Biometrické identifikační metody

Biometric identification methods

Bc. Petr Hrazdira

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

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

Zásady pro vypracování:

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

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kolektiv. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha : Grada Publishing, 2008. 631 s. ISBN 978-80-247-2365-5.**
2. **BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. 1. vyd. Kralice na Hané : Computer Media, 2005. 168 s. ISBN 80-86686-48-5.**
3. **PORADA, Viktor a kolektiv. Kriminalistika. Brno : CERM, 2001. 746 s. ISBN 80-7204-194-0.**
4. **MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. Kriminalistika. 2. přeprac. a dopl. vyd. Praha : C.H. Beck, 2004. 583 s. ISBN 80-7179-878-9.**
5. **NĚMEC, Miroslav. Kriminalistická taktika pro policisty. 1. vyd. Praha : Eurounion Praha, 2004. 328 s. ISBN 80-7317-036-1.**
6. **STRAUS, J.: Kriminalistika, kriminalistická technika : pro kvalifikační kurz kriminalistických expertů. Praha : Policejní akademie České republiky, 2006. 301s. ISBN 80-7251-216-1.**
7. **PORADA, Viktor. Teorie kriminalistických stop a identifikace : technické a biomechanické aspekty. 1. vyd. Praha : Academia, 1987. 328s, barev. obr. příl.**
8. **KAŠPAR, Karel. Kriminalistika : (Úvod, technika, taktika) [online]. Praha : 2008 [cit.]. Dostupný z WWW: http://www.vsrr.cz/pomucka/kriminalistika1.pdf.**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce je zpracována jako výukový materiál do předmětu Kriminalistické technologie a systémy. Dává určitý přehled v druzích dnešní biometrické identifikace člověka a vyjadřuje jejich vývoj na základě vývoje počítačových technologií. Popisuje vlastnosti těchto systémů a rozepisuje oblasti jejich využití, zaměřené zejména na bezpečnostně-komerční aplikace. Také vysvětluje důležité termíny pro orientaci v dané problematice, např. verifikace a identifikace. Práce také obsahuje obrazovou dokumentaci některých používaných systémů biometrické identifikace.

Klíčová slova: kriminalistika, systém, biometrický, metoda, verifikace, identifikace.

ABSTRACT

This thesis is prepared as a teaching material for the subject Criminalistics technology and systems. It gives some insight into the types of present biometric identification and describes their evolution on the basis of the evolution of computer technology. It describes the characterictics of these systems and focuses on the field of their utilization, mainly on security-commercial applications. It also explains terms important for orientation in the subject, such as verification and identification. The thesis also includes visual documentation of some used biometric identification systems.

Keywords: criminalistics, system, biometric, method, verification, identification.

Poděkování, motto

Děkuji JUDr. Vladislavu Štefkovi za vedení při mé diplomové práci a ostatním lidem za pomoc mi věnovanou při jejím řešení. Zvláště děkuji Bc. Tomáši Čechmánkovi za pomoc mi věnovanou při praktické časti mojí diplomové práce. Dále děkuji svým rodičům a blízkým za podporu, které se mi od nich dostávalo během mého celého dosavadního studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Na úvod je třeba vysvětlit, co to vlastně biometrie je. Zavedená definice nám říká, že se jedná o automatickou metodu autentizace, která je založená na rozpoznávání jedinečných biologických charakteristik subjektu, tedy živé osoby. Tato metoda vychází z přesvědčení, že některé biologické charakteristiky (fyziologické, morfologické) jsou pro každého živého člověka jedinečné a neměnitelné.

Již dávní Egypťané popisovali např. prodejce obilí nebo lidi pracující na stavbě pyramid, aby jim poté mohla být jednoznačně vyplacena odměna. Měřila se třeba délka lokte, rozpětí palce a ukazováčku a zapisovaly se taktéž údaje o fyzických zraněních, které byly vidět navenek.

Z toho je vidět, že se víceméně nejedná o nic nového. Jenom s příchodem nových technologií a získáváním dalších a dalších vědomostí se z tehdejší „předpotopní" identifikace stala komplexní věda, která dnes využívá všechny výdobytky moderní civilizace, zejména tedy výpočetní techniky.

Potřeba jednoznačné identifikace člověka v minulosti existovala zejména kvůli vyplacení určité odměny nebo sloužila k poznání protřelého kriminálníka. Během a zejména na konci 20. století se biometrické systémy většinou uplatňují jak v pátrání po lidech (pachatelé, pohřešovaní, teroristé atp.), tak i v jejich rozpoznávání kvůli přístupu k určitým informacím či do určitého objektu. Požadavky na tyto aplikace jsou v současnosti na vysoké úrovni. U jednotlivých druhů se posuzují, krom jiného, dvě důležité věci a to míra chybného odmítnutí člověka uloženého v databázi (FRR) a míra chybného přijmutí člověka, který v databázi není (FAR). Je jasné, že hlavně druhé zmiňované se snaží výrobci snížit na co nejmenší možnou míru, ale i přesto zatím není stoprocentně jisté, že Váš systém nepřijme cizího člověka. Určitá možnost, větší či menší, podle aplikace, tu prostě je a s tím je potřeba počítat. Proto se používá u nejvyšší třídy zabezpečení ještě identifikace pomocí identifikační karty, nebo pomocí nějakého údaje, který zná jen oprávněná osoba (např. PIN či heslo), aby se míra ohrožení ještě snížila.

K rozmachu použití biometrických aplikací vedl nejznámější teroristický útok posledních let a to útok na americká „dvojčata" 11. září 2001 (World Trade Center – Světové obchodní centrum), kde zahynulo přes 3000 lidí a několik stovek bylo zraněno. Dodnes

mají obyčejní lidé i příslušníci zasahujících složek dýchací problémy následkem směsi jemného prachu a skla z padajících budov.

V reakci na tuto událost se biometrie ve Spojených státech amerických (USA) a v celém světě začala nekontrolovatelně šířit. Jedni to vítají kvůli vyšší bezpečnosti a druzí zase protestují, jelikož tím, že jsou skoro všude sledování kamerami a podrobováni prohlídkám, přicházejí o své soukromí. Dle mého názoru ale převládá kladná stránka celé věci a tak osobně proti biometrickým systémům nic nemám.

Toto téma jsem si vybral, protože mě tato problematika velice zaujala. Jedná se o moderní vědu, která se momentálně prosazuje skoro všude, nejen u identifikace lidí a přístupu do systému či budovy, ale i u obyčejných věcí jako je třeba notebook, který využívá otisk prstu. V budoucnu se s biometrií budeme čím dál tím více setkávat, a proto jsem se rozhodl celou oblast popsat, zejména charakterizovat jednotlivé druhy biometrických systémů a názorně je ukázat na přiložených obrázcích.

Ve své práci jsem vycházel z veřejně přístupných materiálů. Informace z nich načerpané jsem analyzoval a setřídil s cílem vytvořit ucelený přehled informací o tomto tématu.

I. TEORETICKÁ ČÁST

1 IDENTIFIKACE

Potřeba identifikace a samotné toto slovo se v poslední době stalo doslova hitem. Jednak jde o větší zájem o tuto problematiku ze strany společnosti a jedinců v ní a u dalších o nutnost se tímto zaobírat kvůli své praktické činnosti, kdy pro jejich práci je nesmírně důležité odlišit od sebe navzájem podobné jevy, činnosti, procesy, potřeby, zájmy, osoby, zvířata, předměty apod. Ve většině případů jde o ochranu určitých zájmů, např. společenských, státních, soukromých či komerčních.

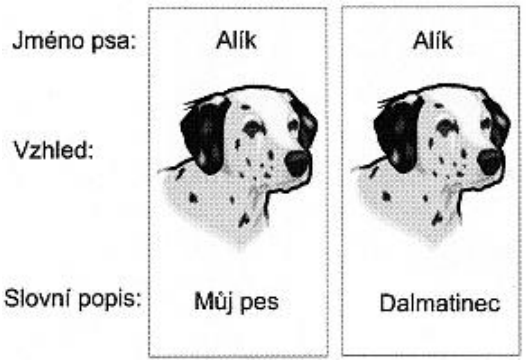
Není to ani tak dávno, kdy se pojem identifikace používal vesměs jenom ve vojenské a bezpečnostní oblasti. Vědecky založená identifikace probíhala na kriminalistické a forenzní úrovni.

Zájem o identifikaci a také o její metody a postupy stoupl ruku v ruce s rozvojem lidstva, světové politiky a moderními technologiemi (informatika, komunikace atd.). V civilní sféře, jak jsem již řekl, hlavně po útoku v roce 2001 na Světové obchodní centrum v USA.

