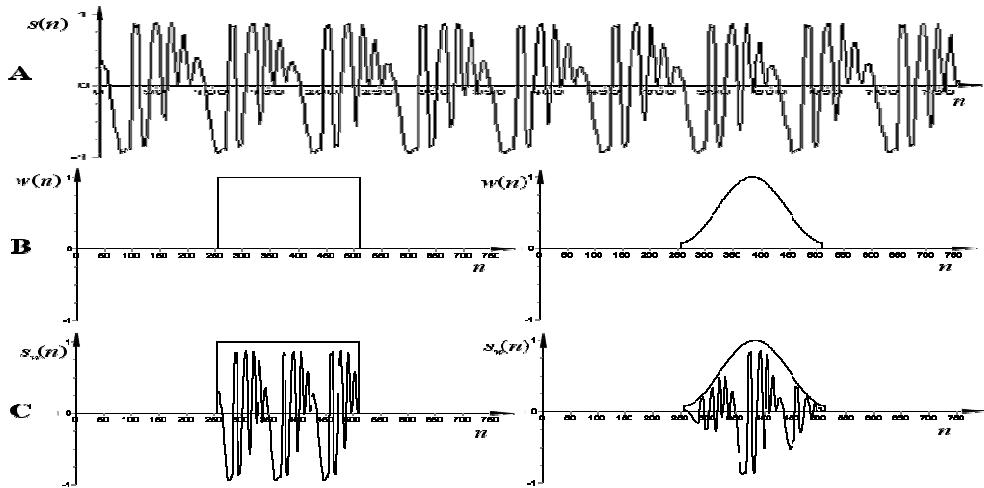
kde  $w(n)$  může být buď implicitní pravoúhlé okno:

$$w(n) = \begin{cases} 1 & 1 \leq n \leq N \\ 0 & jinak \end{cases} \quad (9.4)$$

nebo častěji užívané Hammingovo okno:

$$w(n) = \begin{cases} 0,54 - 0,46 \cdot \cos\left(2\pi \frac{n}{N}\right) & n \in \langle 1, N \rangle \\ 0 & n \notin \langle 1, N \rangle \end{cases} \quad (9.5)$$

Příklad násobení oknem je uveden na obrázku 9.2.3.



Obrázek 9.2.3: Násobení digitálního signálu oknem [Ors05]

**Energie** signálu může být spočtena následovně:

$$E(j) = \sum_{n=1}^N s^2(j, n) \quad (9.6)$$

**Počet průchodů nulou** lze spočítat takto:

$$Z(j) = \frac{1}{2} \sum_{n=1}^{N-1} |sign(s(j, n)) - sign(s(j, n+1))| \quad (9.7)$$

**Autokorelace:**

$$R(k) = \sum_{n=1}^{N-k} s(n) \cdot s(n+k) \quad (9.8)$$

**Predikce průběhu signálu:**

$$s_{pred}(n) = - \sum_{m=1}^M a(m) \cdot s(n-m) \quad (9.9)$$

Významným pojmem jsou **koefficienty lineární predikce LPC** (*Linear Prediction Coefficients*):

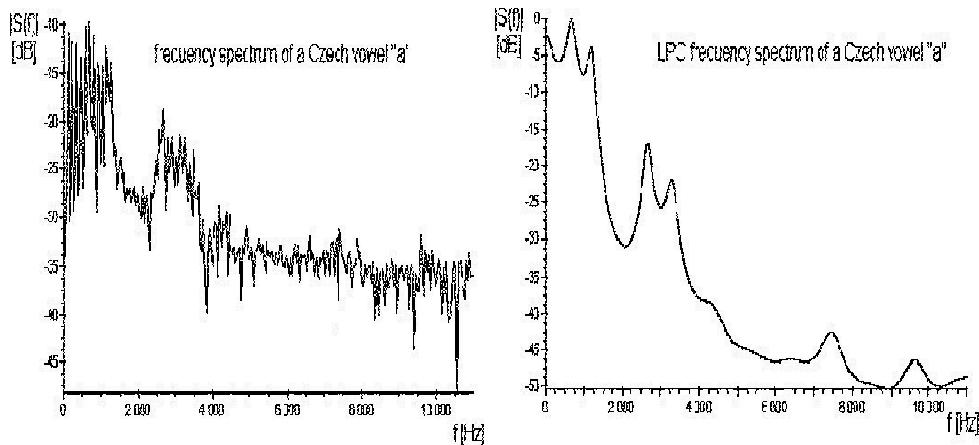
$$\begin{pmatrix} R(0) & R(1) & \dots & R(M-1) \\ R(1) & R(0) & \dots & R(M-2) \\ \vdots & \vdots & \ddots & \vdots \\ R(M-1) & R(M-2) & \dots & R(0) \end{pmatrix} \cdot \begin{pmatrix} a(1) \\ a(2) \\ \vdots \\ a(M) \end{pmatrix} = \begin{pmatrix} -R(1) \\ -R(2) \\ \vdots \\ -R(M) \end{pmatrix} \quad (9.10)$$

Za použití těchto koefficientů vypočteme následně **LPC spektrum** (Obr. 9.2.4):

$$S_{LPC}(k) = \left| 1 - \sum_{m=1}^M a(m) \cdot e^{-2\pi f_j \frac{k}{N}} \right|^{-2}, \quad k = 0, 1, \dots, N \quad (9.11)$$

Po výpočtu LPC spektra můžeme spočítat **dlouhodobé LPC spektrum**. Průměrné LPC  $a(m)$  vypočítáme stejně jako LPC, ale použijeme průměrnou hodnotu autokorelace:

$$\bar{R}(k) = \frac{1}{J} \sum_{j=1}^J R(j, k) \quad (9.12)$$



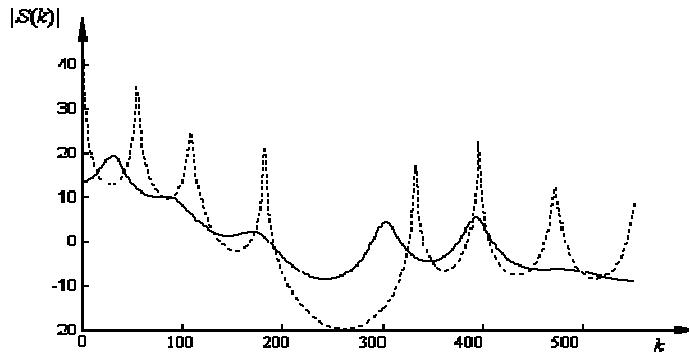
Obrázek 9.2.4: Ukázka LPC spektra české samohlásky „a“ [Ors05]

 Dále je nutno **normalizovat LPC**, jde v podstatě o zvýraznění extrémů. Normalizované autokorelační koeficienty (ukázka na obrázku 9.2.5):

$$R_{norm}(j, k) = R_a(0) \cdot R(j, 0) + \sum_{m=1}^M R_a(m) \cdot [R(j, |k-m|) + R(k, |k+m|)] \quad (9.13)$$

kde  $R_a(k)$  má následující vztah:

$$R_a(k) = \sum_{i=0}^{M-k} \bar{a}(i) \cdot \bar{a}(i+k) \quad (9.14)$$



Obrázek 9.2.5: Ukázka normalizovaného LPC spektra [Ors05]

### Mel-frekvenční kepstrum

 Melová škála:

$$B(f) = 1125 \cdot \ln\left(1 + \frac{f}{700}\right), \quad B^{-1}(b) = 700 \cdot \left(e^{\frac{b}{1125}} - 1\right) \quad (9.15)$$

Banka trojúhelníkových filtrů má následující tvar:

$$H(i, f) = \begin{cases} 0 & f < f(i-1) \\ \frac{f - f(i-1)}{(f(i+1) - f(i-1)) \cdot (f(i) - f(i-1))} & f(i-1) \leq f \leq f(i) \\ \frac{f(i+1) - k}{(f(i+1) - f(i-1)) \cdot (f(i+1) - f(i))} & f(i) < f \leq f(i+1) \\ 0 & f > f(i+1) \end{cases} \quad (9.16)$$

Centrální frekvence filtrů:

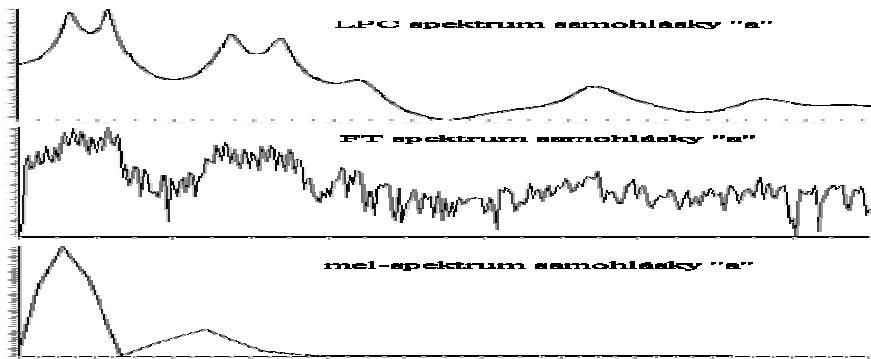
$$f(i) = \left( \frac{N}{F_s} \right) B^{-1} \left( B(F_{low}) + i \cdot \frac{B(F_{high}) - B(F_{low})}{I+1} \right) \quad (9.17)$$

Log-energie výstupů jednotlivých filtrů:

$$C(i) = \ln \left( \sum_{k=0}^{N-1} H(i, k) \cdot |S(k)|^2 \right), \quad i = 1, 2, \dots, I \quad (9.18)$$

Mel-kepstrum (ukázka na obrázku 9.2.6):

$$c(j) = \sum_{i=0}^{I-1} C(i) \cdot \cos \left( \pi n \frac{i-1}{2I} \right), \quad j = 0, 1, \dots, I \quad (9.19)$$



Obrázek 9.2.6: LPC-, FT- a mel-spektrum samohlásky „a“ [Ors05]

### Detecte řečové aktivity

 Detecte řečové aktivity slouží k nalezení počátků a konců slov (náročné téma). Existuje mnoho metod, mají různé výsledky – otázka = která je nejlepší? Metody:

- sledování obálky signálu
- rozdílnost příznaků
- neuronové sítě

**Sledování obálky** = odlišení signálu a šumu podle jejich energie (obecně – energie šumu < energie řečového signálu)  $\Rightarrow$  stanovíme prah  $S$ :

$$S = \frac{1}{2} \cdot \left[ \frac{1}{N_{noise}} \cdot \sum_{n=1}^{N_{noise}} S_{noise}(n) + \frac{1}{N_{sig}} \cdot \sum_{n=1}^{N_{sig}} S_{sig}(n) \right] \quad (9.20)$$



### **Metoda rozdílnosti příznaků:**

Zakládá se na sledování relativních změn autokorelačního koeficientu  $R(0)$ .

Určení křivky  $B(j)$ :

$$B(j) = b \cdot \frac{|R(j + l_1, 0) - R(j - l_2, 0)|}{R(j + l_1, 0) + R(j - l_2, 0)} + \sum_{k=1}^K |R(j + l_1, k) - R(j - l_2, k)| \quad (9.21)$$

Vyhlazení průběhu  $B(j)$ :

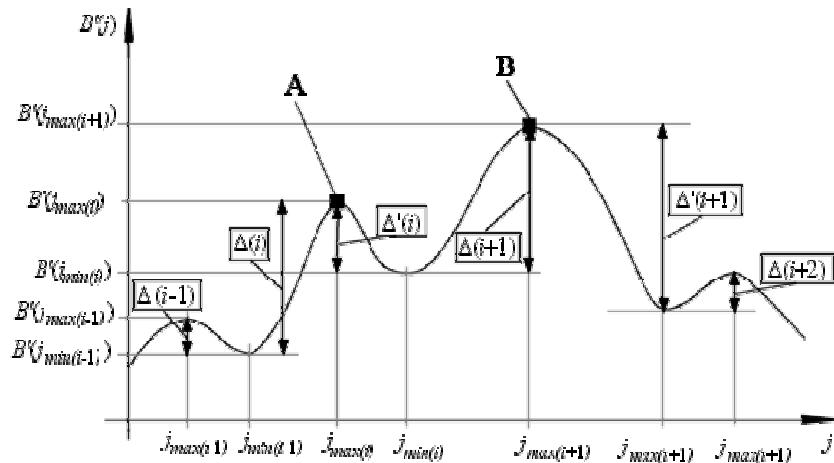
$$B'(j) = \frac{1}{3} \cdot [B(j-1) + B(j) + B(j+1)] \quad (9.22)$$

Určení lokálních maxim:

$$\Delta(i) = B'(j_{\max(i)}) - B'(j_{\min(i-1)}), \Delta'(i) = B'(j_{\max(i)}) - B'(j_{\min(i)}), i = 1, 2, \dots, M \quad (9.23)$$

$$\Delta(i) < \frac{1}{2} \cdot \Delta'(i-1), \Delta'(i) < \frac{1}{2} \cdot \Delta(i+1), i = 1, 2, \dots, M \quad (9.24)$$

Situace je znázorněna na obrázku 9.2.7.

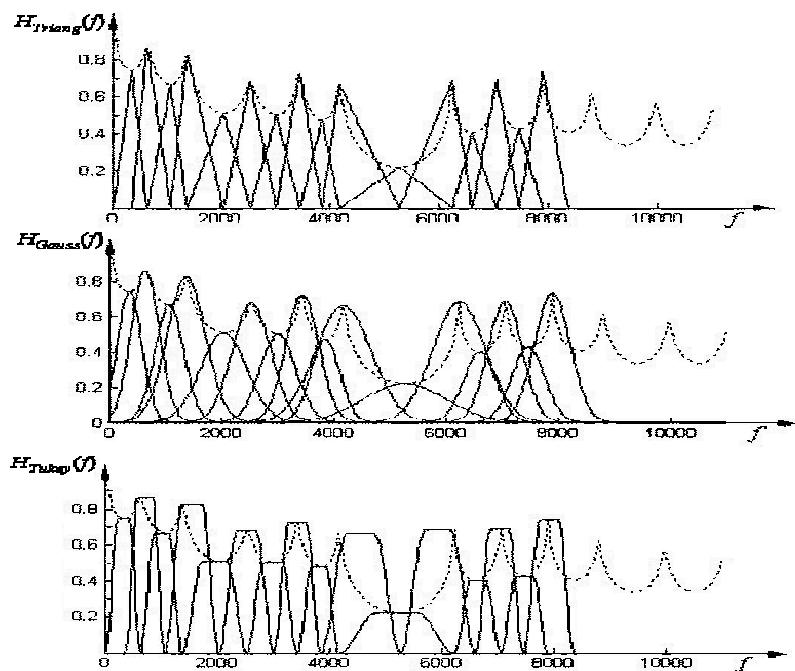


Obrázek 9.2.7: Detekce řečové aktivity – určení lokálních maxim [Ors05]



### Banka filtrů závislých na mluvčím:

- Podobá se bance filtrů u MFCC.
- Je však vhodnější pro účely rozpoznávání mluvčích – je silně závislá na mluvčím.



Obrázek 9.2.8: Koeficienty závislé na mluvčím [Ors05]



### Koefficienty závislé na mluvčím (Obr. 9.2.8):

- Vycházejí z MFCC. Redefinujeme rovnice pro MFCC takto:

$$\circ \quad C_{SDFB}(j) = \ln \left( \sum_{k=0}^{N-1} H_{SDF}(i, k) \cdot |S(k)|^2 \right), i = 1, 2, \dots, I \quad (9.25)$$

$$\circ \quad c_{SDFB}(j) = \sum_{i=0}^{I-1} C_{SDFB}(i) \cdot \cos \left( \pi n \frac{i-1}{2I} \right), j = 0, 1, \dots, I \quad (9.26)$$



### Proces rozpoznání:

Existují různé postupy zpracování příznaků:



- HMM (skryté Markovovy modely)
  - diskrétní
  - spojité
- Neuronové sítě

Typicky je výsledkem míra shody dvou vektorů příznaků, nejčastěji je to hodnota z intervalu <0,1>

- 0 = absolutní neshoda
- něco mezi = míra podobnosti
- 1 = absolutní shoda

Stěžejní je určení prahu, kdy je shoda dostatečná...



Příklad verifikace:

***Speaker Verification***

User comes.

```

USERNAME = Read user name ();
NEW_VOICE = Record voice password ();
NEW_PATTERN = Extract features (NEW_VOICE);

STORED_PATTERN = Load pattern from database (USERNAME);
LIKELIHOOD = Compare (STORED_PATTERN, NEW_PATTERN);

ANSWER = Decide-Verify (LIKELIHOOD);

System answers YES or NO.

```



Příklad identifikace:

```
Speaker Identification

User comes.

USERNAME = Read user name ();
NEW_VOCIE = Record voice password ();
NEW_PATTERN = Extract features (NEW_VOICE);

For each user USERNAME in the voice database
    STORED_PATTERN = Load pattern from database(USERNAME);
    LIKELIHOOD[USERNAME] = Compare(STORED_PATTERN, NEW_PATTERN);
End;

ANSWER = Decide-Identify (LIKELIHOOD);

System answers YES or NO.
```



V této kapitole jsme se věnovali dynamické biometrické vlastnosti – hlasu. Musíme rozlišovat rozpoznávání hlasu / řečníka a rozpoznávání obsahové stránky mluveného slova. Poslední nespadá do našeho biometrického rozpoznávání, ale předchozí dvě varianty ano.