1.1 Identita a identifikace

V prvé řadě je potřeba pro pochopení dalšího textu vysvětlit, co tyto stěžejní termíny znamenají. Slovo identita obecně znamená totožnost. Jedná se o to, že jestliže porovnáváme dva objekty a lze mezi ně dát znaménko rovná se, mluvíme o identitě. O té se dá mluvit ve dvou úrovních. Za prvé je to příklad shody, kdy slovní popis je jiný, ale věcný obsah je stejný. Příklad uvádí Roman Rak a kolektiv např. tento: trojúhelník rovnostranný je totéž jako trojúhelník rovnoúhlý. Popis je různý, ale podstata, tedy obsah je stejný.

Druhou úrovní je absolutní totožnost, kdy se pojmy shodují jak ve znacích, tak i v rozsazích. Např. auto = auto.



Obr. 1. Jeden a ten samý pes je popsán dvěma osobami. Popis je sice jiný, ale i tak se jedná o identické zvíře. [1]

Obr. 2. Dva různí psi jsou popsání naprosto stejně, ale i přes to se nejedná o identické zvíře. [1]

Obecné pojetí je, že „něco“ je s „něčím“ identické, pokud splňuje určité náležitosti, má všechny své vlastnosti stejné jako druhý objekt. Za identické objekty považujeme takové, o nichž platí, že vše to, co lze vypovědět o jedné z nich, lze také vypovědět o druhé. [1]

1.1.1 Identita osoby

Otázka lidské identity je poněkud složitější. Lidská identita je souhrn psychických a biologických, vrozených i získaných vlastností, jak individuálních tak i speciálních, kde důležitou roli hraje schopnost vnímat sám sebe. Každý jedinec je individuální a taktéž identický pouze sám se sebou. Problematiku lidské identity můžeme posuzovat podle několika hledisek:

1. biologická identita – nezávislá na vědomí osoby; dědičné a získané biologické vlastnosti člověka, je dána strukturou deoxyribonukleové kyseliny (DNA).
2. identita z hlediska psychologie – jedná se o totožnost vědomí; zdravý jedinec si po celý život uvědomuje svou identitu a i přes její různé změny v průběhu času se stále cítí být tou samou osobou.
3. identita osoby v souvislosti s termíny osobnost, individualita či individualismus – identita je slovo nezaměnitelného významu, které lze nahradit jen slovem totožnost.
4. sociální identita – jedná se o to, že každý patří do určité sociální skupiny na základě společenských, jazykových, geografických, kulturních a jiných vlastností.

5. více identit – některé osoby si identity mění či používají několik identit naráz, může jít o osoby provádějící kriminální nebo zpravodajskou činnost, ale také o herce či umělce a jiné.

1.1.2 Identifikace

V prvé řadě si musíme říct, že jde o proces, a to buď:

- takový, který prokazuje či zjišťuje identitu,
- takový, kterým se vyhodnocuje identita jednoho objektu ve vztahu k dalším objektům,
- takový, který prokazuje či zjišťuje existenci konkrétní osoby,
- takový, jehož cílem je určit, zda porovnávané objekty jsou identické či ne.

Jedná se o proces, kdy porovnáváme dva objekty z hlediska jejich shod a rozdílů na základě všech jejich vlastností. Proces je to velmi složitý, neboť vlastností může být velmi mnoho a také proto, že tento rozhodovací proces by měl být realizován v konečném čase (omezený čas a kapacity). Dalším důvodem je to, že zpravidla bývá motivován určitými praktickými potřebami.

Kvůli neustále častější potřebě něco či někoho identifikovat se stále více setkáváme ve vyspělých zemích s automatickou identifikací, která je v dnešní době možná na základě rozvoje identifikačních prostředků a technologií. Podle Raka rozeznáváme tyto kategorie aplikací systémů automatické identifikace:

- záznam informací (např. docházkové systémy),
- identifikace a vyhledávání informací (např. informace o pacientovi v čárovém kódu na pacientově záznamu),
- identifikace a vyhledávání předmětů (např. vyhledávání dokumentů),
- řízení a kontrola stavů (např. inventura),
- sledování a řízení pracovních procesů (např. výrobní procesy),
- identifikace, sledování a kontrola lidí (např. kontrola vstupů do objektů),
- transakční procesy (osobní peněžní převody či na základě jiných vstupů, např. fax).

1.1.3 Identifikace včera a dnes v kostce

Pravěcí lidé žili na malém prostoru se známými lidmi. Rozeznávali se mezi sebou pomocí tváře, celkového vzhledu, řeči a dalších projevů chování. Vzdalovat se od rodného ohně příliš nemohli kvůli existenčním problémům a tak za známé považovali jen ostatní ze svého okolí a příslušníky okolních kmenů považovali za neznámé (nebezpečné). Ani věcí a činností, které bylo nutné identifikovat, nebylo mnoho.

Potřeba někoho identifikovat byla závislá na mobilitě lidí. Ta se začala zvětšovat až v období před 40 – 30 tis. lety, kdy se objevil člověk moudrý a po jeho dalším vývoji teprve začal využívat zvířata k přesunu z místa na místo (koně, velbloudy apod.). Dalším velkým bodem v oblasti mobility lidí byl vynález automobilu a jeho velké rozšíření v 70. letech 20. století. Zároveň se zlepšovala doprava železniční, námořní a letecká. Čím lepší (větší) byla mobilita lidí, tím více lidé navzájem komunikovali a tím více hrála roli vzájemná identifikace.

Jak už bylo řečeno, s technologickým pokrokem se člověk stále častěji setkává nejen s neznámými lidmi, ale také s věcmi, informacemi, jevy apod. Díky lehce dostupným komunikačním nástrojům (Internet, mobilní telefony, televize, noviny atd.) lze v okamžiku pozorovat osoby a věci, s kterými nejsme ve fyzickém kontaktu, ale existují klidně na opačné straně Země.

Informace a zkušenosti se stávají v současnosti stále žádanějším zbožím a obchod s nimi je velký business. Informace slouží jako zdroj poznání a moudrosti. Dá se říci, že kdo má lepší informace, má větší moc. Z toho vzniká problém jejich ochrany. Ta je dnes realizována především pomocí ochrany informačních systémů, protože většina informací je produkována a předávána právě pomocí nich.

Třeba při bezhotovostní úhradě, která je již dnes běžná, nás při převodu peněz může napadnout, zda je ten dotyčný, co platbu provedl opravdu ta osoba, za kterou ji považujeme nebo zda se za ni jen vydává a tím sleduje nějaké své obohacení či jiný prospěch. V konkurenčním boji se finanční ústavy předhánějí ve stupni zabezpečení soukromých údajů svých klientů (heslo, PIN), ale i tak jsou úniky takřka na denním pořádku.

Zdaleka ale nejde jen o ochranu těchto informací. Jsou další informace, které jen tak někdo nekoupí, např. vojensky citlivé technologie, zbraňové systémy, radioaktivní, chemické,

biologické nebo genetické materiály, drogy, léčiva, utajované informace, osobní údaje, know-how, lékařské tajemství atd. [1]

Střetáváme se tak s otázkou identifikace z pohledu bezpečnosti. Další může být třeba otázka logistická, kdy nás např. zajímá, zda se z našeho skladu něco neztratilo, co nám chybí, co je potřeba objednat apod.

Pokud chceme někoho nebo něco identifikovat, tak většinou nejdříve sbíráme a posléze ověřujeme jednotlivé informace o objektu, který identifikujeme. Nemusí se nutně jednat o osoby. Může jít také o živočichy, rostliny, předměty, ale i činnosti, požadavky, projevy atd. Jako příklad uvádí Roman Rak s kolektivem lékařskou diagnózu, kdy se na základě projevů choroby pacienta posuzuje podle statisticky nashromážděných informací druh jeho nemoci.

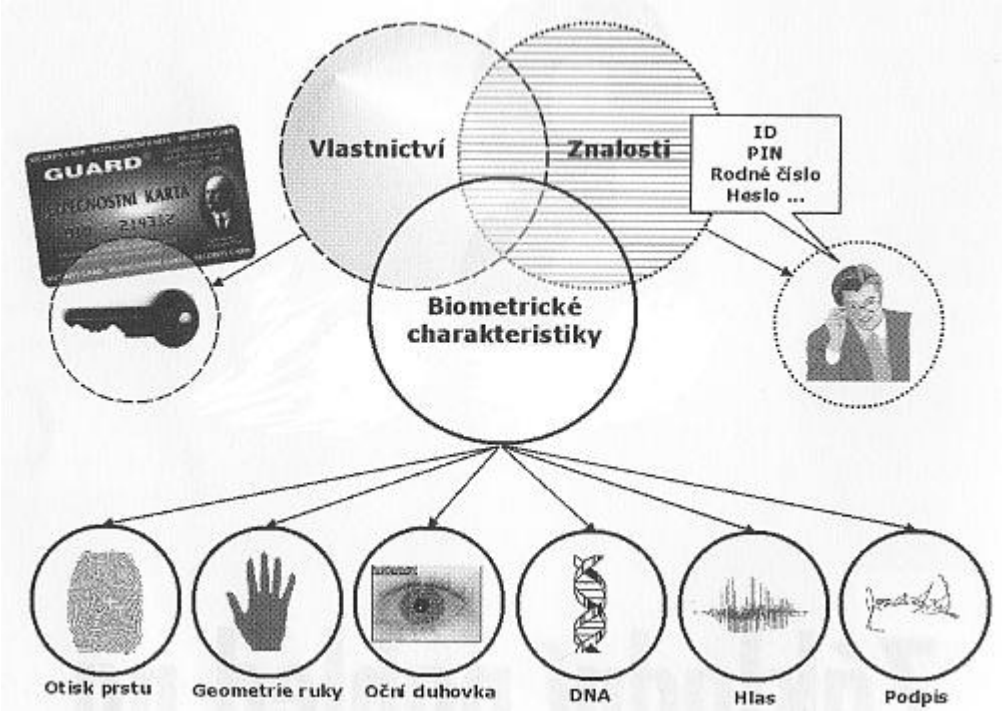
Z uvedeného vyplývá, že identifikace je proces velice náročný a složitý, který se týká nespočet vědních oborů a lidských činností. Z tohoto důvodu a hlavně také, jelikož nám jde o biometrii, budeme řešit jen identifikaci osob. Pozornost bude věnována zejména metodám a způsobům identifikace, které lze automatizovat pomocí výpočetní techniky a tím vlastně snížit cenu těchto systémů, na základě čehož je možný další rozvoj použití těchto technologií v běžném životě.

1.2 Identifikace osoby

Identifikace osoby je specifický případ identifikace jako takové. Můžeme na ni nahlížet z několika hledisek. Jednak můžeme rozeznávat vnější identifikaci, která se provádí na základě podoby člověka nebo vnitřní identifikaci, která demonstruje vnitřní myšlení a cítění člověka.

Když pomineme tyto dvě základní větve identifikace osoby, můžeme konstatovat, že člověka lze identifikovat podle nepřeberného množství věcí a informací. V zásadě ho lze však identifikovat na základě:

- ***znalostí,***
- ***vlastnictví,***
- ***biometrických charakteristik.***



Obr. 3. Základní způsoby identifikace osoby. [1]

1.2.1 Znalosti

Znalostmi myslíme určité informace či dovednosti, které má jenom určitá osoba. Například jde o znalost minulého jména, příjmení, znalost přezdívky, znamení, rodinného stavu, vyznávaného náboženství, skryté choroby atd. Hodně používané prostředky identifikace na základě znalostí jsou hesla či kódy. Může jít o klasická statická, která se nemění, např. k výběru hotovosti v bankomatu nebo přihlášení do e-mailové schránky či o dynamická, která se mohou měnit v závislosti na čase či místu přihlašování. Nevýhod takovéto identifikace je hned několik. Jednak může člověk heslo zapomenout, je mu odcizeno či odhadnuto, když si osoba nedá pozor a užívá jednoduchá hesla jako jméno, datum narození apod. Dále je riziko tím větší, čím víc přístupů si musíme pamatovat. V praktickém životě si toto ulehčujeme a v zásadě střídáme jedno či dvě hesla, což také není zrovna bezpečné. Identifikaci pomocí hesla lze využít zejména v méně rizikovějších aplikacích. Pro tvorbu hesla najdeme v každé knize o informatice či na Internetu několik rad, které se vesměs neliší. Můžeme je shrnout takto:

- délka hesla by měla být alespoň 8 znaků; čím více, tím lépe,

- heslo by nemělo obsahovat slova a už vůbec ne žádný údaj z našeho života (jméno, přezdívka, data jakékoliv významné události atd.),
- při tvorbě hesla použít jak malá a velká písmena, tak i číslice,
- používat speciální znaky (%, @, &, #, * a jiné),
- heslo pravidelně měnit,
- heslo nikomu neříkáme a ani si ho nikam nezapisujeme, a když už tedy musíme, tak nejlépe na místo, kam nemá přístup jen tak někdo (trezor). Pokud si hesla ukládáme do souboru na počítači, použijeme nějaký šifrovací program a soubor zašifrujeme. Nejsnadnější cesta je pomocí např. WinRARu, kdy soubor při komprimování zaheslujeme.

1.2.2 Vlastnictví

Vlastnictvím myslíme získané nebo nám přidělené věci a charakteristiky. Jedná se o nejčastější druh vnější identifikace člověka, na základě které je mu umožněn vstup mezi další lidi, do organizací, spolků, k zařízením, informacím a v neposlední řadě také ke komunikaci s různými orgány. Tyto identifikační znaky si jednak vybíráme sami na základě preferencí nebo nám jsou přidělena jinými lidmi (úředníci, bezpečnostní pracovníci atd.). Mezi tyto znaky zařazujeme: [1]

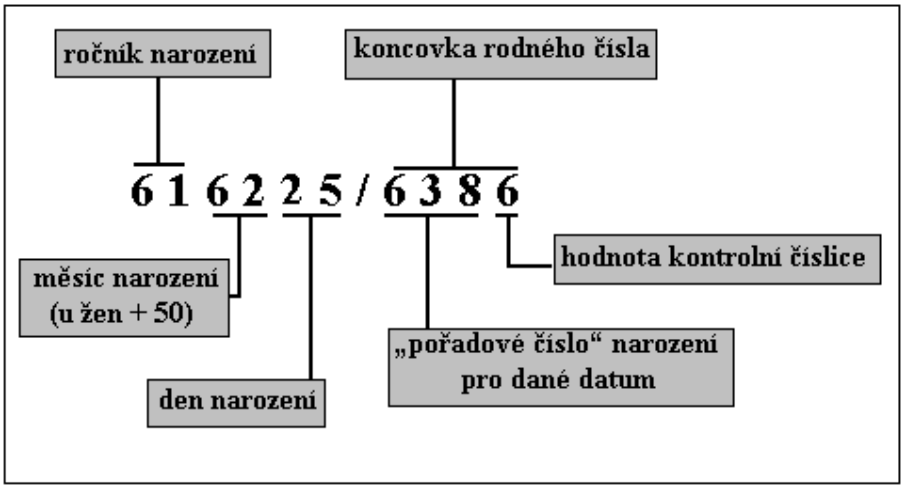
a) jméno a příjmení,
b) identifikační čísla a kódy,
c) osobní doklady,
d) identifikační karty a čipy,
e) biočipy.

Ad. a) Problematika u **jmen a příjmení** je v několika ohledech. Je možná lehká záměna, jelikož jich není tolik jako lidí. Jiným problémem je rozdíl mezi tím, jak je vyslovujeme a píšeme, zejména u cizích jmen. Další riziko je v jejich časové nestálosti a lehké změně.

Možným bližším údajem, který nám může pomoci při identifikaci určité osoby je buď např. prostřední jméno či titul a hodnost osoby. I tak je ale riziko záměny veliké.

Ad. b) V současné době (ale i v minulosti) používáme **čísla** k označení skoro všeho. Jednak lidí, ale i zboží, domů, knih, automobilů atd. Slouží k jednoznačné identifikaci objektu (rodné číslo, VIN kód, ISBN knih apod.). K ověření pravosti mohou mít některé číselné údaje kontrolní číslici, např. poslední číslice u rodného čísla (metoda modulo 11).

Příklad výpočtu kontrolní číslice: 616225638/11=56020512 zbytek **6** (kontrolní číslice)



Obr. 4. Schéma tvorby rodného čísla. [18]

Dalším častým typem identifikátoru je **čárový kód**, který nalezneme doslova všude kolem nás. Jeho jednoduchost, malá cena a velká vypovídací hodnota ho postavila do role čísla 1 v označování čehokoliv.

Obr. 5. Čárový kód. [19]

Hojně používané identifikátory jsou i technologie OCR (Optical Character Recognition), jejíž výhoda je v rozpoznání textu i bez speciálního snímacího zařízení. Dále je to radiofrekvenční kódování RFID (Radio Frequency Identification) a taktéž identifikace pomocí magnetických karet.

Hlavní nedostatky identifikačních čísel a kódů jsou tyto: nedodržení pravidel jejich tvorby, omezenost většinou na jednu zemi, lehká zneužitelnost.

Ad. c) Jako prvotní **osobní doklad** je brán rodný list, na jehož základě se vydávají další doklady. Dalšími doklady mohou být oddací list, cestovní pas, občanský průkaz, řidičský průkaz a jiné karty (kreditní, členské). V dnešní době již staré doklady ztrácejí na významu pro své nedostatky a tak se pomalu zavádí osobní plastové karty s čipy. Problémem u dokladů je možnost jejich falzifikace, či zneužití cizího dokladu. Tím největším kamenem úrazu je ale závislost na základním dokladu – rodném listu, jehož ochraně je věnována minimální pozornost.