Na začátku jsme si definovali složení vokálního traktu. Následoval popis filtrování a zpracování hlasu, abychom byli schopni extrahat z něj významné informace pro další proces rozpoznávání.



Příklady otázek:

1. Z jakých částí se skládá generování řeči?
2. Co jsou formanty?
3. Z jakých kroků se skládá zpracování řeči?
4. Co je LPC spektrum?
5. Popište princip rozpoznání řeči.



Odpovědi:

1. Strana 73.
2. Strana 74.
3. Strana 75.
4. Strana 77.
5. Strana 81.



# 10. Rozpoznávání podle písma a podpisu

V této kapitole nás čekají informace o biometrickém rozpoznávání písma a podpisu, přičemž oba přístupy je nutno rozlišovat. Budou zde uvedeny markantní informace, které lze nalézt v našem písmu.

Rozpoznávání písma a podpisu patří částečně do statických vlastností a částečně do dynamických.

**Rozpoznávání písma** – klasifikace písmen do tříd, utváření vět a rozpoznávání smyslu psaného textu.

**Rozpoznávání podpisu** – určení jedinečných vlastností podpisu (buď statických a nebo dynamických).

Verifikace vs. Identifikace – u podpisu se jedná téměř ve všech případech o verifikaci, identifikace zatím nenalezla velké uplatnění.

Trocha historie:



- 1975 – první vědecké práce
- 1977 – první off-line systém (*Nagel & Rosenfeld*)
- 1977 – první on-line systém (*Liu & Herbst*)
- 1989 – 1994 – vědecké rozbory písma
- 1995 – první komerční systém
- 1996 – nyní – různé metody k analýze písma

## 10.1 Základy rozpoznávání písma a podpisu



Existují dvě zvláštní varianty verifikace (autentizace), založené na ručním zadání:

- Fráze
  - Získání vzorku: ~ 5 sec.
  - Závislost na písme
  - Vysoký stupeň individuálních vlastností
  - Relativně stabilní vlastnost s jednoduchou reprodukovatelností
- Skica
  - Získání vzorku: ~ 2 sec.
  - Závislost na stejných tazích
  - Anonymní (na rozdíl k podpisu)



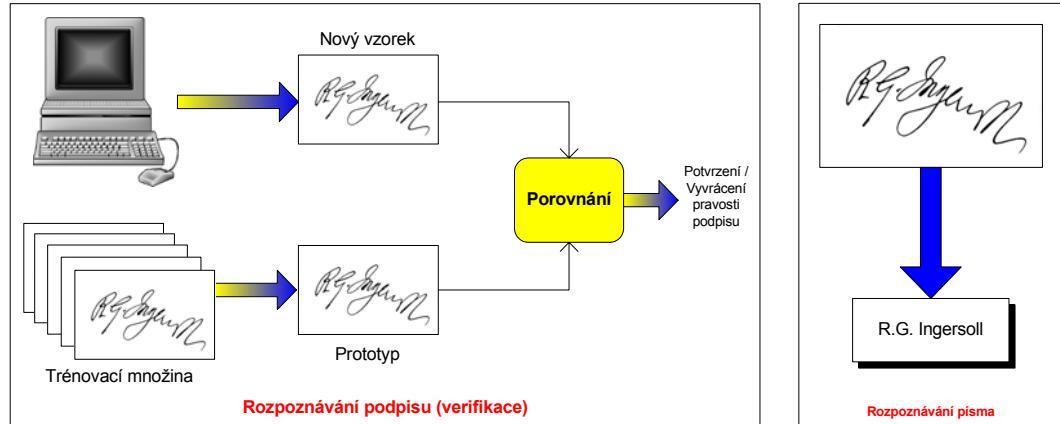
### Rozpoznávání písma versus podpisu

Oba typy rozpoznávání jsou odlišné, ale pro jejich zpracování se používají obdobné techniky. V obou případech nutné učení vzorů, přičemž oba typy rozpoznávání využívají odlišných informací. Ukázka rozdílnosti je ztvárněna v obrázku 10.1.1.



## Rozpoznávání znaků – klasifikace

Základní klasifikací je **PCA** (*Principal Component Analysis*) [Bal02], přičemž ta slouží k redukci dimenze na  $p$ . Používanější je ale **FDA** (*Fisher Discriminant Analysis*). Využívá matici vnitrotřídního a mezitřídního rozptylu  $\Phi_B$ ,  $\Phi_W$ .



Obrázek 10.1.1: Rozpoznávání podpisu vs. písma



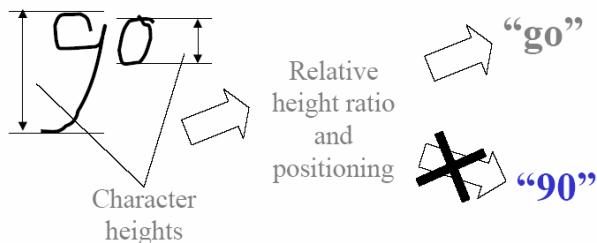
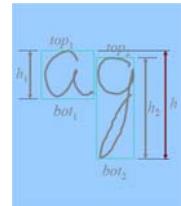
## Rozpoznávání znaků – rozlišování

Některé znaky jsou si velmi podobné:  $g \leftrightarrow 9$ ;  $I \leftrightarrow e$ ;  $0 \leftrightarrow O$

$$\text{HDR} = (h_1 - h_2) / h \quad \text{Height Differential Ratio}$$

$$\text{TDR} = (top_1 - top_2) / h \quad \text{Top Differential Ratio}$$

$$\text{BDR} = (bot_1 - bot_2) / h \quad \text{Bottom Differential Ratio}$$



Obrázek 10.1.2: Obtížné rozpoznávání znaků

Rozdělení aplikací (viz Tabulka 10.1.1) [Bal02]:

*On-line systém* – digitalizační tablety (výstupem je sekvence souřadnic bodů a signály o zvednutí / položení pera, tzv. **stroky** (*strokes*)).

*Off-line systém* – písmo / podpis se nascannují a systém s těmito údaji pracuje v off-line režimu.

Rozdíl mezi on-line a off-line systémem pro rozpoznávání podpisu je znázorněn na obrázku 10.1.3.



Výzvy u rozpoznávání podpisu:

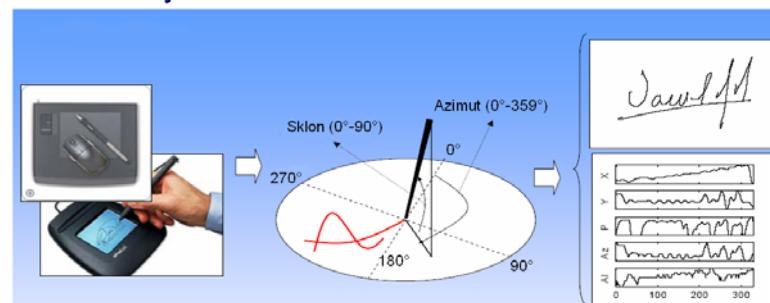
- Silně závislé od uživatele (různé rysy / prahy pro různé uživatele)!
- Vysoká vnitrotřídní (*intra-class*) variabilita!

- Statistické / elastické porovnávání.
- Adaptace šablony.
- Problém s detekcí „pravého“ podpisu. Výkonnost je závislá na útočníkově schopnosti napodobit podpis.

Tabulka 10.1.1: Rozdělení aplikací

Aplikace	Cíl	Doména	Mikrorysy	Makrorysy	Metoda
Rozpoznávání dokumentů	Extrakce informací	Automatické rozpoznávání obsahu	Slovo, znak	-	Off-line
Forensní	Verifikace	Evidence	Slovo, znak	Odstavec, strana	Off-line
Spolehlivost	Identifikace / Verifikace	Osobní digitální zařízení	Slovo, znak	-	On-line
Přístupové systémy	Verifikace	Bezpečnost, důvěrnost	Segmenty	Podpis	On-line
Elektronický podpis	Verifikace	Bezpečnost	Segmenty	Podpis	On-line

→ On-line systém:



→ Off-line systém:



Obrázek 10.1.3: On-line a off-line systém pro rozpoznávání podpisu



Výhody používání rozpoznávání podpisu:

- Uživatelsky přívětivé systémy
- Akceptované jak společností, tak i právně
- Neinvazivní
- Integrované do mnoha aplikací
- Je-li podpis vyzrazen, může být změněn
- Velké zkušenosti z grafologie, která se jevem rozpoznávání rysů písma zabývá již řadu let



Nevýhody používání rozpoznávání podpisu:

- Vysoká vnitrotřídní variabilita
- Lehká možnost napodobení / padělání
- Vyšší chybové míry, než ostatní biometriky
- Změny vyvolané často fyzickým a emocionálním stavem uživatele
- Silné změny typu *inter-template* (tedy v podstatě vnitrotřídní)

Aplikace:

- On-line:
  - Login (např. TabletPC, notebooky)
  - Autentizace dokumentů a transakcí
  - Autentizace v managementu podpisových aplikací (DHL, EES, TNT atd.)
- Off-line:
  - Ověření autentičnosti
  - Forenzní aplikace

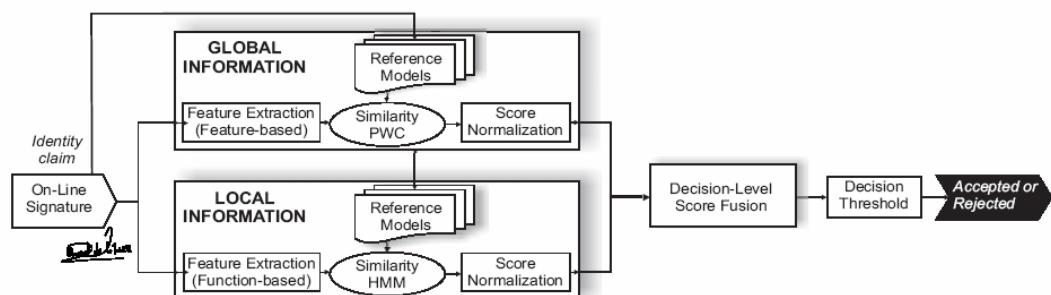
## 10.2 Metody rozpoznávání podpisu



### Metody rozpoznávání podpisu [Fie05]



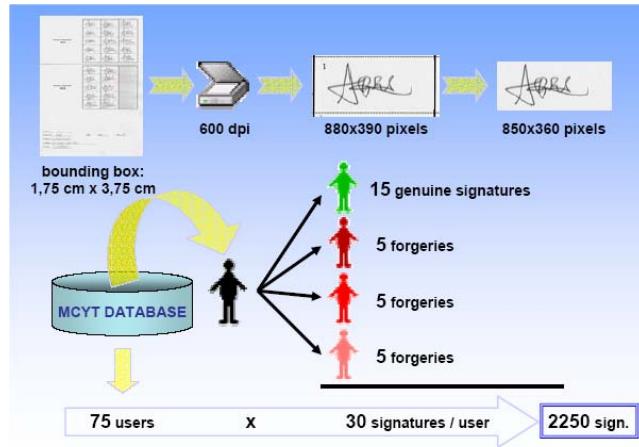
- **Holistická metoda**
  - Reprezentace: vektor rysů
  - Porovnání: vzdálenost mezi vektory
- **Regionální metoda**
  - Reprezentace: sekvence vektorů (stroky, segmenty, okna)
  - Porovnání: porovnání vektorů s ohledem na strukturu v sekvenci
- **Lokální metoda**
  - Reprezentace: funkce času a prostoru
  - Porovnání: elastické porovnání funkcí



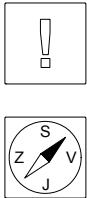
Obrázek 10.2.1: Systém založený na více metodách

Existuje ale i systém založený na více metodách (viz obrázek 10.2.1). Skládá se z pod systému globálních informací **PWC** (*Parzen Windows Classifier*) a systému lokálních informací **HMM** (*Hidden Markov Models*).

**Nahrání (registrace) podpisů** je znázorněno na obrázku 10.2.2.



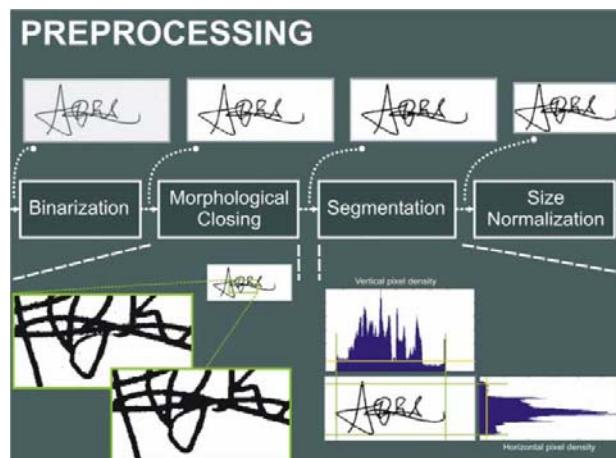
Obrázek 10.2.2: Nahrání (registrace) obrázků



Po fázi registrace podpisů do systému přichází fáze **předzpracování**. Pro on-line systémy není nutná segmentace (všechny části podpisu jsou zřejmě – přímé na snímání). Předzpracování je určeno k eliminaci šumu ze vstupu a především k eliminaci rychlosti psaní a přítlaku. Minimalizuje vlivy na výsledný vzhled podpisu, způsobené uživatelem.

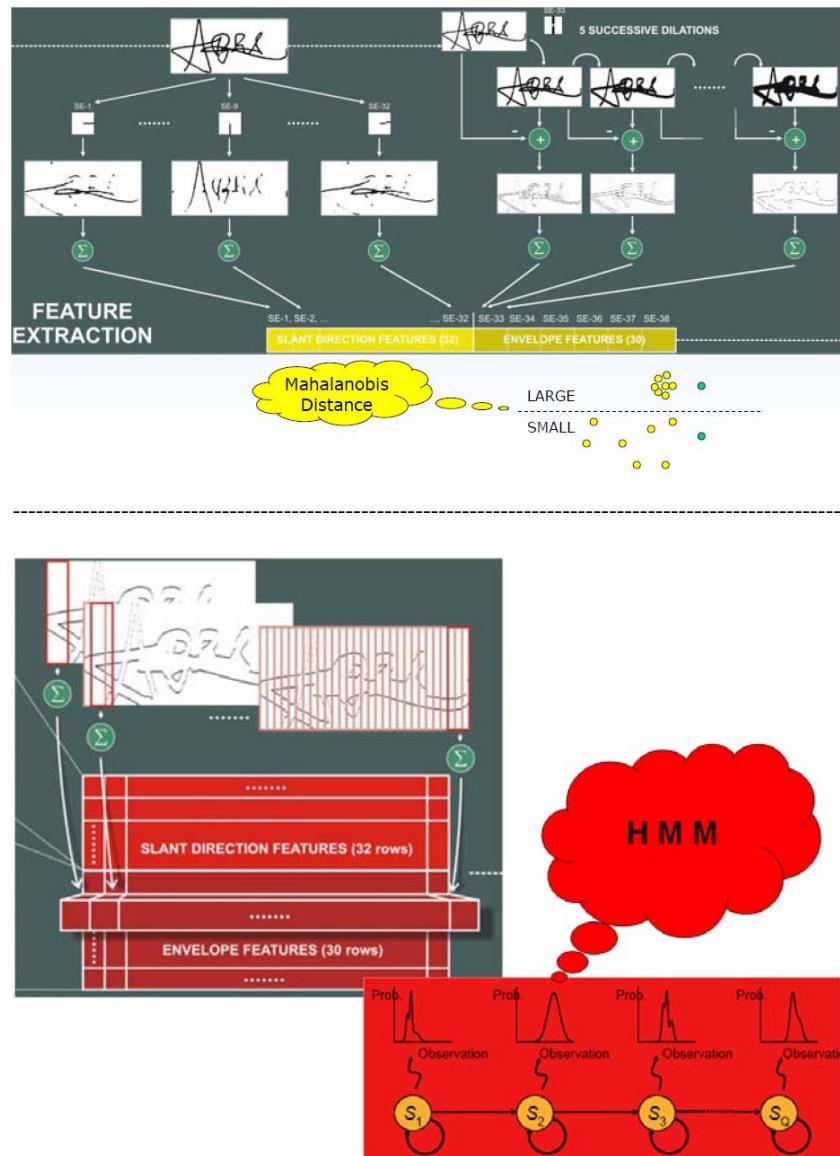
Fáze předzpracování se skládá (obrázek 10.2.3) z:

- Normalizace velikosti
- Normalizace pozice
- Vyhlažování
- Převzorkování
- Spojení (morphologické uzavření)



Obrázek 10.2.3: Fáze předzpracování podpisu

Po předzpracování přichází fáze extrakce rysů z podpisu. Na obrázku 10.2.4 jsou znázorněny dvě metody pro extrakci rysů (holistická a regionální).



Obrázek 10.2.4: Extraktce rysů – holistická (nahoře) a regionální (dole)

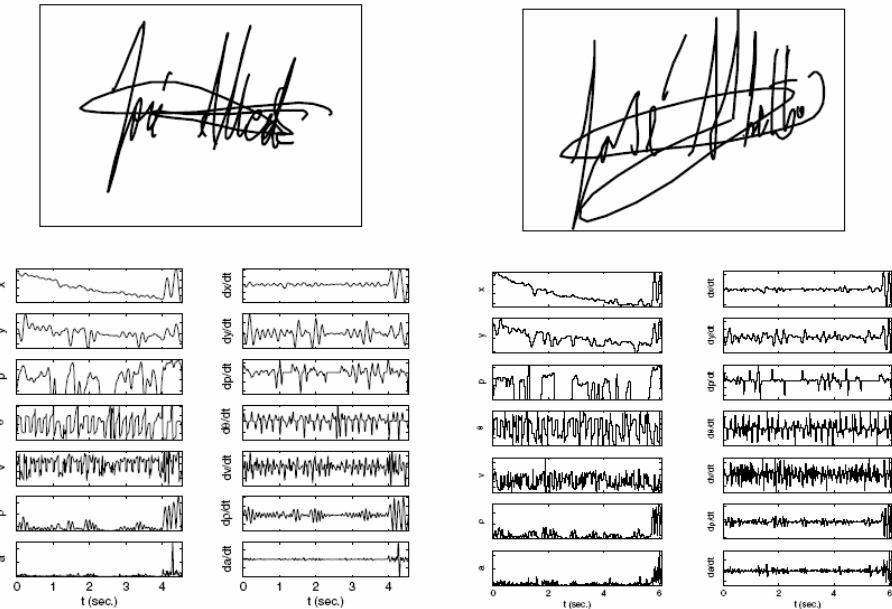


Samotné rozpoznávání podpisu následuje po předchozí extrakci rysů. Postup **holistického rozpoznávání** je znázorněn na obrázku 10.2.5.

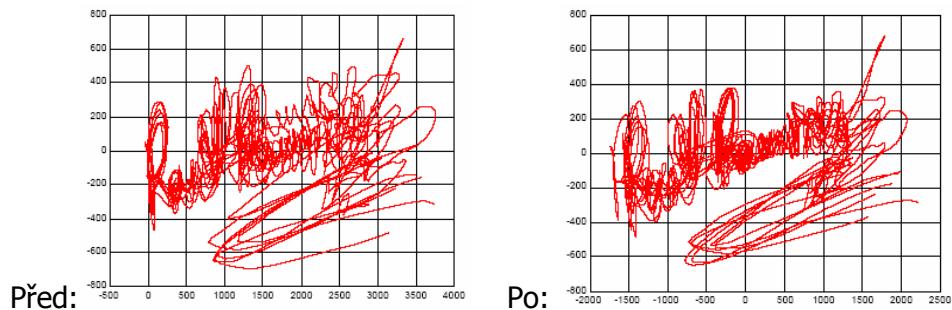
**Regionální rozpoznávání** využívá následující funkce (Obr. 10.2.4) [Yeu04]:

- 3 základní funkce
  - X-funkce
  - Y-funkce
  - Tlak (100 Hz)
- Geometrická normalizace (Obr. 10.2.6)
  - Pozice + rotace
- Čtyři další funkce

- Úhel cesty
- Rychlosť cesty
- Polomer zakřivení
- Zrychlení



Obrázek 10.2.5: Holistické rozpoznávání podpisu



Obrázek 10.2.6: Geometrická normalizace (regionální rozpoznávání)

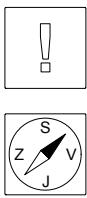
### Převzorkování

K zajištění dobrého porovnání dvou podpisů se provádí převzorkování, aby se eliminoval vliv rychlosti během psaní. Používá se 1D Gaussův filtr v  $x$  a  $y$  směru:

$$x_t^{\text{filtered}} = \sum_{i=-2\sigma}^{2\sigma} f_i * x_{t+i}^{\text{original}} \quad (10.1)$$

$$f_i = \left( e^{-\frac{i^2}{2\sigma^2}} \right) / \left( \sum_{j=-2\sigma}^{2\sigma} e^{-\frac{j^2}{2\sigma^2}} \right) \quad (10.2)$$

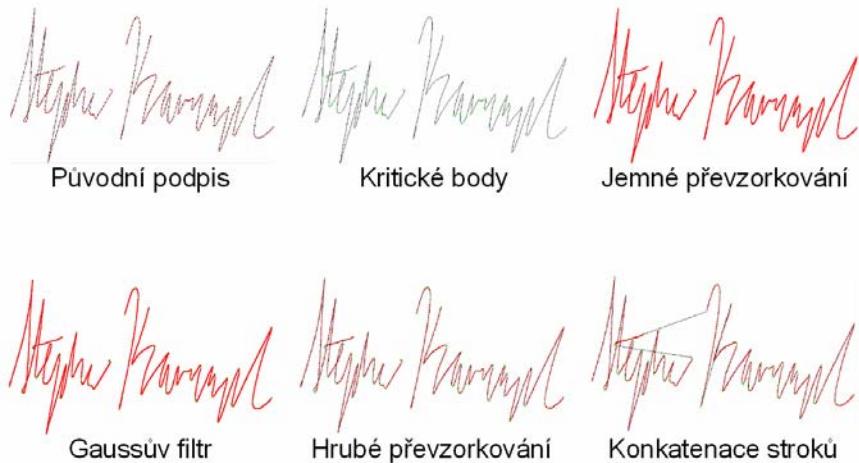




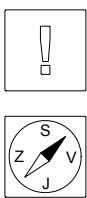
### Konkatenace stroků [Yeu04]

**Stroky** jsou místa mezi zvednutím a položením pera. Veškeré stroky jsou spojeny do dlouhého řetězce. **Kritické body**: body nesoucí více informace než ostatní body (koncové body a stroky + body změny trajektorie).

Příklad celkové části předzpracování je uveden na obrázku 10.2.7.

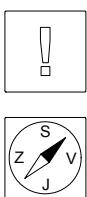
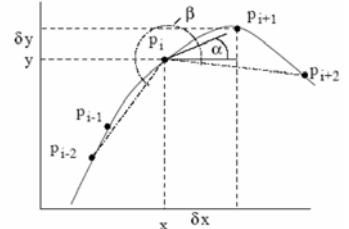


Obrázek 10.2.7: Celkový příklad fáze předzpracování



### Extrakce rysů (lokální rysy)

- Statické rysy
  - Změna vzdálenosti mezi dvěma body  $\delta x, \delta y$
  - Absolutní  $y$ -souřadnice
  - Sinus a kosinus s osou  $x$  ( $\alpha$ )
  - Zakřivení ( $\beta$ )
  - Šedé body v okolí okna  $9 \times 9$  pixelů
- Temporální rysy
  - Absolutní a relativní rychlosť v každém převzorkovaném bodu
  - Absolutní a relativní rychlosť mezi dvěma kritickými body



### Porovnání podpisů

K porovnání podpisů se používá metoda **DTW** – *Dynamic Time Warping*.  
K výpočtu zarovnání se používá:

$$D(i, j) = \min \begin{cases} D(i-1, j-1) + d_E(i, j) \\ D(i-1, j) + \text{Penalty}_{\text{Miss}} \\ D(i, j-1) + \text{Penalty}_{\text{False}} \end{cases} \quad (10.3)$$

$D(i, j)$  je optimální zarovnání bodu  $i$  z prvního řetězce a bodu  $j$  z druhého řetězce,  
 $d_E(i, j)$  je Eukleidovská vzdálenost mezi body  $i$  a  $j$ .

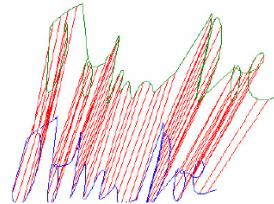
Celková podobnost je definována:

$$Dist(I, J) = \frac{D(I, J)^2}{Norm\_Factor(N_I, N_J)} \quad (10.4)$$

Každý bod je reprezentován  $n$ -árním vektorem rysů. Eukleidovská vzdálenost se používá k porovnání vzdáleností dvou vektorů rysů. Každý rys je normalizován pomocí  $z$ -skóre:

$$f' = \frac{f - \mu}{\sigma} \quad (10.5)$$

Hledá se množina párových bodů mezi vzorem a porovnávaným podpisem, přičemž výsledkem je suma těchto párových vzdáleností – viz obrázek 10.2.8.



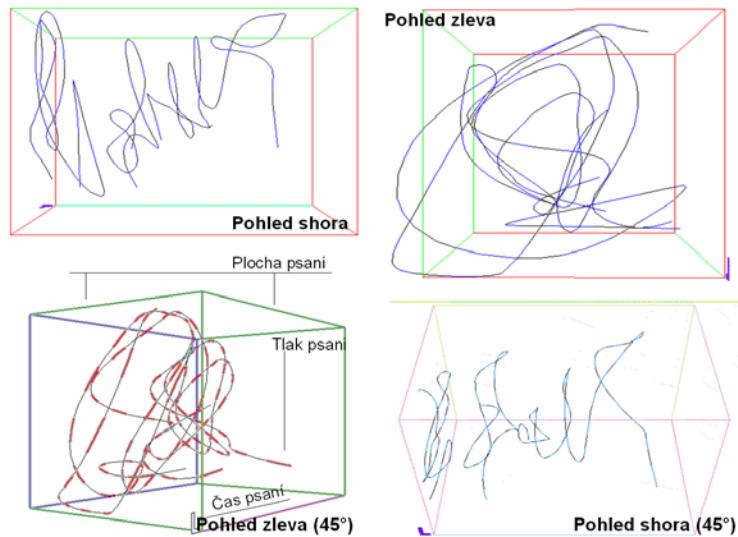
Obrázek 10.2.8: Porovnání podpisů

 K porovnání podpisů se používá tzv. **Mahalanobisova vzdálenost**. Byla defino-vána panem *P.C. Mahalanobisem* r. 1936. Vzdálenost, která vyjadřuje korelace mezi rysy:

$$d_M(x, y) = (x - y)' S^{-1} (x - y) \quad (10.6)$$

kde  $d_M$  je čtvercová Mahalanobisova vzdálenost,  $S$  reprezentuje kovariační matici vnitřní grupy,  $y$  je vektor středů skór grupy,  $x$  je vektor obsahující individuální skóre vzorku.

Za zmínku ještě stojí, že krom 2D podpisu existuje i 3D varianta rozpoznávání podpisu. Tato je uvedena schematicky na obrázku 10.2.9.



Obrázek 10.2.9: 3D rozpoznávání podpisu



V této kapitole jsme probrali rozpoznávání písma a podpisu. Samotné rozpoznávání obsahu písma (tj. určení obsahu ze znakové stránky) nás nezajímá, ale zajímají nás specifické rysy písma (tahy a stroky). Rozlišujeme statické rozpoznávání písma a dynamické. Pro rozpoznávání písma / podpisu existuje několik metod, které jsme si uvedli.



Příklady otázek:

1. Jaký je rozdíl mezi rozpoznáváním podpisu a písma?
2. Jaké znáte metody rozpoznávání podpisu?
3. Jaké funkce používá regionální rozpoznávání podpisu?
4. Co je konkatenace stroků?
5. Jak funguje porovnání podpisů?



Odpovědi:

1. Strana 83.
2. Strana 86.
3. Strana 88.
4. Strana 90.
5. Strana 90 – 91.



# 11. Dynamické biometrické vlastnosti

Dynamické biometrické vlastnosti se vyznačují tím, že pro jejich vyhodnocení hraje velmi důležitou roli čas, tj. dochází k nahrání průběhu nějaké lidské činnosti a na základě těchto údajů dochází k rozpoznání či nerozpoznání.



V následujících třech podkapitolách probereme metodu **rozpoznávání dynamiky stisku kláves**, metodu **rozpoznávání chůze** a metodu **rozpoznávání pohybů rtů**. Výčet těchto dynamických vlastností ale samozřejmě nekončí jen třemi variantami. K jiným možnostem dynamických biometrických vlastností patří:

- Dynamika pohybu myši
- Gestikulace obličeje
- Srdeční puls
- (Reakce duhovky na světlo) – více pro detekci živosti [Tot05]
- Srdeční puls a duhovka → testování živosti
- Gestikulace obličeje je obsažena zčásti v rozpoznávání 3D obličeje
- Hlas (řeč) a dynamika písma byly rozebrány v předešlých kapitolách

## 11.1 Rozpoznávání dynamiky stisku kláves



**Dynamika stisku kláves** je proces analýzy způsobu psaní uživatele na klávesnici, jež je založená na identifikaci jeho přirozeného rytmu psaní (stisků kláves).

Šablona psaného vzorku (dynamické vlastnosti) by měla být pro každého jedince jednoznačná, protože každý z nás má jiné neurofyziologické faktory, které rytmus psaní ovlivňují.

Dynamika stisku kláves patří do biometrie chování (dynamických biometrických vlastností) → přirozená vhodnost pro počítačový login a síťovou bezpečnost.

Trocha historie:

- Během 2. světové války objevila armáda tzv. metodu „*Fist of the Sender*“, kde telegrafisté byli schopni podle dynamiky vysílané Morseovy abecedy identifikovat telegrafistu na druhé straně.
- 1979 – SRI International – první HW implementace
- 1984 – NIST shledává tuto technologii z 98% efektivní
- 1988 – Nová technologie odpovídající definici NISTu z roku 1987 (*NIST Computer Security Act 1987*)
- 2000 – Společnosti FSTC / IBG verifikují technologii dynamiky stisku kláves
- 2001 – Integrace této technologie do telefonních aparátů a domácí bezpečnosti (Home\_PC)



### Rysy vzorů psaní:

Dynamika stisku kláves se nezabývá tím, co píšete, ale tím jak píšete.

### Rysy používané k popisu vzoru psaní uživatele [Ilo03]:

- Časové prodlevy mezi úspěšnými stisky kláves (uběhnutý čas mezi uvolněním staré klávesy a stiskem nové klávesy)
- Délka trvání každého stisku (jak dlouho je klávesa stisknuta)
- Poloha prstu na klávese (je-li k dispozici)
- Tlak aplikovaný na klávesu (je-li k dispozici)
- Celková rychlosť psaní

Použití např. pro login k počítači, při psaní uživatelského jména a zadávání hesla. Rysy jsou funkcií uživatele a prostředí. Při záznamu dynamických vlastností úhodou hraje roli i samotné psané slovo, protože ergonomie klávesnice neumožňuje stejně napsání slova „Martin“ a např. „987654“. Proto je dynamika stisku kláves závislá i na psaném textu.

### Statická vs. průběžná verifikace

Při **statické verifikaci** jsou stisky kláves analyzovány pouze ve specifikovaných časech, např. během loginu. Statické verifikační přístupy umožňují mnohem robustnější verifikaci, než samotné zadání hesla. Statické přístupy ovšem neposkytují průběžnou bezpečnost – neumí detekovat záměnu uživatelů po přihlášení k počítači.

**Průběžná verifikace** monitoruje celkové chování uživatele během jeho práce s počítačem. U průběžné verifikace je ovšem nutný vyhodnocovací proces, který neustále běží – zatížení počítače.

### Měřítka vzdálenosti [Mon99]

L1 norma:

$$D(R, U) = \sum_{i=1}^N |r_i - u_i| \quad (11.1)$$

Eukleidovská vzdálenost:

$$D(R, U) = \left[ \sum_{i=1}^N (r_i - u_i)^2 \right]^{1/2} \quad (11.2)$$

Vážená pravděpodobnost:

$$score(R, U) = \sum_{i=1}^N \frac{w_{u_i}}{o_{u_i}} \left[ \sum_{j=1}^{o_{u_i}} prob\left( \frac{x_{ij}^{(u)} - \mu_{r_i}}{\sigma_{r_i}} \right) \right] \quad (11.3)$$

kde  $w_{u_i}$  je váha rysu  $u_i$ ,  $o_{u_i}$  je počet výskytů  $u_i$ ,  $x_{ij}^{(u)}$  je hodnota  $j$ -tého výskytu  $u_i$ ,  $\mu_i$  a  $\sigma_i$  jsou střední a standardní odchylky od  $i$ -tého rysu.

Bayesovský klasifikátor:

$$D(R, U) = \sum_{i=1}^N w_i \left( \frac{|r_i - u_i|}{\sigma_i} \right)^\alpha \quad (11.4)$$

Dvě po sobě napsaná písmena se nazývají **digraf**. Tři po sobě napsaná písmena se nazývají **trigraf**. Délka trvání u trigrafů – čas mezi stiskem první klávesy a uvolněním třetí klávesy. U digramů je to mezi první klávesou a druhou klávesou.

Předpokládejme např. text „america“:

- $ame = 277; mer = 255; eri = 297; ric = 326; ica = 235$

Ve vektoru uloženo ve vzestupném pořadí:

- $ica = 235; mer = 255; ame = 277; eri = 297; ric = 326$

### **Porovnání trigrafů**

Stupeň „nepořádku“: suma absolutních změn v pozici mezi dvěma uspořádanými poli.

**Vzor<sub>1</sub>:**  $ica = 235; mer = 255; ame = 277; eri = 297; ric = 326$

**Vzor<sub>2</sub>:**  $mer = 215; ica = 258; ame = 298; ric = 306; eri = 315$

<b>Vzorek<sub>1</sub></b>		<b>Vzorek<sub>2</sub></b>		
ica	235	d = 1	mer	215
mer	255	d = 1	ica	258
ame	277	d = 0	ame	298
eri	297	d = 1	ric	306
ric	326	d = 1	eri	315

Obrázek 11.1.1: Porovnání trigrafů

$D(Vzor_1, Vzor_2) = (1+1+0+1+1) / 12 = 0,33$ . Výsledek se normalizuje, aby ležel v rozmezí  $<0,1>$ .