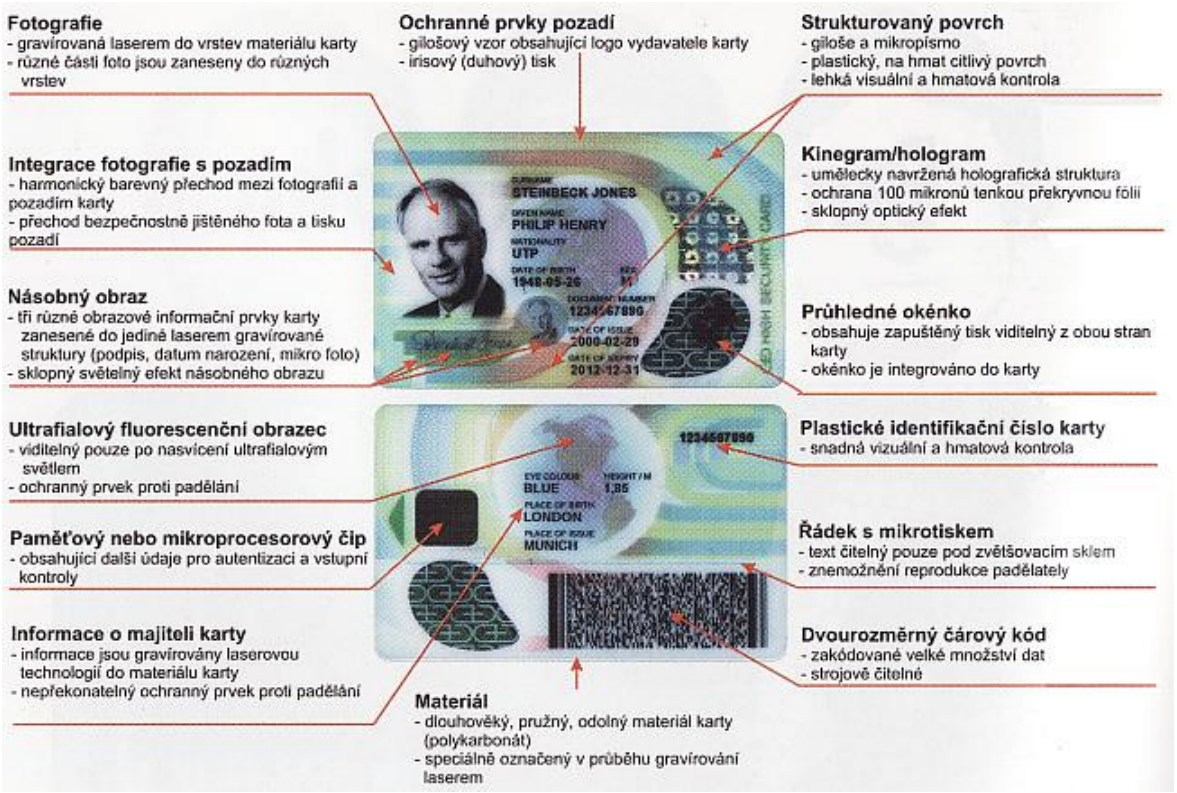
Ad. d) Plastové **identifikační karty a čipy** postupně nahrazují jejich papírové předchůdce díky efektivnějšímu a automatickému zpracování. Obsahují to samé jako papírové kartičky (foto majitele, údaje o něm, podpisový vzor atd.). Dnešní plastové karty jsou odvozeny od platebních karet a používá se jich několik druhů v nepřeberném množství aplikací, např. jednoúčelové občanské a řidičské průkazy sloužící státní administrativě, bankovní karty, karta pojišťovny, klubová karta či karty v supermarketech. Tyto karty používají také dopravní společnosti (pozemní, železniční, letecké, námořní), hotely, autopůjčovny, benzínové stanice, telekomunikační společnosti atd.

Důležité jsou zejména průkazy totožnosti (občanské průkazy, řidičské průkazy, služební, cestovní a diplomatické pasy), kdy každý druh karty má jiné požadavky na kvalitu zpracování, ochranu proti padělání a způsob zpracování.

Základní způsoby ochrany platebních a bankovních karet a různých identifikačních průkazů tak, jak je vyjmenovává Roman Rak:

- bezpečnostní tisk,
- hologram,
- kinogram,
- laserové gravírování,

- mikročip
- sklopný efekt,
- hmatové značky,
- mikrotext,
- UV barvy,
- fotografie držitele,
- podpis držitele,
- záměrná chyba,
- čárový kód,
- polykarbonátový nosič,
- měnící se barva,
- soutisková značka,
- podpisový proužek,
- tisk čísla karty na podpisový proužek,
- zvláštní embosovaný znak,
- elektronické kódy,
- tisk identifikátoru PIN na kartu.



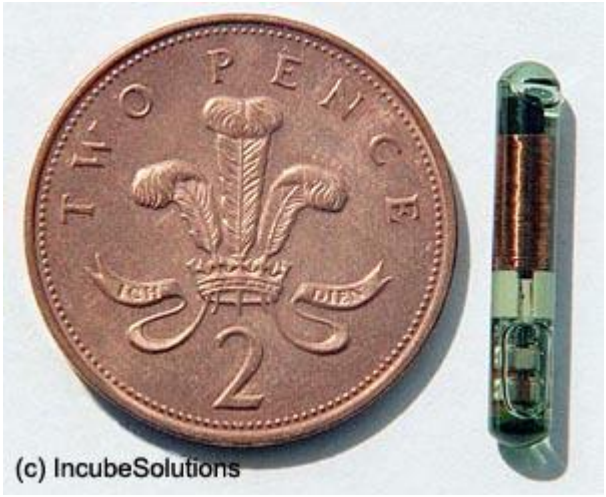
Obr. 6. Ukázka moderní plastové identifikační karty s ochrannými prvky. [1]

Nedostatky identifikačních karet jsou podobné jako u osobních dokladů. Je možná jejich falzifikace, odcizení či zneužití a i přes veškeré ochrany se tomuto nelze úplně ubránit. Lze je jenom stále zlepšovat, abychom dosáhli co nejmenšího rizika výskytu těchto problémů.

Největším problémem je vydávání na základě primárního dokladu – rodného listu. Jak jsem již zmínil, ten není nijak chráněn a po jeho odcizení může být cizímu člověku vydán zcela legálně pravý průkaz.

Ad. e) Biočipy se uplatňují po rozvoji výpočetní techniky zejména u zvířat. Mikročip velikosti zrnka rýže může například pomoci najít majitele zatoulaného psa. Také se jím značkují zvířata pro výzkumnou činnost. Umístění je jednotné u jednotlivých druhů, aby byla možná lehká identifikace po přejetí speciálním skenerem.

S identifikací lidí pomocí mikročipů to ale tak lehké není. Myšlenky sice občas takové jsou, označit všechny jedince čipem, ale narážíme zde na několik problémů. Největším z nich je asi možnost neustálého sledování kohokoliv, což je pro většinu lidí nepřípustné. Tyto čipy by například v sobě mohly nosit informace o majiteli (jméno, příjmení, datum narození, bydliště), ale i zdravotní záznamy a také by mohly ovládat věci kolem nás, např. otevírat dveře do domu, rozsvěcovat světla při příchodu atd. Využití GPS technologie také není nemožná. V budoucnu se předpokládá prvotní použití biočipů u speciálních kategorií lidí. Těmi mohou být osoby zvláštně nemocné (specifické nemoci, osoby s voperovaným kardiostimulátorem, alergici), drogově závislí, imigranti či trestanci.



Obr. 7. První čip implementovaný do těla člověka (profesor Kevin Warwick), 1998, Cyborg 1.0, délka cca 11mm. [20]

Biočip odstraňuje problémy, které mají všechny předešle uvedené technologie identifikace (znalosti, vlastnictví) – hesla, papírové doklady či plastové karty. Každá osoba by byla již od narození označena čipem a tak by existoval rychlý a přesný způsob, jak kohokoliv identifikovat. Další výhodou je možnost identifikace na dálku.

Nevýhody jsou u této technologie ale stále. Pořád se jedná o identifikaci na základě vlastnictví. Jenom se naše věci přesunuly z kapes do našeho těla. Určitě se najde někdo, kdo bude chtít zcizit cizí čip, aby tak mohl zneužít jeho identitu či zakrýt tu svou. Dalším problémem je fakt, že než by vznikla určitá standardizace, tak by se na trhu vyskytovalo mnoho druhů čipů a tím by existovala potřeba mít i několik čtecích či záznamových zařízení. Také na každou věc by byl například jeden čip, zdravotní záznam, platby, MHD, otevírání domu atd. Nenechali by se určitě ani zahanbit specializovaní zloději, kteří by určitě vymysleli jiný čip, který bude schopen nahradit ten v těle někoho jiného a využívat tak neprávem cizí identitu, např. k placení, kradení či k přístupu k informacím.