### Přesnost dynamiky stisku kláves u digrafů:

Pro vyhodnocení [Jai04] byla použita databáze 63 uživatelů, přičemž data byla nasbírána během 11 měsíců. Účastníci pracovali na svých počítačích.

Dvě varianty:

- Volný text (klasická práce)
- Fráze / předem definovaný text

**FAR** = 0,01% a **FRR** = 3,0%. Správné vyhodnocení pro:

- Vážená pravděpodobnost: 87%
- Bayesovský klasifikátor: 92%



### Přesnost dynamiky stisku kláves u trigrafů:

Pro vyhodnocení [Jai04] byla použita databáze 44 oprávněných uživatelů a 110 útočníků. Pevně stanovený text o 683 znacích; 5 vzorků na uživatele. Všechna data nahrána na stejně klávesnici. Pro psaní se používalo pouze vybraných kláves. Všichni uživatelé byli zkušení v práci s PC.

Výsledky:

- **FRR**  $\cong 1,8\%$
- **FAR**  $\cong 0,042\%$
- Vnitrotřídní variabilita uživatele šablony A:
  - $md(A, B) = [d(A_1, B) + d(A_2, B) + d(A_3, B)] / 3$



### Výhody dynamiky stisku kláves:

- Neinvazivní
- Dobře akceptovaná uživateli
- Přirozený způsob autentizace u počítačů a sítí
- Je možné průběžné monitorování
- Nutnost minimálního tréninku (učení)
- Žádný přídavný hardware
- Možnost tvorby **silného hesla**:
  - Textové heslo + dynamický vzorek jeho psaní
  - Vyšší bezpečnost
  - Nebezpečí **FRR** díky změně stylu psaní



### Nevýhody dynamiky stisku kláves:

- Vysoká míra **FRR**
- Citlivá metoda na změny klávesnice, fyzického či psychického stavu uživatele a příp. vlivů okolí
- Úzká oblast použitelných aplikací
- Musí umět zahrnovat problémy jako jsou překlepy či opravy při psaní

## 11.2 Rozpoznávání chůze

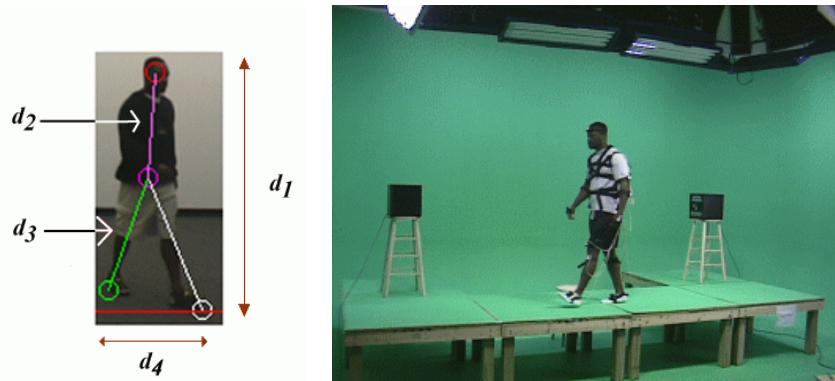


Účelem je rozpoznat osobu na základě chůze. K rozpoznání by mělo být využito běžných typů kamer. Rozpoznávání chůze může sloužit k identifikaci osob na dálku. Malá rozlišovací schopnost. Dříve bylo nutné používat speciální označovače na oblečení (*test-dummy*). Požadovaným výsledkem je rozpoznání v každé situaci. Metriky pro rozpoznávání chůze jsou uvedeny na obrázku 11.2.1a.

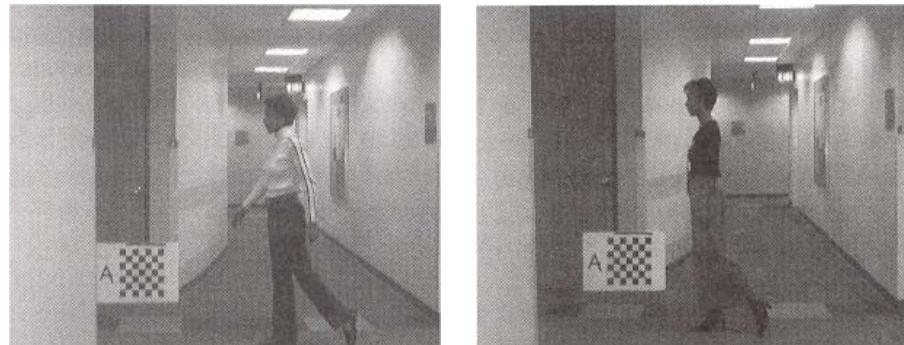
Rozpoznávání je závislé na těchto faktorech (viz ukázka na obrázku 11.2.2):

- Oblečení

- Obutí
- Fyzický stav uživatele
- Okolní prostředí + osvětlení
- Množství osob v daném prostředí
- Vážná onemocnění / úrazy



Obrázek 11.2.1: a) Metriky pro rozpoznávání chůze; b) Forma nahrávání vzorů



### **Rozpoznávání chůze**

Algoritmus funguje následovně [Suu04]:

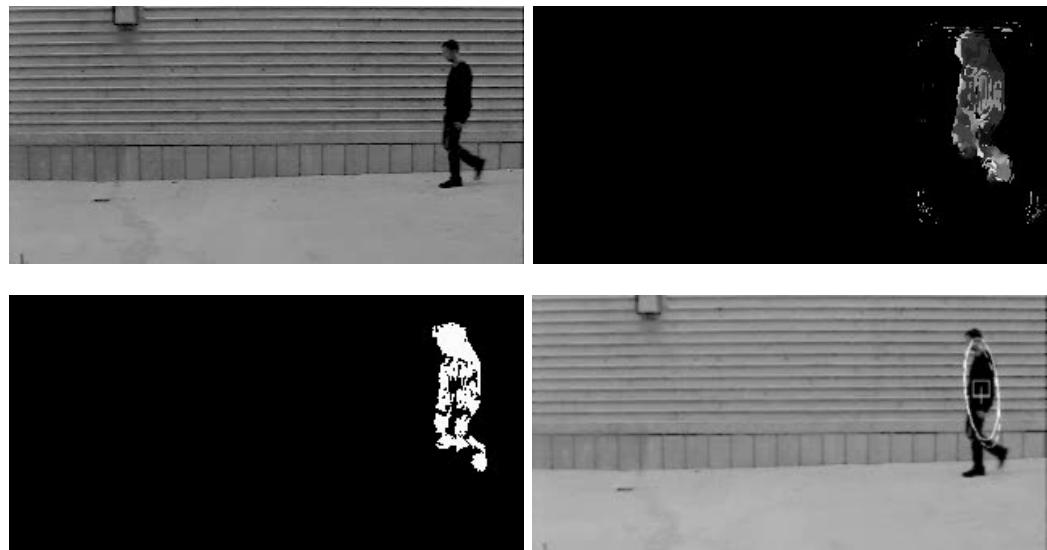
- Definování hraničních boxů pro postavu ve videosignálu
- Extrakce siluety postavy dle hraničních boxů (viz obrázek 11.2.3).
- Změna rozlišení hraničních boxů na  $128 \times 88$  pixelů, aby byl krok provedení korelace výpočetně nenáročný.



Obrázek 11.2.3: Extrakce siluety postavy

Praktický průběh se skládá z následujících fází (obrázek 11.2.4):

- Záznam videa z kamery
- Výpočet optického toku  $u$ ,  $v$  a  $|u+v|$
- Binarizace – výsledkem jsou tzv. *Moving Blobs*
- Pohyb (v obrazu mají symboly následující význam: + je centrum; čtverec je vážený centroid  $|u+v|$ ; plná elipsa vyjadřuje poměr stran pohybujícího se objektu; čárkovana elipsa vyjadřuje poměr stran váženého centroidu  $|u+v|$ )



Obrázek 11.2.4: Průběh rozpoznání chůze (nahoře vlevo: nahrání videa z kamery; nahoře vpravo: výpočet optického toku; dole vlevo: binarizace; dole vpravo: rozpoznání pohybu)

### 11.3 Rozpoznávání pohybu rtů



Účelem je rozpoznat osobu na základě pohybu rtů. Porovnání probíhá na základě charakteristik pohybů rtů během rozhovoru / vyřčení předdefinované fráze. Pomáhá při identifikaci řečníka na základě hlasu.

Možnosti osvětlení a snímání:

- **FIR** (*Far-InfraRed*) – vysoká bezpečnost, ale také vysoké finanční náklady
- **NIR** (*Near-InfraRed*) – levné, nejčastěji použito pro aktivní snímání



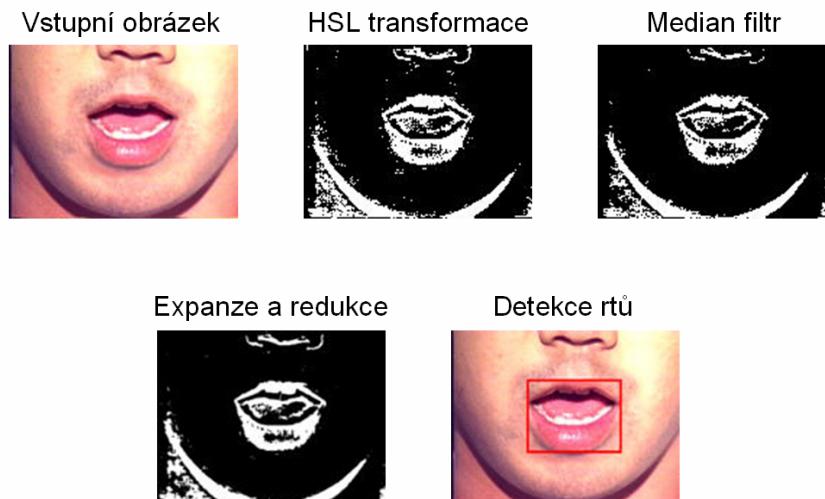
Velmi výhodnou možností je tvorba multimodálního biometrického systému, který slučuje:

- Rozpoznávání hlasu
- Rozpoznávání obličeje
- Rozpoznávání pohybů rtů

Takový systém nabízí velmi vysoký stupeň bezpečnosti. Téměř každý počítač má mikrofon a minimálně webovou kamerku → realizace nenákladná. Profesionální produkt se jmenuje *Bioxid* (k testování byly využity databáze M2VTS (*Multi Modal Verification for Teleservices and Security Applications*)).

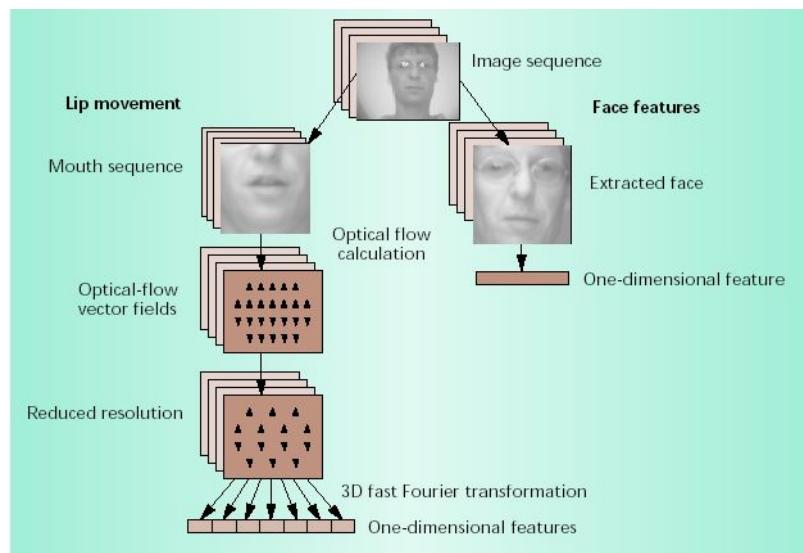
Detekce úst v obličeji může být provedena algoritmem na zpracování obličeje (viz kapitola 7). Jednotlivé pohyby jsou nahrány z posloupnosti snímků ve videu. Pro nahrání snímků pohybu rtů lze použít také termokameru, címž ale bohužel stoupnou pořizovací náklady na celý systém. Pro správnou funkčnost systému je nutné zajistění vhodného osvětlení, není-li použito infračervené světlo (např. u webové kamery).

Postup zpracování oblasti úst pro rozpoznání pohybu rtů je uveden na obrázku 11.3.1.



Obrázek 11.3.1: Postup zpracování oblasti úst

Průběh rozpoznávání je zobrazen na obrázku 11.3.2.



Obrázek 11.3.2: Rozpoznání pohybu rtů

V této kapitole jsme se věnovali dynamickým biometrickým vlastnostem. Nejprve jsme probrali dynamiku stisku kláves, která je lehce aplikovatelná jako doplněk přihlašovacího mechanizmu k počítačům. Pro rozpoznávání se používají buď digrafy a nebo trigrafy (dvojice či trojice kláves, resp. prodlevy mezi nimi).

Dále jsme se věnovali rozpoznávání chůze. To je celkem náročný proces, zejména z důvodu změny oblečení a okolních podmínek prostředí. Navíc i rozlišovací



schopnost takového systému není příliš vysoká. Každopádně se dá použít jako doplněk u kamerových systémů, které sledují příchod/odchod osob do/z budovy.

Na závěr jsme se věnovali rozpoznávání rtů. Tato metoda slouží většinou jako doplněk pro multimodální biometrický systém – krom rozpoznávání hlasu a obličeje uživatele se detekují a rozpoznávají i dynamické pohybu jeho rtů.

 Příklady otázek:

1. Jaký je rozdíl mezi statickou a průběžnou verifikací u technologie rozpoznávání dynamiky stisku kláves?
2. Co je digraf a trigraf?
3. Jak funguje rozpoznávání chůze?
4. Jak funguje rozpoznávání pohybu rtů?
5. Jaké znáte dynamické biometrické vlastnosti?

 Odpovědi:

1. Strana 94.
2. Strana 95.
3. Strana 97.
4. Strana 99.
5. Strana 93.



## 12. DNA a její využití v biometrii

V této kapitole se budeme věnovat biometrickému rozpoznávání DNA. Jedná se o nejspolehlivější metodu pro určení identity jedince (má ovšem svá úskalí). Dozvíme se, jak se postupuje při zpracování DNA a jak funguje samotné rozpoznání.



DNA (*Desoxyribo-Nucleic Acid*) se liší od klasických biometrik v mnoha směrech:

- DNA vyžaduje hmatatelný fyzický vzorek, v opaku proti snímku či nahrávce.
- DNA porovnávání není provedeno v reálném čase a ne všechny části zpracování jsou automatizované.
- Z DNA se neextrahuje rysy, ani šablony, ale reprezentace DNA je ve formě vzorků – klasická metoda porovnává dva vedle sebe ležící vzorky v elektrofluorescenčním gelu.



Výhody a nevýhody použití DNA:

- DNA je nazývána „definitivním identifikátorem“, je naprostě unikátní pro každého jedince planety (dvojčata mají stejnou základní strukturu DNA)
- Pomocí DNA lze identifikovat informaci z každé buňky těla (výsledek v digitální reprezentaci), lze ji získat z mnoha typů biologických vzorků
- Nejčastější použití je ve forenzní medicíně
- Během života se vůbec nezmění !!!
- Proces není kompletně automatizovaný
- Pomalé a cenově nákladné vyhodnocení
- Osobní údaje – DNA obsahuje informace o rase, otcovství a zdravotním stavu jedince atp.

### 12.1 Základy

Jaké jsou zdroje DNA? Zdrojem pro analýzu DNA mohou být např. pozůstatky na papírovém nebo plastovém nádobí, pozůstatky na skle, ušní maz, zbytky nehtů, ponožky, moč, olíznuté známky, propocené tričko, vlasy s kořeny, zaschlá krev, čerstvá krev, použitá žvýkačka, dentální nit, nedopalky cigaret, použitý kapesník, uschlá kůže, použitá žiletka a další.



**DNA = Desoxyribo-Nucleic Acid.** Jedná se o dvojitě točenou spirálovou molekulu, tvořící kroucený žebřík. Hřbet je tvořen cukrem a fosfátem, vnitřek nukleovou kyselinou. Je k nalezení ve všech jádřech buněk (DNA se nachází v mitochondrii každé buňky). Svázání do chromozómů - **chromozóm** se replikuje při každém dělení buňky.

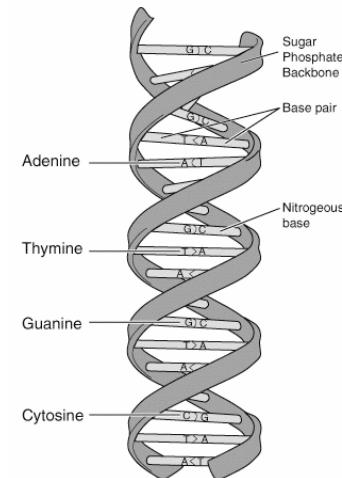
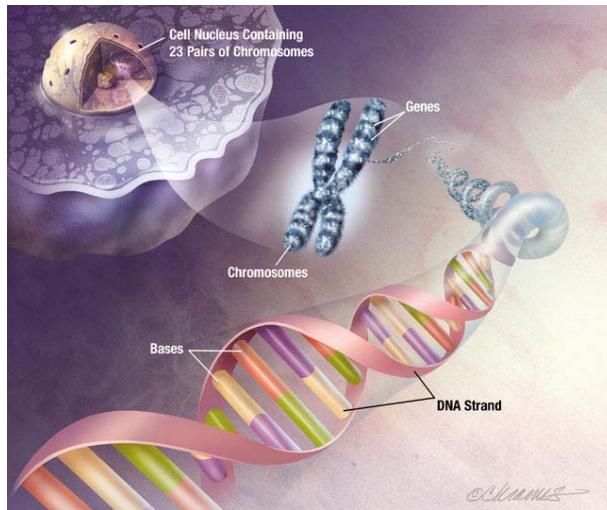
Pouze čtyři **nukleové kyseliny (nukleotidy)** tvoří genetický kód DNA:

- **Adenin**
- **Thymin**
- **Guanin**
- **Cytosin**

Základní párování (obrázek 12.1.1):

- A-T
- G-C

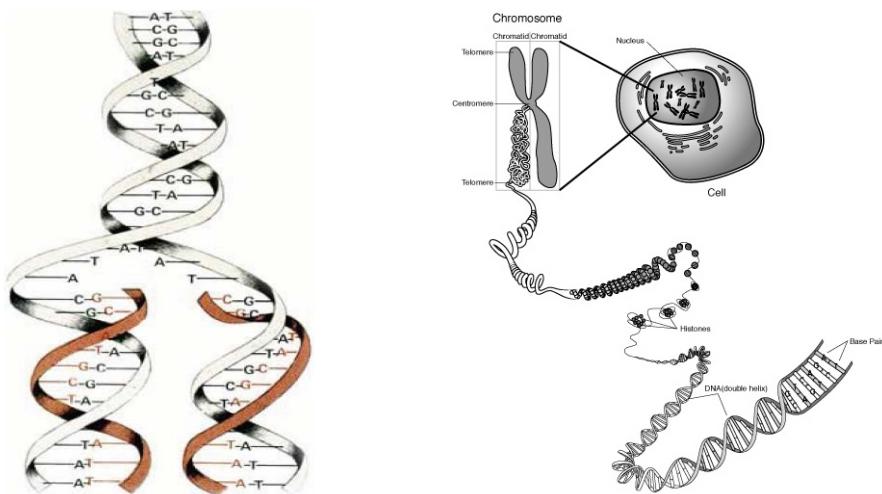
V DNA se nachází celkem 3 miliardy takových párů.



Obrázek 12.1.1: Struktura DNA



**Replikace DNA** – Během replikace se oba DNA pásky oddělí nebo se deformují, a je vytvořen nový komplementární pás, za použití odkrytých základů jako šablon (obrázek 12.1.2). Lidé mají 23 souhlasných párů chromozómů ( $\Sigma=46$ ). Od každého rodiče obdržíme 23 chromozómů. 99,7% DNA je sdíleno. 0,3% DNA je variabilní.



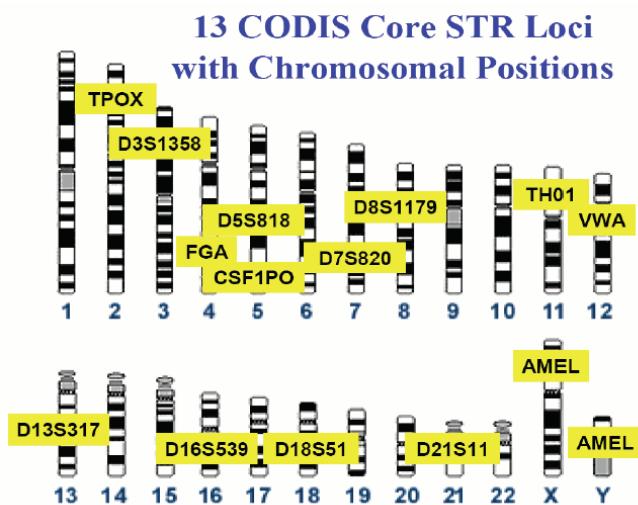
Obrázek 12.1.2: Replikace DNA

Ona 0,3% (přibližně 1 milión nukleotidů) variabilita je děděna, určuje tudíž onu individualitu jedince. Tyto variabilní regiony, zvané STR (*Short Tandem Repeats*), mohou být zkoumány a slouží k vzájemnému odlišení lidí.

Abychom mohli od sebe navzájem odlišit lidi, jsou právě třeba regiony DNA s vysokou proměnlivostí. V počátku roku 1980 byly tyto regiony objeveny a bylo zjištěno, že se mohou použít k odlišení lidí. V současnosti existuje celkem 13 tako-

vých regionů (také nazývané *locus* – obrázek 12.1.3), které se využívají v DNA profilování. V každém z těchto 13 regionů je opakující se sekvence, která je variabilní ve své délce (např. opakování sekvence ACCT nebo TTTC). Počet opakování v každé pozici může být změreno během DNA sekvencování.

Každý počet opakování má statistiku s ní asociovanou, která může být porovnána s populací. Pravidlo násobení může být použito na násobení statistiky pro všechn 13 regionů, podávající vysoce individualizované výsledky. Většina DNA profilů uvádí jako výhodu jejich sílu – pravděpodobnost sdílení stejného profilu jinou osobou je přibližně 1 : triliónu!



Obrázek 12.1.3: 13 regionů locus

## 12.2 Práce s DNA



### Dešifrování kódu DNA [Sol04]:

Tři základní kroky:

- *Extrakce* (získání a izolace vzorku DNA)
- *Kopírování* (tvorba kopí cílových sekvencí)
- *Sekvencování* (získání unikátního kódu nukleové kyseliny z DNA vzorku)



### Extrakce DNA

Hlavní metody extrakce:

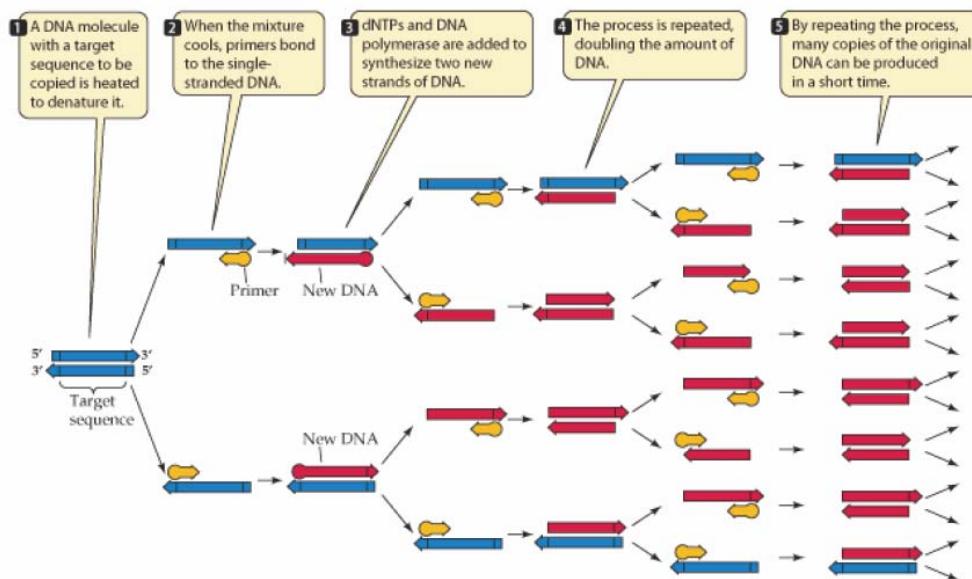
- *Organická* (používá fenol, chloroform a pro separaci DNA z buněk centrifugu; trvání 3 hod.)
- *Chelex™* (zahřívání a iminodiaceticke kapičky pro navázání DNA na sebe; trvání méně 1 hod.; nečistá analýza – náchylná k chybám)
- *papírová FTA™* (vzorek umístěn na papír, usušen a poté několikrát prán; papír je poté možné použít ke kopírovací reakci; trvání méně jak 1 hodina)
- *alkalická* (vzorek je rozpuštěn v zásaditém roztoku (např. NaOH) a DNA je odfiltrována; trvání několik hodin)



## Kopírování DNA + Reakce PCR

Po izolaci DNA z biologického vzorku musí být zvýšen počet kopí. DNA musí být zkopirována před sekvencováním, aby byl zajištěn dostatek pro reakci.

**PCR = Polymerase Chain Reaction** (enzymatické kopírování DNA – exponenciální kopírování vzorku). Reakce vyžaduje extrahovanou DNA, podkladovou barvu, polymerázu (enzym), volně pohyblivý nukleický základ a tlumící roztok. Tyto ingredience umožňují přesnou replikaci DNA, využitím zvýšení a snížení teploty. Délka trvání: 2-3 hodiny pro 32 cyklů. Reakce PCR je znázorněna na obr. 12.1.4.

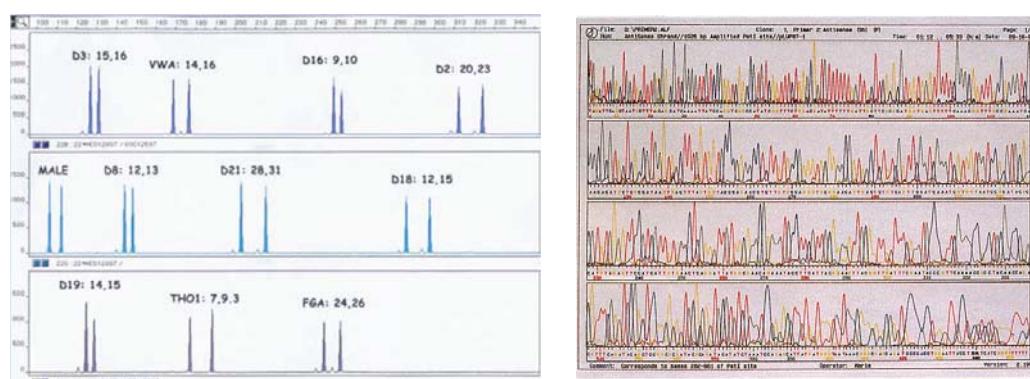


Obrázek 12.1.4: Reakce PCR



## Sekvencování DNA

DNA sekvencování je krok generování profilu DNA. Zkopírovaná DNA je nahrána do genetického analyzátoru (sekvenceru) s fluorescenčně označenými komponentami A, T, C a G, přidanými k DNA. K systému je připojen elektrický proud a DNA části rostou kolem laseru – části, které prošly laserem jsou nahrány a výsledně je vytvořen profil, který může být následně vizuálně prezentován. Délka trvání: přibližně 30 minut / vzorek.



Obrázek 12.1.5: Ukázka profilu DNA

Časové nároky na získání a vyhodnocení DNA:

- Získání vzorku: ~ 10 sekund
- Extrakce DNA: 0,5 – 3 hodiny
- Kopírování DNA: 2 – 3 hodiny
- Sekvencování DNA: 0,5 – 1 hodina

Celkový čas: Minimálně 3 hodiny!



## Pokroky v technologii DNA

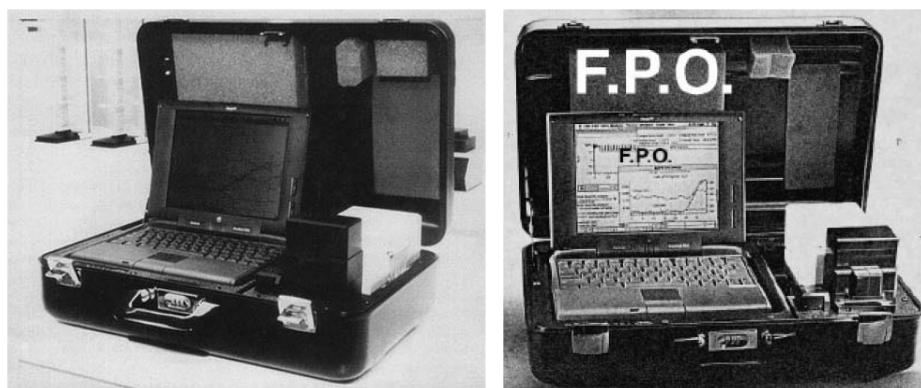
### Extrakce DNA

- K dispozici jsou již komerční produkty, které umožňují rapidní extrakci DNA.
- Nový model *The Bode Technologies Buccal DNA Collector* pracuje na obdobném principu jako FTA™.
- Výsledná množina extrahovaných vzorků DNA může být v tomto případě ihned přímo přeposlána do kopírovací jednotky PCR.
- Délka extrakce – přibližně 30 sekund.



### Kopírování DNA

- Nové produkty umí kopírovat DNA již v minutách.
- Nové zařízení umožňuje prudké změny teploty, čímž je docílena velmi rychlá kopie DNA.
- MATCI (*Miniature Analytical Thermal Cycling Instrument*) (Obr. 12.1.6) je přenosná PCR jednotka, která zvládne 32 cyklů kopírování za 21 minut!



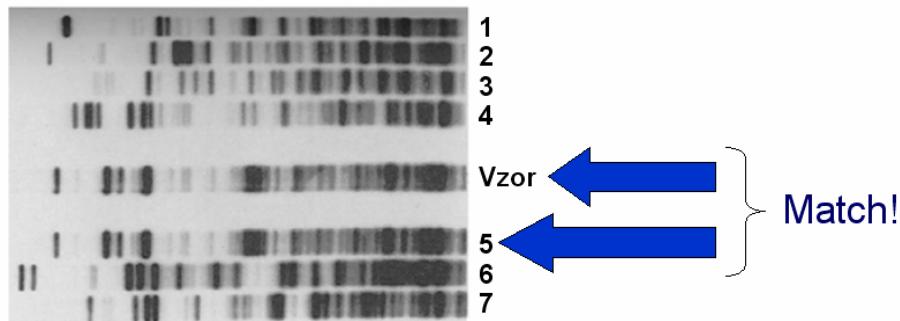
Obrázek 12.1.6: MATCI - *Miniature Analytical Thermal Cycling Instrument*



### Sekvencování DNA

- Rychlá analýza DNA je možná např. u komerčního produktu ABI 3730xl, nebo u produktu Nanochip™ Microchip, kde jsou úzké kanálky, kterými DNA prudce stoupá a laser provádí přímou detekci.
- Použití krátké vzdálenosti pro růst, tj. pro sloupek přibližně 2 cm, oproti původním 35 cm ~ 30 sec.

Nové DNA technologie kombinují kopírování a sekvencování DNA do jednoho kroku. Kombinace všech třech kroků dohromady je prozatím hrdou budoucností, ale pracuje se na tom.



Obrázek 12.1.7: Systém CODIS – analýza DNA



### Systém CODIS

Systém CODIS je u FBI, jeho funkčnost je obdobná AFISu. U závažných trestních činů jsou DNA profily zločinců automaticky ukládány do databáze. Porovnání vzorků je relativně jednoduchý proces – pozice pásků ve sloupcích (viz obrázek 12.1.7).



DNA je vysoce individuální a unikátní – má vysoký potenciál stát se ideálním biometrickým identifikátorem.

Přirozenost DNA a stav současné technologie zabráňí DNA stát se efektivní biometrikou.

Nové technologie a výzkum výrazně snížily čas potřebný k tvorbě profilu DNA (přibližně pod 30 minut).

Obava osob ze zneužití informace z DNA – dědičné choroby, možné mutace, klonování...



Příklady otázek:

1. Jaké znáte nukleotidy?
2. Jak funguje replikace DNA?
3. Vyjmenujte kroky dešifrování kódu DNA.
4. Jak funguje kopírování DNA?
5. Jak funguje sekvencování DNA?



Odpovědi:

1. Strana 101.
2. Strana 102.
3. Strana 103.
4. Strana 103.
5. Strana 104.



## **13. Biometrické standardy**

V této kapitole se jsou popsány standardy, díky nimž je možná jak výměna dat, tak i integrace externích modulů do stávajících systémů. Jak zjistíme, standardů je celkem dost, ale mezi používané a akceptované patří jen část z nich.



## Standard

Utvořen běžným a opakovaným používáním pravidel, podmínek, směrnic nebo charakteristik produktů či spřízněných procesů a produkčních metod a souvisejících praktik managementu systémů [DeW05].



## **Technický standard**

Definice terminologie; klasifikace komponent; nástin procedur; specifikace dimenze, materiálu, výkonu, designu a funkčnosti; měřítka kvality a kvantity pro popis materiálu, procesů, produktů, systémů, služeb nebo praktik; testovací a vzorkovací metody; popis měřitek přesnosti, velikosti a stability ~ kombinace těchto pojmu tvorí technický standard [DeW05].

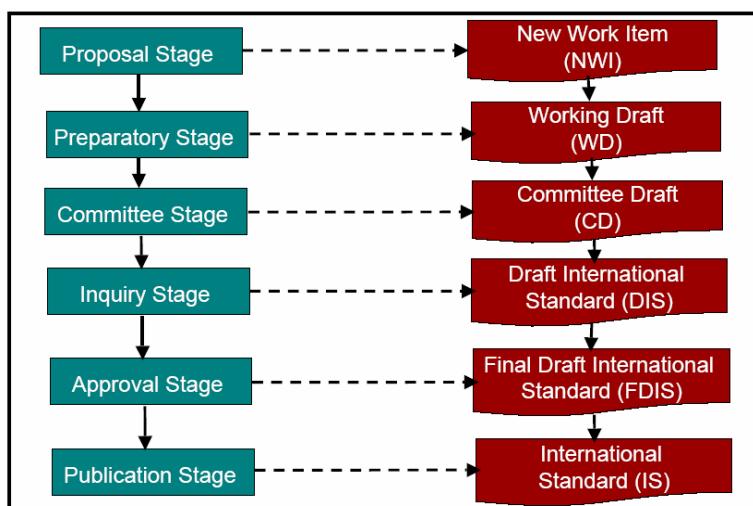
**Otevřený standard** – standard plně otevřený veřejnosti.