1.2.3 Biometrické charakteristiky

Biometrickými charakteristikami máme na mysli měřitelné biologické (fyzické) vlastnosti člověka jako je vnější vzhled, hlas, pach, rozměry a tvar těla, DNA, otisky prstů atd.

Základní myšlenkou je to, že biologické znaky každého člověka jsou jedinečné. Tzn., že každý člověk je identický jen sám se sebou. Identitu osoby je tak téměř nemožné napodobit, pozměnit či odcizit, protože identifikační znaky jsou přímo spojené s konkrétní osobou. Na to navazuje fakt, že biometrické znaky má každý člověk již od narození a jsou mu tudíž vlastní a nijak ho neobtěžují. Současný rozvoj technologií umožňuje to, že se biometrická identifikace stále více prosazuje ve všech oborech a směrech lidské činnosti.

Jak uvádí Rak, má biometrická identifikace několik hlavních výhod oproti jiným způsobům:

- nelze ji zapomenout nebo ztratit,
- je těžké až nemožné ji odcizit či napodobit,
- je nepřenositelná,
- vysoká přesnost a rychlost identifikace,

- je velice snadno a rychle použitelná,
- je lidsky přirozená,
- možnost plné či částečné automatizace.

Denně se každý z nás setkává s několika elektronickými zařízeními od mobilů po notebooky a mnohé z nich vyžadují identifikaci uživatele. Možnosti identifikace na bázi znalostí a vlastnictví jsou v dnešní době velmi nejisté a mnohdy velice průhledné a se zvětšujícím zájmem o elektronické transakce či komunikaci je riziko ztráty identity či jiných dat a peněz stále větší. Na základě tohoto se zvyšuje i zájem uživatelů a státní administrativy na tom, aby zabezpečení proti zneužití cizí identity bylo neustále zdokonalováno.

Můžeme říci, že biometrická identifikace v budoucnu zasáhne oblasti jako cestování a turistiku, telekomunikace, peněžní transakce, ochrana osob, majetku a informací, ochrana vstupu do objektů, identifikace osob, vyhledávání pohřešovaných osob, kontrola docházky, vězeňství či ochrana zbraňových systémů tak silně, že bude prakticky nenahraditelná.

1.2.4 Vliv výpočetní techniky

S rozvojem lidského poznání a tak, jak se rozvíjela věda a technika, společně s dalšími faktory jako pominutí studené války či globalizace světové ekonomiky, se spousta tajných strategických technologií uvolnila ke komerčnímu využití. Jejich uživatelé se tímto nenechali zaskočit a hojně tyto technologie začali využívat. Jak rostl jejich počet, snižovala se postupně cena těchto technologií, takže např. situace, kdy si osobní počítač mohla pořídit pouze finančně zajištěná osoba, je již dávno minulostí. I konkurenční boj mezi tržními subjekty na trhu umožnil další příliv nových technologií mezi jejich uživatele. Další změnou v posledních 10 – 20 letech je fakt, že výzkum a vývoj pomalu ale jistě přecházel a dále přechází z rukou státních institucí do soukromých rukou a jen málo světových velmocí si udržuje svůj vlastní (nákladný) vývoj špičkových technologií, určených primárně pro vojenské účely.

Jako příklad postupného zapojení výpočetní techniky můžeme uvést kontrolu vjezdu do objektu. Dříve tuto činnosti vykonávali vrátní na základě papírových dokladů. S rostoucím provozem se objevily identifikační karty, které po vložení do příslušného zařízení otevřely bránu. Tyto karty později z důvodu pohodlí vystřídaly kamerové systémy, které rozpoznaly registrační značku (RZ) vozidla a porovnaly ji s databází povolených RZ. Kvůli potřebě spíše než auto identifikovat osobu žádající o vstup, byly kamery nahrazeny biometrickými vizuálními identifikačními systémy, které identifikují osobu jedoucí ve vozidle a tak rozhodnou o jejím možném vstupu nehledě na auto, ve kterém jede. Případně tato identifikace může probíhat v kombinaci s povolenými RZ.

Identifikace lidí je ale daleko složitější, než se může na první pohled zdát. V minulosti byli lidé identifikování na základě osobní známosti. Během vývoje civilizace toto ale přestalo stačit a tak se později začaly k prokázání identity používat občanské či řidičské průkazy, rodné listy, pasy atd. Pro identifikaci k elektronickému přístupu se začaly používat hesla či PINy. Oba uvedené okruhy jsou vlastně vlastnictvím a znalostmi, tedy dvě věci, o kterých jsem již mluvil. Na jejich základě nelze ale s jistotou říci, že osoba používající daný doklad či přistupující do systému pomocí hesla, je skutečně ta osoba, za kterou se vydává. Proto se hledaly jiné způsoby a metody, jak osobu identifikovat. Metoda, jevící se jako nejperspektivnější pro budoucí využití, je již zmíněná biometrická identifikace vhodná jak pro bezpečnostní aplikace, tak pro obyčejný život.

2 BIOMETRIE

V závislosti na potřebě vzájemné identifikace mezi lidmi začali přední myslitelé a vědci intenzivně přemýšlet, jak od sebe odlišit jednotlivé osoby. Pamatovat si všechny anebo mít papírový popis bylo značně neefektivní, ne-li zhola nemožné.

Tak vznikla biometrie, což je metoda, která se zabývá identifikací a verifikací osob. Je založena na rozpoznávání jedinečných biologických charakteristik (znaků) každého člověka. Tyto znaky můžeme najít po celém těle i přímo v něm (DNA).

Rozvoj biometrie je spojen s vývojem výpočetní techniky, která může obrovské množství různých informací rychle a efektivně zpracovat a na základě výsledků jejich zpracování dokáže s větší či menší určitostí identifikovat danou osobu.

2.1 Historie biometrie

Historie biometrie a měření lidí je starší, než se na první pohled může zdát. Již od dávných dob existovala určitá potřeba jednotlivce identifikovat. Sice ne v takové míře jako dnes, ale určitou podobnost s dneškem určitě najdeme.

Dříve se lidé popisovali podle základních fyziologických vlastností jako jizvy, znaménka či jiná viditelná znamení (tvar tváře, barva vlasů, očí a pleti). V pozdějších dobách se tak dělo pomocí různých matematických údajů (délka různých částí těla, délka kroku aj.).

V dnešní době lze na člověku popsat tolik fyziologických a jedinečných vlastností, že záměna za jiného jedince je doslova nemožná.

Historii jako takovou rozdělím do 4 základních etap, z nichž každá zahrnuje určité období v dějinách lidstva.

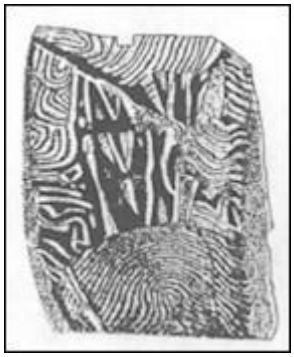
2.1.1 Dávné začátky

Jedná se o období několik tisíc let před naším letopočtem až po zhruba 13. století našeho letopočtu (n. l.) včetně.

Ač by se to nemuselo zdát, tak historie biometrie sahá až do dávné faraónské dynastie v Egyptě. Již tehdy se prováděla identifikace lidí za komerčním účelem. Měřili se zde pěstitelé obilí, kteří svou úrodu prodávali do státních rezerv. Na základě jejich identifikace podle unikátních jizev a poranění, charakteristik kůže, barvy očí, rozměrů a vah těla jim byla vyplácena odměna za prodané obilí.

Jiný historicky podložený případ je existence faraónského úředníka Khaseka, který měl na starost vyplácení mezd statisícům dělníků, kteří pracovali na stavbě pyramidy. Jelikož jeho faraón Khafre po něm chtěl i důkladný rozpočet na prováděnou stavbu, musel zabezpečit, aby nedocházelo k neoprávněnému vyplácení mezd. Proto nařídil svým podřízeným, ať vedou o každém dělníkovi podrobný záznam. V něm byly základní věci jako jméno, rodiče, věk, profese, popis obličeje a těla včetně viditelných zranění a také rozšiřující informace jako např. délka lokte, rozpětí mezi palcem a ukazováčkem ruky. Před každou výplatou byla osoba vždy detailně identifikována.

I v jiných částech světa byla biometrická identifikace známa. Například v dnešním státě Indiana byly nalezeny kameny s vyrytými obrazy, tzv. petroglyfy, které znázorňují lidskou ruku s vyznačenými papilárními liniemi. Tyto rytiny vytvořily indiánské kmeny, které obývaly toto území v období několika tisíc let před naším letopočtem (př. n. l.). Důvod, proč byly tyto obrazy zhotoveny, zatím nebyl objasněn.