## Trocha historie:

- Do roku 1996 existoval pouze standard na otisky prstů – daktyloskopické karty a výměna dat pro forenzní medicínu.
  - Listopad 2001 – organizace INCITS (*International Committee for Information Technology Standards*) založila divizi pro biometrii, označenou M1.
  - V červnu 2002 vytvořila organizace ISO *Joint Technical Committee 1* (JTC1) subdivizi pro biometrii, SC37 (*Sub-Committee 37*).
  - V dalších měsících byly vytvořeny subdivize SC17 (*Cards and Personal Identification*) a SC27 (*IT Security Techniques*).

Průběh standardizace je znázorněn na obrázku 13.1.



Obrázek 13.1: Průběh standardizace



### Proč potřebujeme standardy?

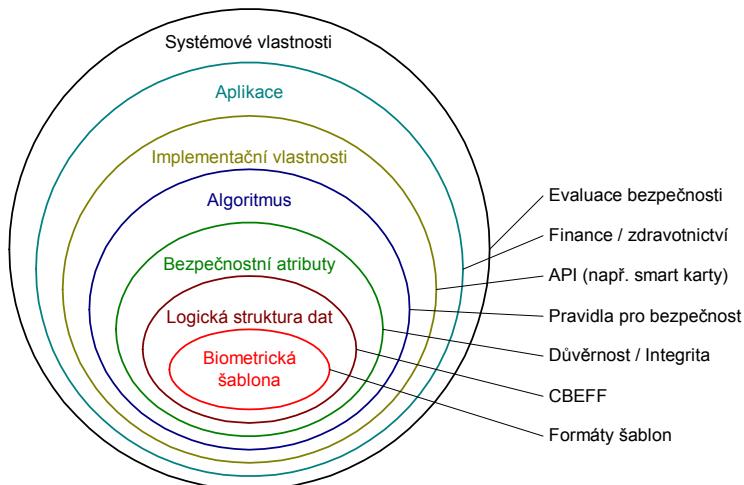
- V současnosti je výměna dat z různých biometrických systémů velmi limitovaná.
- Každý výrobce má vlastní formát, který je nekompatibilní s ostatními.
- Pro biometrické dokumenty je nutný standard, aby byla data použitelná i u jiného výrobce.
- NTTAA 104-113 (1996) – *National Technology Transfer and Advancement Act* – donucovací prostředek ke standardizaci, ovšem je nutný dohližitel – v USA např. NIST či DoD.
- 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:

- Standardy k výměně dat
  - Aplikační struktura
  - Datové formáty
- Standardy pro výkonnost biometrických systémů
  - Best Practices pro testování
  - Standardní databáze
  - Praktiky při tvorbě reportů
- Standardy pro celkovou bezpečnost systémů
  - Zjišťování zranitelnosti dle standardních postupů
  - Ochrana dat
  - Zajištění funkčnosti komplexní ochrany

Struktura biometrické aplikace je znázorněna na obrázku 13.2.



Obrázek 13.2: Struktura biometrické aplikace



Obecné rozdělení biometrických standardů:

- **Forenzní a identifikační standardy**
- **Datové standardy**
- **API standardy**
- **Bezpečnostní standardy**
- **Testovací a certifikační standardy**
- **Jiné standardy** (např. COPRAS – Cooperation Platform for Research & Standards).

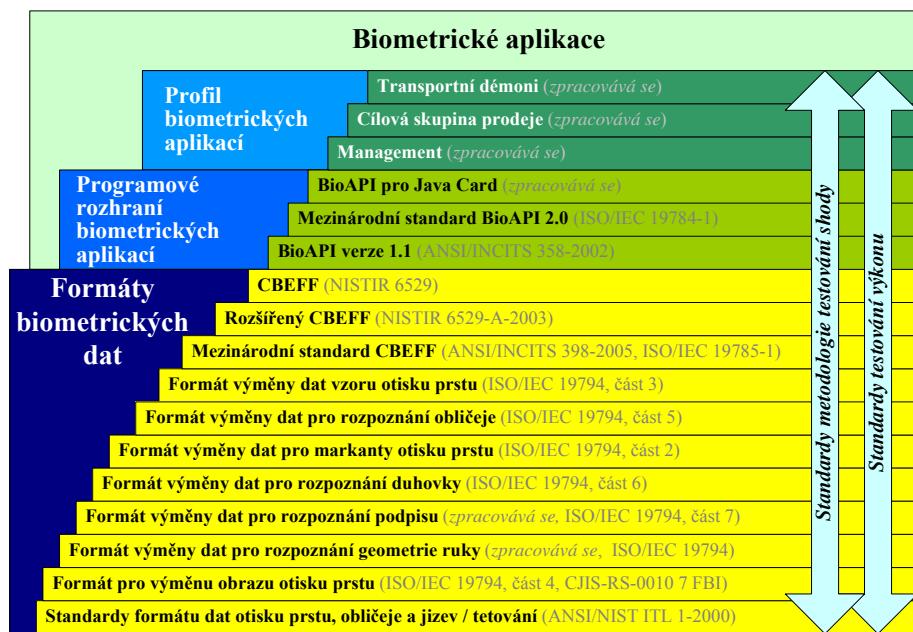


### Forenzní a identifikační standardy

- **ANSI / NIST ITL 1-2000** (*Data Format for the Exchange of Fingerprint, Facial and SMT Information*)
- **CJIS / FBI IAFIS-IC-0110** (*FBI Wavelet Scalar Quantization Standard*)
- **CJIS-RS-0010 7 FBI** (*Electronic Fingerprint Transmission Standard*)
- **AAMVA DL / ID-2000** (*National Standard for the Drivers License / Identification Card*)
- **ANSI / INCITS B10.8** (*Identification Cards Standard*)
- **ISO JTC1 SC17** (*Cards and Personal Identification*)



Přehled standardů je znázorněn na obrázku 13.3.

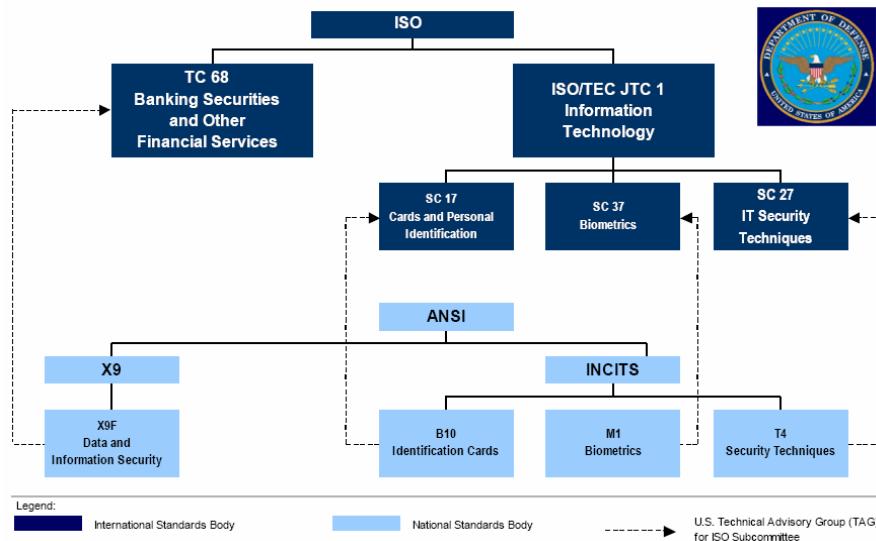


Obrázek 13.3: Přehled standardů

Přehled základních organizací, které se zabývají 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](http://www.biometrics.org/html/work_groups.html)
- DoD-BMO, BEMWG
  - <http://www.biometrics.dod.mil>
- U.K. BWG, FVC2004, FVRT2004, IBG



Obrázek 13.4: Přehled standardů dle DoD (*Department of Defense*)

### BioAPI Consortium

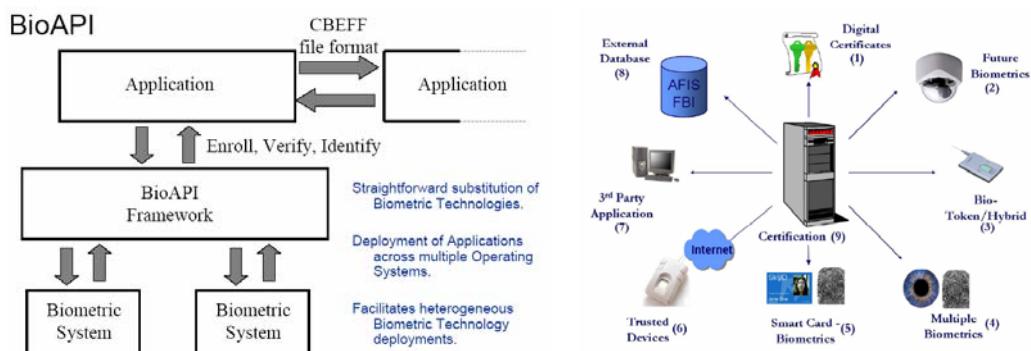


Založeno roku 1998

Účel: vývoj standardního API (*Application Programming Interface*) rozhraní k zajištění nezávislosti vývojářů vzhledem k rozhraní aplikace / zařízení (senzor)

Sedm zakladajících organizací: Bioscrypt, Compaq, Iridian, Infineon, NIST, Saflink, Unisys. Více jak 90 členů (65% ze severní Ameriky, 25% z Evropy a 10% z Asie); patří sem průmysl, vláda a akademické instituce.

Struktura standardu BioAPI je znázorněna na obrázku 13.5.



Obrázek 13.5: Struktura standardu BioAPI



## Standard X9.84

Organizace založena roku 2001

Účel: Bezpečnostní požadavky na registraci, verifikaci / identifikaci, uložení a přenos... Formát šablony kompatibilní s CBEFF.

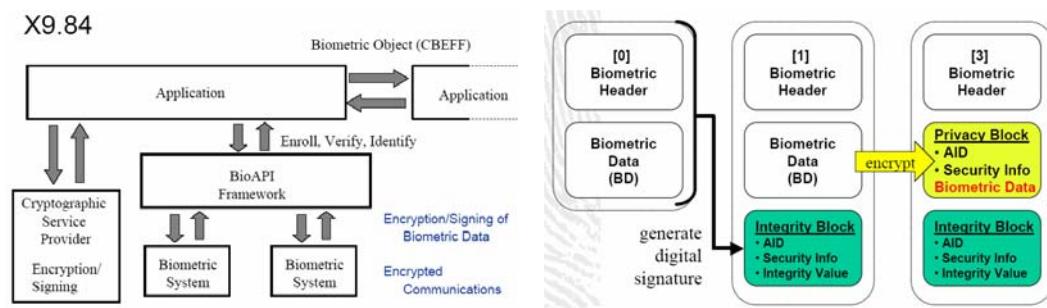
Členové:

- *Committee on Financial Services X9*
- *Subcommittee on Information Security X9F*

Požadavky:

- Chybovost menší než  $10^{-4}$  (verifikace / identifikace)
- *False Match* by mělo odpovídat použití PINu

Struktura standardu X9.84 je znázorněna na obrázku 13.6.



Obrázek 13.6: Struktura standardu X9.84



## Standard CBEFF

**CBEFF** = *Common Biometric Exchange File Format*

- Definuje základní pole pro biometrická data
- Registrace biometrických dat (IBIA)
- Umožňuje nové adaptace
- Publikován jako NISTIR 6529 roku 2001
- Nová verze se jmenuje NISTIR 6529-A
- Spolupracovníci:
  - Současní: BioAPI, ANSI X9.84, TOG CDSA HRS, NIST
  - Budoucí: AAMVA, XCBEFF (XML), ISO SC17 7816-11

Standard se skládá z *hlavičky*, *specifického datového bloku* a *podpisu*. Hlavička obsahuje:

- Bezpečnostní nastavení (např. šifrovaný, otevřený, ...)
- Integritní nastavení (např. podepsaný)
- Verze CBEFF hlavičky
- Vydavatel (např. *BioAPI Header Version*)
- Typ biometriky (např. obličej, otisk prstu, ...)

- Typ datového záznamu (např. zpracovaný)
- Účel záznamu (např. registrace)
- Kvalita záznamu
- Datum vytvoření
- ... a další údaje

### **Standard INCITS M1**



Formát pro výměnu dat. Zaměřen na otisk prstu, obličej a duhovku oka, tedy na biometrické charakteristiky využitelné v kriminalistice.

Tvořen organizací NIJ (*National Institute of Justice, Office of Science and Technology, USA*).

V rámci tohoto projektu byl vytvořen katalog biometrie (Biometrics Catalogue<sup>2</sup>), který obsahuje nejen různé typy biometrie (včetně návrhů na datový formát), ale i různé kategorie produktů, v nichž může být biometrie využita.

### **Standard „Best Practices“**



Účel: Popis nejlepších metod pro testování biometrických systémů.

Použití na jakoukoliv biometriku a aplikaci!

Rysy:

- Experimentální evaluace
- Evaluace technologie / scénáře / operační
- Definice experimentálních podmínek
- Reprezentace výkonnosti
- **ROC** křivky
- **FMR / FNMR + FTA, FTE, FTM**
- Detailní zpráva (pro opakovatelnost)

### **Common Criteria**



Pojem **Trusted Device** (obrázek 13.7)

- Šifrované komunikační kanály
- Zpracování on-board a šifrování

Integrace do bezpečnostní architektury (WinNT)

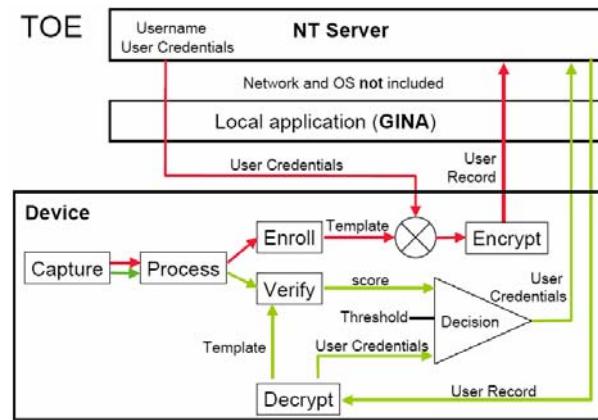
Definování slabých míst (zranitelnosti):

- Důvěrnost uživatelských dat (3DES)
- Integrita dat (podpis)
- Replikace starých dat (*Replay-Attack*)

---

<sup>2</sup> <http://www.biometricscatalog.org/>

- Reverzní inženýrství na firmware
- Analýza zbytků dat v paměti
- Latentní informace, falzifikáty
- Nastavení prahu (**FMR** / **FNMR**)
- Aktivní útok – následky a možnosti

Obrázek 13.7: *Trusted Device*

### Ochrana dat:

- Může / smí jiná aplikace číst a používat stejnou biometrickou šablonu?
- Pokud ano, jak je zajištěna důvěra mezi oběma aplikacemi?
- Jak zajistíme přístup k šabloně od neověřené aplikace?
- Mohou být data oddělena pro různé aplikace?
- Může toto všechno být docíleno, budeme-li brát na zřetel také principy ochrany osobních údajů (dat)?
- Musíme rozlišovat důvěrnost biometrických dat, důvěrnost osobních dat a důvěrnost šablony (souhrn obou dat do jedné množiny).

Deset principů privátnosti (CSA model):

1. Zodpovědnost
2. Účel – identifikace / verifikace
3. Souhlas – přímý / implikovaný
4. Limitovaná data (např. data bez os. údajů)
5. Limitované použití
6. Přesnost
7. Důvěrnost
8. Otevřenost (ochrana)
9. Individuální přístup
10. Vyžádané svolení



V této kapitole jsme probrali existující standardy pro biometrické aplikace. Rozlišujeme několik základních tříd standardů, přičemž nejvýznamnější z nich jsou pro výměnu dat (datové standardy) a standardy pro integraci modulů do biometrického systému (API standardy). Významnou skupinu tvoří i testovací a certifikační standardy, jejichž obsah úzce souvisí se 4. kapitolou této studijní opory.



Příklady otázek:

1. Co je to standard a technický standard?
2. Jaké typy standardů existují?
3. Popište standard BioAPI.
4. Popište standard CBEFF.
5. Co nalezneme v *Best Practices*?



Odpovědi:

1. Strana 107.
2. Strana 108.
3. Strana 110.
4. Strana 111.
5. Strana 112.



# 14. Biometrické systémy budoucnosti



V této závěrečné kapitole zmíníme na začátku čtyři atypické biometrické vlastnosti, jejichž význam v IT oblasti narostl až v poslední době. Mezi ně patří **tvar ucha**, **odontologie**, **otisk dlaně + přítlaky pera během psaní** a nakonec **3D tvar prstu**.

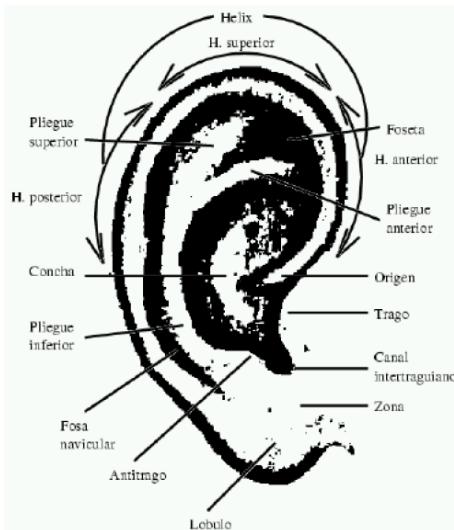
V následující kapitole popíšeme **multimodální biometrických systém**, jejichž význam začíná být silný.

Na závěr zmíníme další zajímavé aplikace, např. biometrické pasy.

## 14.1 Atypická biometrika – Tvar ucha



**Tvar ucha** (obrázek 14.1.1) může sloužit jak k verifikaci, tak i identifikaci. Porovnání je provedeno na základě komplexní struktury ucha. Růst ucha probíhá v prvních 4 měsících, pak se jen zvětšují proporce. Výhodou je možnost získání snímku na dálku – neinvazivní metoda.



Obrázek 14.1.1: Tvar ucha s popisem



### Anatomie ucha:

1. Vnější závit ucha
2. Ušní lalůček
3. Protizávit ucha
4. Concha
5. Tragus
6. Antitragus
7. Ústí vnějšího závitu
8. Delta
9. Intertragica

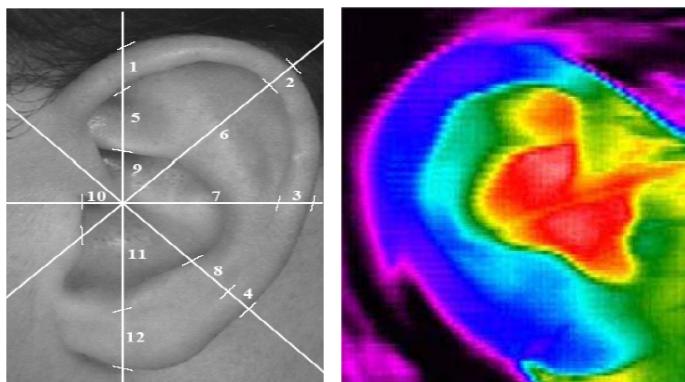
Možné aplikace, využívající tvar ucha:

- Bankovní automaty ATM
- Služby dohledu
- Forenzní aplikace
- Přístup do chráněných prostor
- Integrace do systémů na obličeji (z boku)



### Iannarellisův systém

Jedná se o antropometrický systém aplikovaný na ucho, využívající 12ti ušních rozměrů (obrázek 14.1.2a). Pro porovnání vyžaduje tento systém zarovnání a normalizaci obou uší. Rysy jsou uloženy s informací o rase a pohlaví. Na vyjádření vzdáleností se používají jednotky o rozmezí 3 mm, což je nutné z důvodu pohledu na ucho.



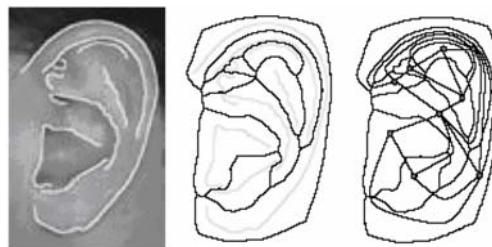
Obrázek 14.1.2: a) Rozměry Iannarellisova systému; b) Termogram ucha

### Limitace Iannarellisova systému

- Malá rozlišovací schopnost – máme-li v populaci odchylku o čtyřech 3 mm jednotkách, rozlišovací schopnost našeho systému je  $4^{12} \sim 17$  miliónům.
- Veškerá měření jsou vztahována k počátku (bodu 10). Je-li tento bod chybně lokalizován, ostatní body vykazují chybné odchylky.
- Rozpoznávání ucha není proveditelné, je-li ucho zakryto – lidé s dlouhými vlasy.



Další možnost je termogram ucha (14.1.2b). **Grafový model** (založen na diagramu Voronoi) ucha je znázorněn na obrázku 14.1.3.



Obrázek 14.1.3: Grafový model ucha



**Vlastní uši** („*Eigenears*“) – metoda podobná „vlastním obličejům (*Eigenfaces*)“, tzv. PCA metoda.

V obrázku 14.1.4 je ukázán postup předzpracování ucha.

1) Nalezení typických bodů (značek)



2) Předzpracování 2D dat

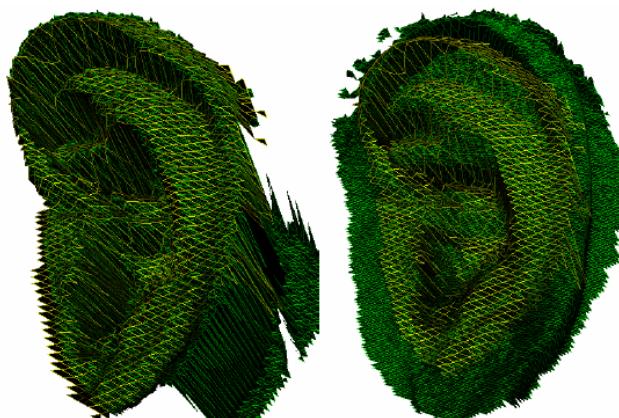
3) (Předzpracování 3D dat)



4) Extrakce ucha

Obrázek 14.1.4: Postup předzpracování ucha

Existuje i varianta porovnání 3D tvaru ucha (metoda využívající tvarů a zakřivení) – viz obrázek 14.1.5 (vlevo  $D=0,72$ , vpravo  $D=2,80$ ).



Obrázek 14.1.5: 3D porovnání tvaru ucha

## 14.2 Atypická biometrika – Odontologie



Trocha historie:

- Roku 66 !! bylo identifikováno tělo na základě dentální informace
- Roku 1849 byla provedena identifikace mrtvol po vyhoření vídeňské opery
- Roku 1849 zavedena odontologie do právního systému USA

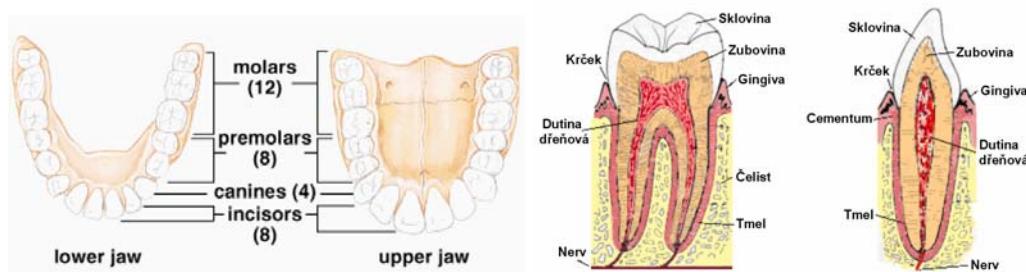
Aplikace:

- Identifikace osob
- Identifikace těl po mimořádných událostech
- Analýza otisků zubů (např. kousnutí)



## Základy:

Celkem 32 zubů → 4 typy zubů – stoličky (*molars*), zuby třenové (*premolars*), špičáky (*canines*) a řezáky (*incisors*) – viz obrázek 14.2.1a.



Obrázek 14.2.1: a) Zuby; b) Složení zuba

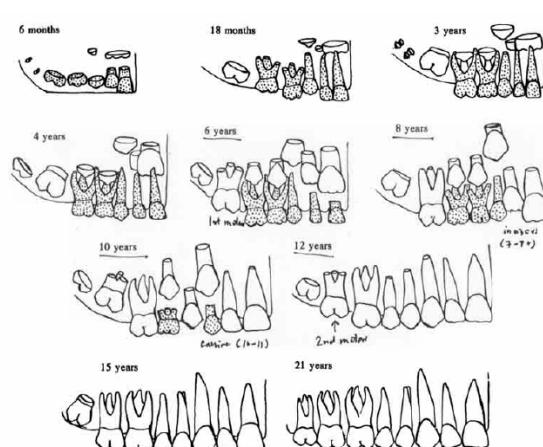
Složení zuba je ztvárněno na obrázku 14.2.1b. Opravy / náhrady zubů:

- Korunky
  - Výplně
  - Kanálky s kořeny
  - Můstky
  - Extrakce



## Individualita zubů:

- Mnoho kombinací oprav / úprav
  - Velikost a orientace mohou být značné
  - Velké množství tvarů zubů
  - Velké množství tvarů kořenů



*Figure 3.3A Average developmental stages of the human dentitions from 6 months of age to 21 years. Stippled teeth represent the milk (deciduous) dentition.*

Obrázek 14.2.2: a) Dentální karta; b) Určení věku ze zubů



Identifikace pomocí zubů:

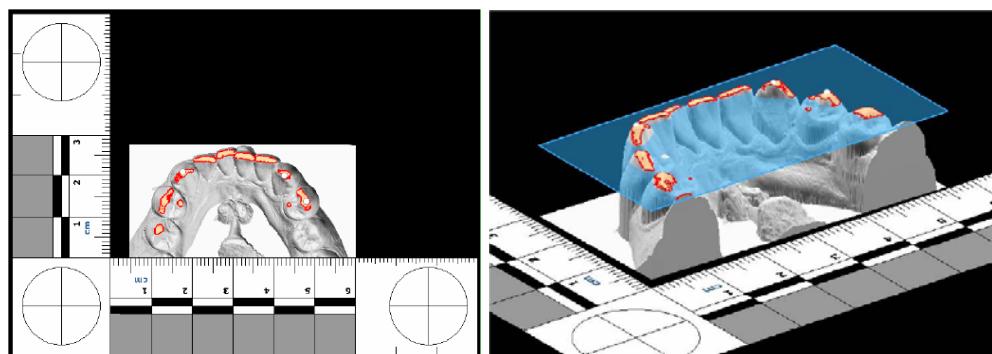
- Dentální karta (obrázek 14.2.2a)
- Rentgenové snímky
- Záznam prováděn u neidentifikovatelných mrtvol
- Určení věku (obrázek 14.2.2b)

Ve forenzní medicíně se využívá i kousnutí – ukázka je na obrázku 14.2.3.



Obrázek 14.2.3: Ukázky otisků zubů / kousanců

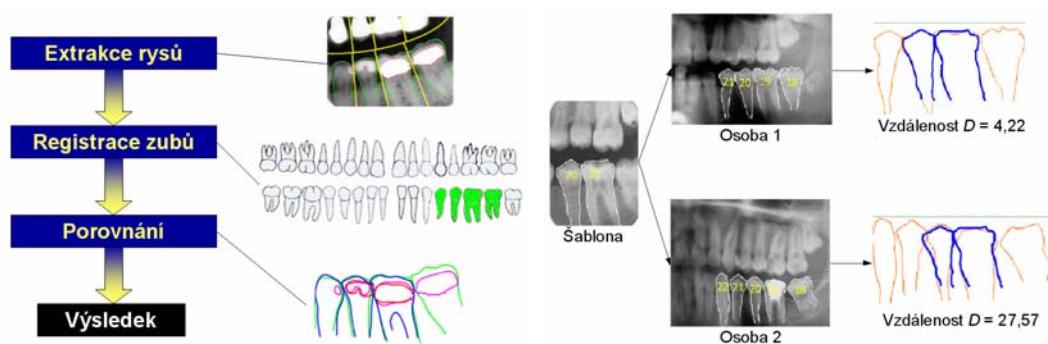
Analýza 3D snímků zubů (nejen pro biometrii, ale i pro tvarování nových zubů/korunek apod.) – viz obrázek 14.2.4.



Obrázek 14.2.4: Analýza 3D snímků zubů



Pro rozpoznávání se používá systém **ADIS** = *Automatic Dental Identification System*. Jeho struktura a funkční princip je znázorněn na obrázku 14.2.5.

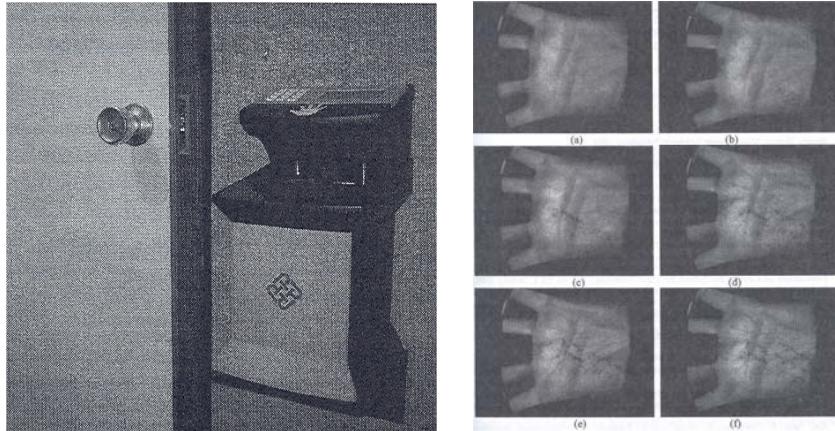


Obrázek 14.2.5: Systém ADIS

### 14.3 Atypická biometrika – Otisk dlaně, Přítlaky na pero a 3D prst



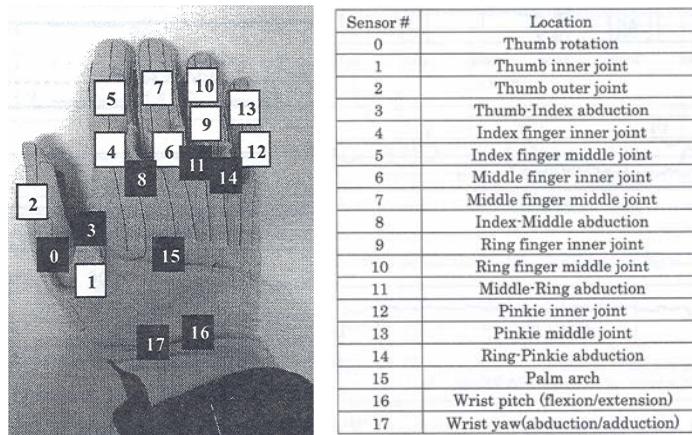
**Systém pro rozpoznávání obrazu dlaně**, včetně scanů dlaní je uveden na obrázku 14.3.1.



Obrázek 14.3.1: Systém na rozpoznávání obrazu dlaně + scany dlaní



**Systém pro rozpoznávání přítlaků na pero během psaní** je zobrazen na obrázku 14.3.2, včetně tabulky významu jednotlivých bodů.



Obrázek 14.3.2: Systém pro rozpoznávání přítlaku na pero během psaní



Pro zpracování **3D tvaru prstů** se používají pouze ukazováček ( $\alpha$ ), prostředníček ( $\beta$ ) a prsteníček ( $\gamma$ ). Indexy v závorkách označují popisky tvaru, které se potom používají pro vyhodnocení.



### 14.4 Multimodální biometrický systém

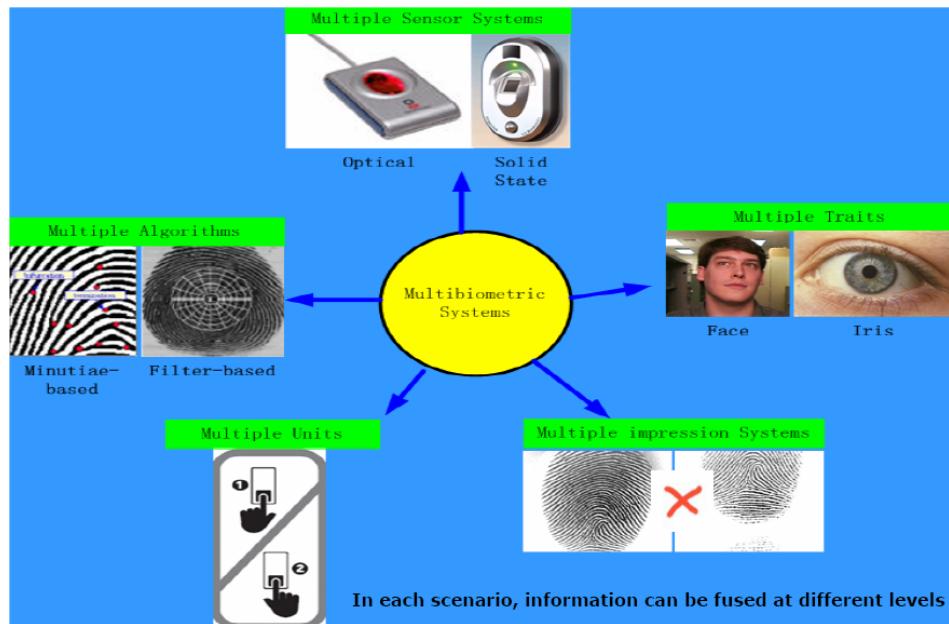
**Multimodální biometrický** systém kombinuje více biometrických vlastností do jednoho systému. Zvyšuje přesnost rozpoznání a zvyšuje rozlišovací schopnost na

větší počet osob. Snižuje šanci na podvedení systému – zfalšovat více biometrických vlastností je těžší jak pouze jednu.