Obr. 8. Kámen z období cca 2000 př. n. l. s naznačenými papilárními liniemi. [21]

Další civilizací, která znala otisky prstů, byli Asyřané. V troskách jejich známého města Ninive byla objevena část slavné Aššurbanipalovy knihovny založené v 9. století př. n. l. Tam se našly na hliněných deskách kromě textů i otisky prstů, které na ně umístili jejich autoři, aby tak předešli falzifikaci svého díla. Podobně toto fungovalo i v Řecku či na území Římského impéria, což dokazují archeologické vykopávky, při kterých se našla keramika, na níž byly otisky prstů.

Podobné snahy o využití charakteristik lidského těla a jeho chování jsou známy po celá další staletí. I staří Číňané znali daktyloskopickou[1] identifikaci. Babylóňané zase používali jako podpis na smlouvě otisk palce. Podobné to měli i v Persii.

2.1.2 Další rozvoj a využití

V této části se budu zabývat dobou mezi 14. a 18. stoletím n. l.

Asi první písemnou zmínkou o praktickém využití některé z metod biometrie je ta od cestovatele jménem Joao de Barros. Ten popisuje určité použití metody založené na otiscích prstů ve středověké Číně. Popisuje, jak jeden čínský kupec otiskuje pomocí inkoustu dlaně a chodidla svých dětí na papír, aby je od sebe vzájemně rozeznal.

Na evropském kontinentě popsal poprvé obrazce papilárních linií tvořené vrstevnicemi, spirálami a smyčkami v roce 1686 italský profesor anatomie Marcello Malpighi, který si ani neuvědomil jejich význam pro identifikaci.

Opravdový rozvoj biometrie ale nastal až v následujícím období.

2.1.3 Start opravdové vědy

Tato etapa zahrnuje 18. a 19. století n. l.

Prvním, kdo se hluboce zabýval biometrickými charakteristikami a to obrazci papilárních linií, byl až kolem roku 1823 český lékař a přírodovědec Jan Evangelista Purkyně. Jeho

[1] daktyloskopie – nauka o kožních papilárních liniích na prstech, dlaních a ploskách nohou

zájem byl však čistě lékařský a přírodovědecký, i když také navrhoval třídění jednotlivých otisků podle vyskytujících se geometrických vlastností. Tyto vlastnosti (kresby) rozdělil do 9 odlišných vzorů. Další významné osobnosti daktyloskopie byli William J. Herschei, Henry Faulds, Francis Galton a Edward Henry. Podrobněji bude tato metoda rozepsána až v samostatné kapitole 3.2.1.

Moderní historie biometrie se ale začíná psát až v souvislosti se jménem Alphonse Bertillion. Tento vědec, antropolog, etnolog a zaměstnanec oddělení identifikace pachatelů pařížské policie hledal nějakou metodu, která by mu umožnila identifikovat již jednou odsouzené zločince, a uvědomil si, že každý má určité tělesné znaky, které jsou stejné a nemění se, i když například člověk přibere na váze či si ostřihá vlasy. Jeho metoda se oficiálně nazývá Systém antropometrické identifikace, ale neoficiálně se označuje po něm, tzv. bertillonáž. Metoda je založena na popisu a geometrickém měření rozměrů lidského těla a hlavy.

Metoda ovšem nebyla zcela dokonalá, protože bylo možno najít dva jedince s totožnými mírami a tak ji koncem 19. století zcela nahradila identifikace založená na otiscích prstů.

Obr. 9. Ukázka měření v antropometrické laboratoři. [21]

Daktyloskopii položil věděcko-teoretický základ Francis Galton roku 1888 ve své práci, kterou tomuto tématu věnoval. Matematickými metodami vypočítal, že existuje 64 miliard různých možností uspořádání papilárních linií. Tímto fakticky prokázal, že neexistuje téměř možnost, aby existovaly dvě osoby se stejnými otisky prstů. Praktické základy položil sir W. J. Herschel, který otisky prstů využil při vyplácení důchodů penzionovaným

vojákům v Indii. Aby předešel vyplácení již mrtvým, musel každý příchozí při výplatě zanechat otisk ukazováku a prostředníku pravé ruky. Takto podvodům zabránil.

a) Alphonse Bertillion (1853 – 1914)

b) Francis Galton (1822 – 1911)

c) William James Herschel (1833 – 1917)

Obr. 10. (a, b, c) Významné osobnosti světové historie, které se zasloužily o rozvoj biometrických metod. [21]

2.1.4 Integrace výpočetní techniky

Zde se budeme pohybovat v době od konce 19. století n. l. až po současnost.

Jelikož otisk prstu vlastně vznikl jako první opravdový biometrický způsob identifikace osob, je jasné, že dále se kladl důraz zejména na něho. Až posléze se přidaly další možnosti jako DNA, tvar tváře, oční sítnice, oční duhovka atd.

Dalším poznatkem, na který přišel Joseph T. James z univerzity v Miami, byly dvě hypotézy, na kterých vlastně stojí daktyloskopie do teď. První je, že obrazce papilárních linií se po celý život člověka nemění a druhá říká, že žádní dva lidé na světě nemají shodné otisky prstů. Pro své tvrzení ale neměl žádný důkaz. S tím přišel až o dva roky později Francis Galton.

Významným krokem bylo založení identifikační divize Federálního úřadu pro vyšetřování (FBI) americkým Kongresem v roce 1924. Tato skupina zvolila jako základní identifikační metodu otisky prstů a v roce 1946 již jejich sbírka čítala 100 milionů karet. V roce 1971 jich již obsahovala 200 milionů.

Jako taková sloužila daktyloskopie od konce 19. století zejména k identifikaci pachatelů v kriminalistice a protože všechna porovnávání prováděli technici ručně, byl to proces velmi zdlouhavý a náročný. Toto se změnilo až s rozvojem výpočetní techniky v 60. a 70.

letech 20. století. Byly vyvinuty Automatizované identifikační systémy otisků prstů (AFIS), které do té doby nepříjemné porovnávání proměnilo jenom v možnost dlouhého čekání. Tyto systémy mohou porovnávat zvolený otisk prstu hned v několika databázích, ať už státních či mezinárodních. V dnešní době se zpracování daktyloskopických stop provádí, až na výjimky, výhradně pomocí počítačové techniky.

Technologie AFIS později pronikla i do civilní sféry, kde se používá ke kontrole přístupu do budov, k informacím, k bankomatům atd. Toto bylo ale možno až po rozvoji zejména snímací technologie v 80. letech 20. století. Masové rozšíření následovalo v letech 90., kdy na trh přišly levné optické snímače a rychlé a spolehlivé porovnávací algoritmy. Pro počítačové porovnávání je metoda získávání otisků prstů pomocí inkoustu náročná kvůli potřebě otisk napřed digitalizovat a tak se používají zejména elektronické snímače otisků.

Další metody biometrické identifikace měly podobný vývoj jako otisky prstů, avšak většího použití se samozřejmě dočkaly až po nástupu výpočetní techniky. V 80. letech 20. století se objevuje možnost identifikace pomocí sítnice a oční duhovky. Identifikace pomocí tvaru lidské tváře a podle podpisu je ještě mladší, 90. léta 20. století. Na přelomu 20. a 21. století nastupuje identifikace podle DNA. Několik nejpokrokovějších zemí světa, např. USA nebo Velká Británie (VB) zakládají národní registry DNA profilů pachatelů trestné činnosti. Ve Spojených státech amerických buduje za vynaložení obrovských prostředků FBI registr nazývaný CODIS (Combined DNA Index System), který shromažďuje profily DNA ze všech laboratoří v USA.

Dalšími biometrickými metodami, které se objevily či objevují v souvislosti s výpočetní technikou je identifikace podle hlasu či podle dynamiky stisku kláves.

Počítačově podporované identifikační metody se zabývají různými operacemi – vyhledávání, rozpoznávání a porovnávání obrazců, tvarů, objektů, povrchů, pohybu, zpracování 2D a 3D grafiky, animace, speciální optické, elektronické, laserové nebo sonarové senzory pro snímání obrazů atd. [1]

Závěrem lze říci, že čím větší a rychlejší bude pokrok ve výpočetní technice, tím více se budeme ve svém životě s biometrickými systémy setkávat. Důležitým faktem ovšem zůstává to, že aby se tyto technologie mohly masově rozšířit, musí je lidé nejdřív přijmout a musí jim především věřit.

2.2 Důležité pojmy a jejich členění

S pojmy jako biometrika, biometrická identifikace, autentifikace, verifikace a jinými se dříve veřejnost setkávala většinou pouze v televizi či literatuře a to v oblasti sci-fi. Je jasné, že si každý myslel, že to, co čte či vidí, je jenom výtvor myslí autorů a nijak nezohledňuje realitu. Opak je ale pravdou a důvod, proč tomu tak bylo, je jasný. Jednalo se vždy o utajované technologie, které střežily ty nejdůležitější zájmy vlád, a nikdo neměl zájem na tom, aby kdokoliv věděl o jejich existenci či dokonce fungování. S postupným vývojem počítačové techniky a jeho rozšířením mezi lidi, tyto technologie začaly vyplouvat na světlo, protože si subjekty na trhu uvědomily, že v těchto technologiích je skrytý velký potenciál zisku.

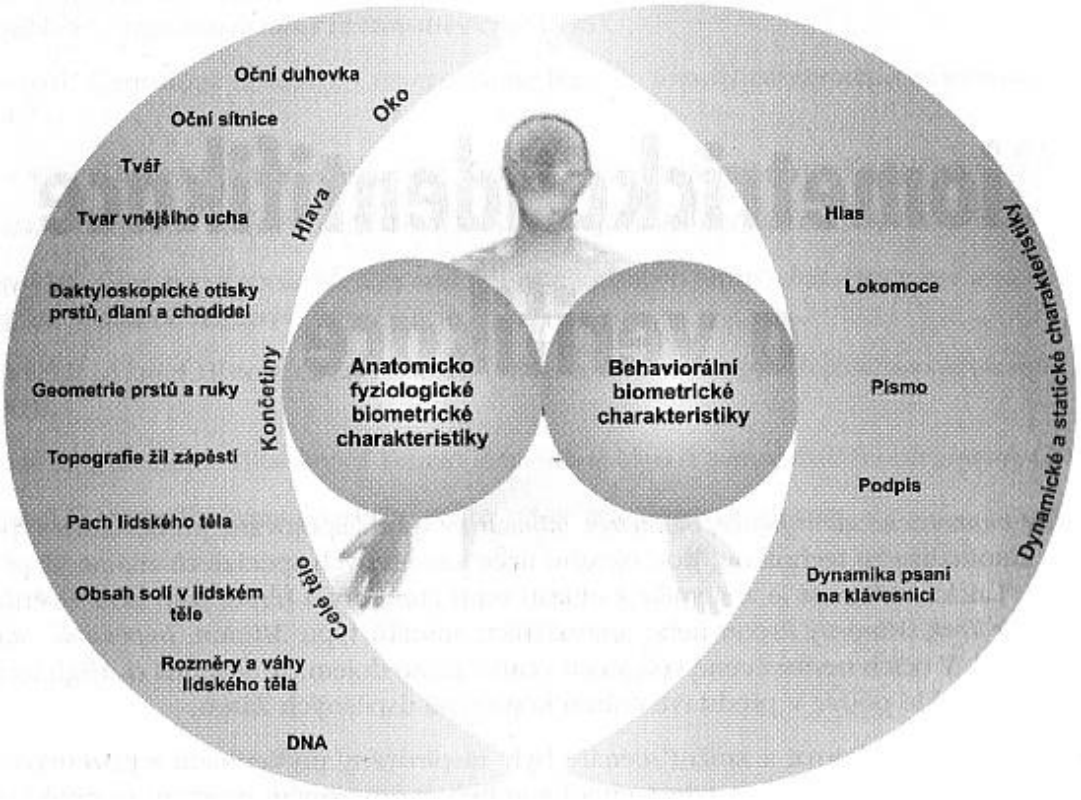
2.2.1 Biometrická identifikace

Při identifikaci (zjištění, ztotožnění) člověk identitu sám nepředkládá, systém prochází všechny (relevantní) záznamy v databázi, aby našel patřičnou shodu a identitu člověka sám rozpoznal. Systém odpovídá na otázku: „Kdo to je?“ [22]

Nasnímaný biometrický vzorek se porovnává s referenčními šablonami v databázi, a jakmile je nalezena shoda, je tato identita přiřazena žádající osobě.

K biometrické identifikaci můžeme přistupovat ze dvou pohledů. Prvním je pohled z hlediska anatomických a fyziologických charakteristik a tím druhým jsou behaviorální[2] charakteristiky, pomocí nichž ale není identifikace prováděna tak často, jako v prvním případě.

[2] behaviorální – behaviorální čili týkající se chování; pro identifikaci se využívají také specifické rysy lidského chování označované jako behaviorální.



Obr. 11. Dva základní přístupy ke členění biometrické identifikace. Pohled na v současnosti experimentální i praktické metody biometrické identifikace. [1]

Biometrickou identifikaci a verifikaci můžeme na základě přesnosti, spolehlivosti, objektivnosti, způsobu použití a praktického využití rozdělit dle Raka na:

a) policejně-soudní,

b) bezpečnostně-komerční,

c) ezoterickou.

Ad a) Policejně-soudní identifikace/verifikace

Důraz je kladen na identifikaci. Tato je používána bezpečnostními složkami či jinými orgány činnými v trestním řízení a jako taková patří k nejnáročnějším a zároveň nejspolehlivějším, jelikož jsou podloženy vědecky a prověřeny velkým množstvím zkoumaných vzorků. Závěry této identifikace se používají u soudních řízení a tak je velmi důležité vyhnout se jakýmkoliv chybám, jež bezprostředně ovlivňují lidské osudy. Výsledky těchto zkoumání vždy na konci hodnotí člověk, specialista v oboru (soudní

znalec), který tyto závěry taktéž popřípadě obhajuje u soudu. Hardware a software k vyhodnocování těchto informací je velice nákladný a proto existuje pouze několik specializovaných pracovišť (např. kriminalistické ústavy či policejní laboratoře), které toto vybavení vlastní. Je ovšem možný dálkový přístup oprávněných osob. K metodám zde používaným patří např. daktyloskopie, analýza DNA či lidského hlasu a analýza písma a podpisu.

Ad b) Bezpečnostně-komerční identifikace/verifikace

Důraz je kladen na verifikaci. Je odvozena od policejně-soudní a její metody se více nebo méně přizpůsobily požadavkům v bezpečnostní a komerční sféře. Obecně vzato jsou tyto metody méně přesné a jsou levnější díky svému rozšířenému nasazení než policejně-soudní. Některé metody byly zjednodušeny a jiné zase zdokonaleny. Všeobecné požadavky pro bezpečnostní aplikace je přístup buď do fyzických objektů či k určitým informacím (servery, bankovní transakce atd.). Komerční v tomto smyslu znamená, že tyto aplikace jsou volně k prodeji na trhu. Podstatným faktem je to, že tyto aplikace vyžadují automatizované systémy pracující v reálném čase a na to dřívější výpočetní technika nestačila. Až s postupným rozvojem počítačových technologií byl možný komerční přístup. Používané metody jsou zde např. daktyloskopie, oční duhovka, oční sítnice, hlas, tvář, geometrie dlaně a prstů ruky, podpis a dynamika psaní na klávesnici.

Ad c) Ezoterická identifikace/verifikace

Již název vypovídá o využívaných metodách. Ezoterická znamená přístupná jen zasvěceným. Tzn., že tato identifikace je známa jen úzkému okruhu specialistů a její metody se zatím běžně nepoužívají pro bezpečnostně-komerční aplikace. I pro policejně-soudní potřeby je využití minimální. Je to dáno nedostatečnou znalostí těchto metod, protože ještě nebyly prověřeny na širokém vzorku testovaných subjektů. Mezi metody, které zde řadíme, patří lokomoce (rysy lidské chůze), otisky rtů a pórů, pach lidského těla, tvar vnějšího ucha, topografie žil či obsah solí v lidském těle.

2.2.1.1 Pozitivní a negativní identifikace

Jedná se o dvě rozdílná pojetí biometrických aplikací, z nichž každá má za cíl něco jiného. U **pozitivní** jde o zabránění používání identity jedné osoby osobami jinými. Aplikace, která využívá pozitivní identifikaci, srovnává šablonu osoby, která žádá o vstup, s šablonami v databázi. Pokud žádná šablona nevykazuje shodu, je přístup osoby zamítnut. Pokud je nalezena shoda, je přístup povolen. Typické je použití např. pro vstup do chráněných laboratoří různého druhu.

Cílem **negativní** identifikace je zabránit tomu, aby se osoba přihlásila do systému více jak jednou, a to pomocí cizích identit. Jde o to, že získaná biometrická šablona od posuzované osoby se porovnává se šablonami uloženými v databázi a pokud najde shodu, je přístup dané osoby zamítnut. Pokud shoda není nalezena, je přístup povolen. Používá se např. k tomu, aby se jedna osoba nemohla přihlásit 2x do systému pod jinou identitou či nemohla pod jinou identitou volit nebo získat jiný prospěch.