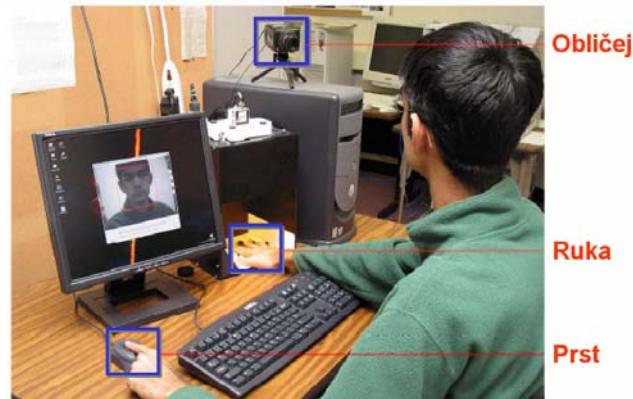
Výsledek je vytvořen:

- *Kombinací* – sloučení skóre porovnání do jednoho výsledku (např. střední hodnota).
- *Klasifikací* – spojení hodnot do vektoru – klasifikátory, fuzzy množiny apod.

Příklad multimodálního biometrického systému je na obrázcích 14.4.1 a 14.4.2.



Obrázek 14.4.1: Význam biometrického systému



Obrázek 14.4.2: Příklad multimodálního biometrického systému (3 biometrické vlastnosti – obličej, ruka a prst)

## 14.5 Další aplikace budoucnosti

### Forenzní aplikace

V minulosti se odehrálo mnoho katastrof, při kterých zahynul velký počet lidí. Těla obětí byla často znetvořena tak, že k identifikaci nemohly být použity běžné bi-



biometrické vlastnosti (např. obličej, otisky prstů), ale musely se využít zvláštní biometrické charakteristiky, jakými je např. dentální informace, příp. DNA.

Existuje malé procento případů, kdy nelze použít žádnou biometrickou vlastnost. V takovém případě lze fyzickou identitu pouze odhadnout, ale přesné určení není možné.



### Známé katastrofy:

- Útok na World Trade Center
  - 645 osob identifikováno pomocí DNA
  - 188 osob pomocí dentální informace
  - 71 osob pomocí otisků prstů
  - 19 osob pomocí fyzických anomalií
  - 16 osob pomocí fotografií
- Zřícení letadla Swissair Flight 111
  - 100 osob identifikováno pomocí DNA
  - 90 osob pomocí dentální informace
  - 30 pomocí otisků prstů



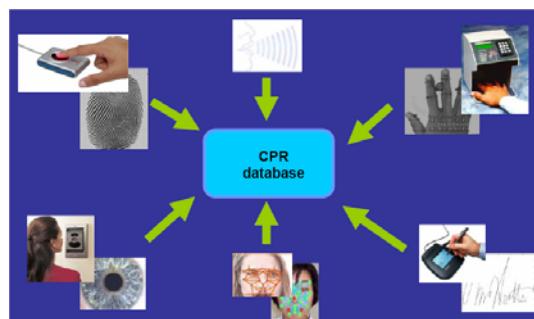
### Elektronická zdravotní karta

**HIPAA** = *Health Insurance Portability and Accountability Act*, Public Law 104-191, rok 1996

Jedná se o elektronickou zdravotní kartu, která je lehce dosažitelná pro kteréhokoliv lékaře. Údaje v této kartě jsou chráněny biometrickou informací – verifikace / povolení přístupu k informacím z karty.

### Starý systém – nedostatky:

- 28% - karta není připravena
- 11% - duplicita karet
- 34% - defekty karet
- 50% práce sester je práce s kartami



Obrázek 14.5.1: Elektronická zdravotní karta (CPR)

**CPR** = *Computerized Patient Record* – definice [Lin04] – obrázek 14.5.1:

Elektronicky spravované informace o zdravotním stavu a péči jedince během jeho celého života. Počítačový záznam kompletně nahrazuje papírovou formu a to tak, aby splňoval veškeré požadavky ze zdravotnického hlediska, právnického hlediska a hlediska ochrany osobních údajů. Takový záznam obsahuje neredundantní data – současný zdravotní stav, vyšetření, výsledky, poskytnutou péči apod.

Příklady CPR systémů:

- *Rex Healthcare, North Carolina* – 39 HandKey terminálů pro pacienty a zaměstnance
- *City Hospital, Bad Reichenhall* – rozpoznávání duhovky pro porodní oddělení
- *UC Davis Medical Center* – komunikátory rozpoznávající hlas
- Zavádí se i v ČR



### Bankovní aplikace

Biometrie se prosazuje silně do bankovní sféry – zajišťuje bezpečnost a zároveň i informace o pohybu osob.

Otisk prstu:

- Bezpečnost transakcí
- Síťová bezpečnost
- Přístupové systémy
- Safetové schránky

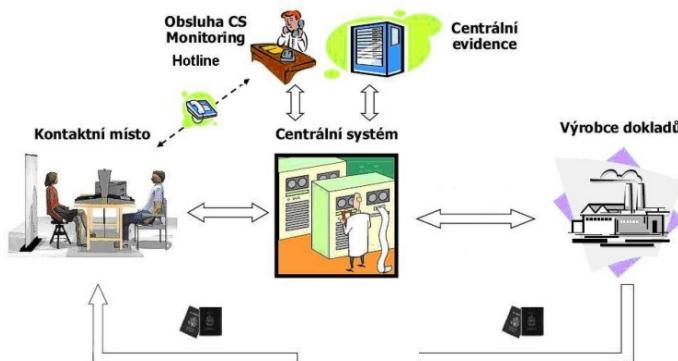
Hlas:

- Telefonní bankovnictví

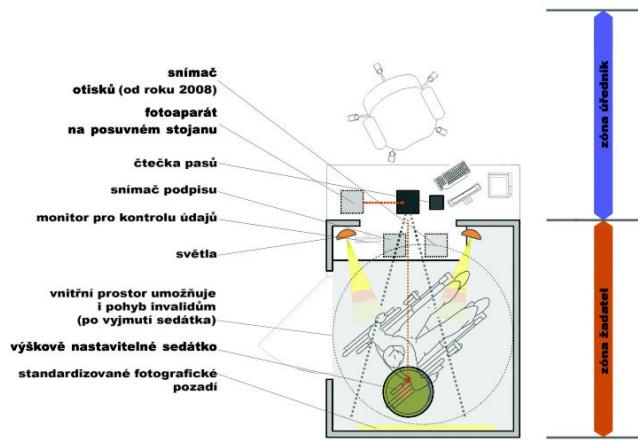
Hlavní cíl je zabezpečení kreditních karet – *Pay By Touch* (otisky prstů, 40 markantů), *Chameleon Cards* (otisky prstů), *MasterCard & VISA* (integrace otisků prstů).



### Biometrické pasy



Obrázek 14.5.2: Funkční princip biometrických pasů



Obrázek 14.5.3: Popis prostoru snímání dat pro biometrický pas



Obrázek 14.5.4: a) Pohled do zóny žadatele (vlevo); b) Pohled do zóny úředníka (vpravo)



### Totální identifikace

Každý z nás bude mít ihned po porodu implantován mikročip, který nás bude na prostě jednoznačně identifikovat – na bázi RFID tagů = totální identifikace (obrázek 14.5.5).



Obrázek 14.5.5: RFID tagy pro lidi



V této kapitole jsme se věnovali biometrickým systémům budoucnosti.

Nejprve jsme se věnovali atypickým biometrickým charakteristikám. Např. tvar ucha je jistě zajímavý, ale v praxi málo použitelný systém (UCHO je často skryto, navíc jeho rozlišovací schopnost není vysoká). Odontologie je oblast, která nalézá své uplatnění ve forenzní medicíně, zejména při identifikaci jinak neidentifikovatelných lidí. Pro přihlašovací účely uplatnění pravděpodobně nenalezne. Existují i varianty rozpoznávání otisku dlaně (i na ní se nacházejí papilární linie a vytváří anomálie v podobě markantů), příp. u písma můžeme doplnit systém pro rozpoznávání přítlaků na pero (zde je ovšem nutná speciální rukavice, což mnoho uživatelů odradí – nevíme po kom rukavici používáme) a na konec jsme si popsali rozpoznávání 3D tvaru prstu, což souvisí s geometrií ruky.

Zmínili jsme i multimodální biometrický systém, jehož význam narůstá - kombinace několika biometrických systémů do jednoho přináší docela dost výhod, zejména z pohledu bezpečnosti.

Mezi další aplikace budoucnosti patří především elektronická zdravotní karta. Tento systém byl spuštěn i u nás, ale zatím je s ním více problémů než užitku. V bankovnictví pomalu hledají biometrické systémy také své místo. A biometrické pasy netřeba zmiňovat. Po útocích na WTC v roce 2001 se celosvětový trend ubírá právě jednoznačnou identifikací lidí – kvůli hrozbě teroristických útoků.

Příklady otázek:

- 1. Jak funguje rozpoznávání tvaru ucha?
- 2. V čem jsou zuby individuální?
- 3. Znáte systém ADIS? Stručně popište.
- 4. Co je multimodální biometrický systém?
- 5. Znáte zkratku CPR? Stručně popište.



Odpovědi:

- 1. Strana 116.
- 2. Strana 118.
- 3. Strana 119.
- 4. Strana 120 – 121.
- 5. Strana 122 – 123.

# 15. Literatura



- [Bal02] Baltus R.: *Unterstiftenprüfer für Normalstifte*, Grafiken, Hesy, 2002
- [BIF04] Project BioFinger, 2004  
<http://www.bsi.de/english/publications/studies/BioFinger.pdf>
- [Bol04] Bolle R.M., Connell J.H., Pankanti S., Ratha N.K., Senior A.W.: *Guide to Biometrics*, Springer-Verlag, New York, 2004, ISBN 0-387-40089-3
- [Bon04] Bonfig K.W.: *Sensoren, Signale, Systeme*, MPA – Messen Prüfen Automatisieren, Band 5, 2004, ISBN 3-933609-19-4
- [Bou02] Bourke P.: *Gabor Function*, 2002  
<http://local.wasp.uwa.edu.au/~pbourke/other/gabor/>
- [Chi03] Chirillo J., Blaul S.: *Implementing Biometric Security*, Wiley Publishing, 2003, ISBN 0-7645-2502-6
- [Das03] Ďásek M.: *Biometrika*, Referát do BIS, EI, 2003  
<http://www.volny.cz/pretorian/biometrika.html>
- [Dau00] Daugman, J.: *How Iris Recognition Works*, University of Cambridge, UK, 2000
- [DeW05] DeWolfe S.: *DoD Biometric Standards*, Biometrics Fusion Center, ID Management Conference, 2005
- [Dit04] Dittman J., Vielhauer C., Schimke S.: *Biometrics (Vorlesung Biometrik)*, Otto-von Guericke Universität Magdeburg, 2004
- [Dra01] Drahanský M.: *Fingerabdruckerkennung mittels neuronaler Netze*, DP, FEI VUT v Brně, 2001
- [Dra05] Drahanský M.: *Biometric Security Systems - Fingerprint Recognition Technology*, Dissertation Thesis, FIT-BUT, 2005
- [Fie05] Fierrez-Aguilar J., Nanni L., Lopez-Penalba J., Ortega-Garcia J., Maltoni D.: *An On-Line Signature Verification System Based on Fusion of Local and Global Information*, Biometrics Research Lab., University of Madrid, AVPBA 2005, LNCS 3546, pp. 523-532, 2005
- [Hau04] Hauptvogel K.H., Ritzschke M.: *Biometrie um die Jahrhundertwende*, 2004
- [Hil04] Hill R.: *Retina Identification*, Portland OR, 2004
- [Ilo03] Ilonen J.: *Keystroke Dynamics*, Lappeenranta University of Technology, Finland, 2003
- [Ihm05] Ihmor H.: *Wird das Rad neu erfunden?*, BSI, 2005
- [Im01] Im S.K., Park H.M., Kim Y.W., Han S.C., Kim S.W., Kang C.H.: *A Biometric Identification System by Extracting Hand Vein Patterns*, Department of Electronics, Korea University, Seoul 136-701
- [Jai04] Jain A.K.: *Biometric Recognition*, Michigan State University, 2004
- [Jai04A] Jain A.K.: *Fingerprint Matching Techniques*, Michigan State University, 2004
- [Joz72] Jozefek A.: *Principy některých daktyloskopických klasifikačních systémů*, Ústav kriminalistiky Právnické fakulty UK, 1972

- [Kra05] Krawczyk S., Michaud C.: *Biometrics in the Banking Industry*, CSE 891, Spring 2005
- [Lin04] Ling Q., Bardzimashvili T.: *Biometrics in Computerized Patient Record*, 2004
- [Mac04] Mack M., Huang W., Jain A.K.: *The Evaluation of Face Recognition Systems*, Michigan State University, 2004
- [Maj99] Majoros B.: *Naive Bayes Models for Classification*, 1999  
<http://www.geocities.com/ResearchTriangle/Forum/1203/NaiveBayes.html>
- [Man02] Mansfield A.J., Wayman J.L.: *Best Practices in Testing and Reporting Performance of Biometric Devices*, National Physical Laboratory & San Jose State University, 2002, ISSN 1471-0005
- [Mon99] Monroe F., Rubin A.D.: *Keystroke Dynamics as a Biometric for Authentication*, New York University & AT&T Labs Florham Park, USA, 1999
- [NN] N.N.: *Hand Geometry*, Michigan State University, 2004
- [Ors05] Orság F.: *Biometric Security Systems: Speaker Recognition Technology*, Brno, CZ, VUTIUM, 2004, s. 32, ISBN 80-214-2771-X
- [Pol04] Polli M., Verasovich N., Akhmedova O., Khaleghi S.: *Biometrie*, Universität Zürich, 2004
- [Soc01] Socolinsky D.A., Wolff L.W., Neuheisel J.D., Eveland C.K.: *Illumination Invariant Face Recognition Using Thermal Infrared Imagery*, Equinox Corporation, New York + Baltimore, 2001
- [Sol04] Soltysiak S., Valizadegan H.: *DNA as a Biometric Identifier*, 2004
- [Suu04] Suutala J., Röning J.: *Towards the Adaptive Identification of Walkers: Automated Feature Selection of Footsteps using Distinction-Sensitive LVQ*, Intelligent Systems Group, University of Oulu, Finland, 2004
- [Tot05] Toth B., von Seelen U.C.: *Liveness Detection for Iris Recognition*, NIST Workshop, Biometrics and E-Authentication over Open Networks, 2005
- [TT02] *Think Thermally*, May 2002
- [Wei05] Weisstein E.: *Wolfram MathWorld*, 2005  
*Binom. Distrib.*: <http://mathworld.wolfram.com/BinomialDistribution.html>  
*Chernoff Face*: <http://mathworld.wolfram.com/ChernoffFace.html>
- [Wik06] Wikipedia, 2006  
<http://www.wikipedia.org/>
- [Yeu04] Yeung D.Y., Chang H., Xiong Y., George S., Kashi R., Matsumoto T., Rigoll G.: *SVC2004: First International Signature Verification Competition*, SVC2004, 2004

# 16. Akronypy



AAM	Active Appearance Model
ADIS	Automatic Dental Identification System
AFIS	Automated Fingerprint Identification Systém
API	Application Programming Interface
ATM	Automatic Teller Machine
BDR	Bottom Differential Ratio
CBEFF	Common Biometric Exchange File Format
CC	Common Criteria
CCD	Charge-Coupled Device
CFT	Continuous Fourier Transformation
CPR	Computarized Patient Record
DET	Detection Error Trade-off
DFT	Discrete Fourier Transformation
DNA	Desoxyribo-Nucleic Acid
DoD	Department of Defense
DPI	Dots Per Inch
DTW	Dynamic Time Warping
EER	Equal Error Rate
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FDA	Fisher Discriminant Analysis
FFT	Fast Fourier Transformation
FIR	Far-InfraRed
FLD	Fisher Linear Discriminant
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
FRVT	Face Recognition Vendor Test
FSTC	Financial Services Technology Consortium
FTA	Failure To Acquire
FTE	Failure To Enroll
FTM	Failure To Match
FVC	Fingerprint Verification Competition
HDR	Height Differential Ratio
HIPAA	Health Insurance Portability and Accountability Act

HMM	Hidden Markov Models
IBG	International Biometric Group
ICP	Iterative Closest Point
IT	Information Technology
LDA	Linear Discriminant Analysis
LED	Light Emitting Diode
LPC	Linear Prediction Coefficients
LPT	Line Printer Terminal
MAE	Mean Alignment Error
MATCI	Miniature Analytical Thermal Cycling Instrument
MFCC	Mel Frequency Cepstral Coefficients
NIJ	National Institute of Justice
NIR	Near-InfraRed
NIST	National Institute of Standards and Technology
PCA	Principal Component Analysis
PCR	Polymerase Chain Reaction
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PWC	Parzen Windows Classifier
RAT	Regional Average Thresholding
RCP	Ridge Continuity Point
RFID	Radio Frequency Identification
RMP	Ridge Meeting Point
ROC	Receiver Operating Curve
SDK	Software Development Kit
SNR	Signal-to-Noise-Ration
STR	Short Tandem Repeats
TCP/IP	Transmission Control Protocol / Internet Protocol
TDR	Top Differential Ratio
UNHC	United Nations High Commision
USB	Universal Seriál Bus