2.2.2 Biometrická verifikace

Verifikace (autentizace) neboli také ověření je proces, při kterém subjekt předkládá tvrzení o své identitě (např. vložením karty nebo zadáním identifikátoru) a na základě takto udané identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají podle záznamů autentizační databáze. Odpovídáme na otázku: „Je to opravdu ta osoba, za kterou se sama vydává?“ [22]

Proces verifikace je podstatně méně náročný než identifikace, protože porovnává podle pravidla 1:1, kdežto identifikace 1:N. Verifikace vlastně ověřuje, zda osoba, která žádá o vstup, je skutečně ta, za kterou se vydává (prokazuje), např. na základě přístupové karty.

Základem je sejmutí biometrického vzorku, na základě něhož se uskutečňuje rozhodovací proces. Tento je u bezpečnostně-komerčních aplikací zcela automatizován a výsledkem je buď přijetí či odmítnutí osoby. V policejně-soudní je závěr rozhodovacího procesu v rukou lidské osoby, která rozhodne, zda je shoda šablony zkoumané a uložené v databázi dostačující pro jednoznačnou identifikaci jedince.

Referenční šablona, podle které se porovnává získaná šablona, může být nejenom uložena v centrální databázi, ale může být uložena přímo v identifikačním prvku osoby (např.

identifikační kartě). Tím odpadají problémy s jakýmkoliv datovým úložištěm a datovým přenosem. Vzorová šablona je přímo na kartě a ta se ihned porovnává v systému se získaným biometrickým vzorkem. Výsledkem není nic jiného než povolení či zamítnutí přístupu.

Jestliže mluvíme o ukládání dat, je potřeba poznamenat, že ukládat se mohou buď kompletní biometrické vzorky i s jejich odvozenými šablonami nebo pouze samotné šablony. První možnost je typická pro policejně-soudní aplikace, kdy původní vzorek je brán jako základní důkaz v soudním řízení. Pouze šablony se ukládají typicky v aplikacích bezpečnostně-komerčních, kde jsou kladeny na identifikaci menší nároky. Oba postupy ale mohou být různě kombinovány dle použité metody a našich potřeb. V každém případě jsou nároky na úložná místa obrovská a tak je kladen velký důraz na softwarové zpracování a komprimaci dat.

2.2.3 False Rejection Rate (FRR)

Hledisek, podle kterých můžeme porovnávat jednotlivé biometrické aplikace a tak posuzovat jejich nasazení je velké množství a jako takové je rozeberu v kapitole 2.3, ovšem jako nejdůležitější se pro všechny aplikace jeví charakteristiky FRR a FAR (vysvětlena v další kapitole). FRR znamená False Rejection Rate, v překladu pravděpodobnost chybného odmítnutí. Jedná se o možnost odmítnutí oprávněného uživatele. V bezpečnostně-komerčních aplikacích se nejedná o zásadní nedostatek, ale s počtem odmítnutých klesá uživatelský komfort a tím i důvěra k danému zařízení, potažmo k biometrii jako takové. Zato v policejně-soudní sféře jde o vážný nedostatek, kdy potencionální pachatel není v systému rozpoznán (ztotožněn) a tím ujde hrozícímu trestu.

FRR můžeme vypočítat pomocí jedné z těchto dvou rovnic: [1]

$$FRR = \frac{N_{FR}}{N_{EIA}}, \tag{1}$$

$$FRR = \frac{N_{FR}}{N_{EVA}}, \tag{2}$$

kde:

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

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

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

2.2.4 False Acceptance Rate (FAR)

Jak jsem již řekl, druhou důležitou vlastností biometrických systémů je FAR, tedy pravděpodobnost chybného přijetí neoprávněného uživatele. V reálu se jedná ještě o důležitější faktor než FRR, protože každého, kdo používá biometrickou identifikaci pro vstup někam nebo přístup k něčemu, nejdříve zajímá míra chybného přijetí neoprávněných osob. V případě této chyby nastává bezpečnostní incident, který může mít za následky dalekosáhlejší škody a tak je FAR velice důležitým hlediskem. V bezpečnostně-komerčních aplikacích je riziko FAR důležité z důvodů, které jsem již popsal výše, a tudíž opravdu nejde o zbytečné kritérium hodnocení celého systému. Pokud dojde k chybnému přijetí v policejně-soudní sféře, znamená to, že posuzovaná osoba je chybně ztotožněna s jinou osobou a tím pádem se celé vyšetřování ubírá úplně jiným (špatným) směrem.

FAR můžeme vypočítat pomocí jedné z těchto dvou rovnic: [1]

$$FAR = \frac{N_{FA}}{N_{IIA}}, \tag{3}$$

$$FAR = \frac{N_{FA}}{N_{IVA}}, \tag{4}$$

kde:

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

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

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

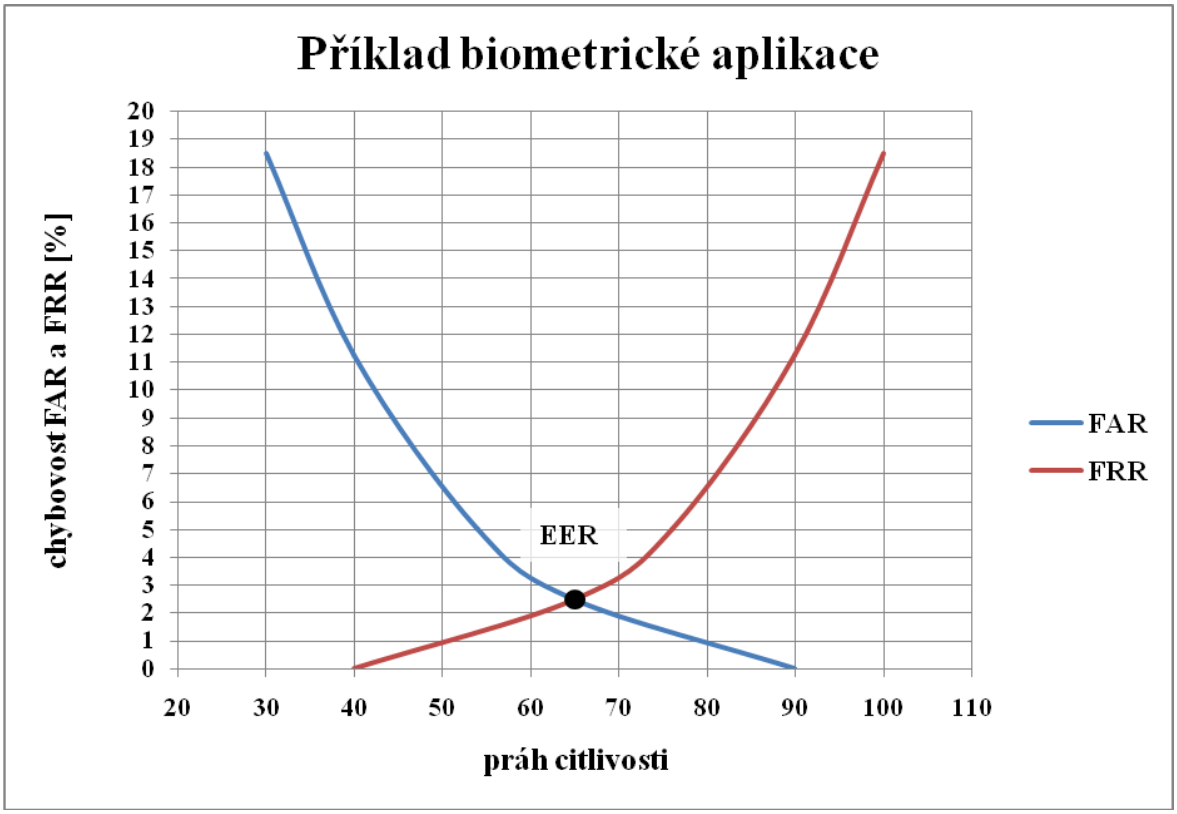
Každá aplikace má nastavený určitý práh citlivosti (tzv. threshold) a o tom, zda je uživatel považován za oprávněného či neoprávněného, rozhoduje tzv. match score. Čím vyšší je nastavená citlivost, tím méně je neoprávněných přístupů (FAR), ale tím více je zamítnutí oprávněných uživatelů (FRR). Proto je velmi obtížné v praxi nastavit tento práh tak, aby bylo FRR co nejvyšší a FAR co nejnižší.

S tímto souvisí match score, které vyjadřuje, z kolika procent se shoduje biometrický vzorek uživatele s referenční šablonou. Například pro kritické objekty se nastaví práh citlivosti na match score 95%, což skoro zamezí neoprávněným přístupům, ale také to způsobí to, že stoupne počet odmítnutí oprávněných uživatelů.

Je na provozovateli systému, jaký práh citlivosti zvolí. Zda dá přednost komfortu uživatelů tím, že bude stačit například ledabyle položit prst na senzor a systém ho ihned vpustí nebo dá přednost bezpečnosti a občas se bude muset někdo pokusit o identifikaci vícekrát či se prokázat jiným způsobem.

Většina výrobců ovšem udává mezní hodnoty faktorů FRR a FAR a pro praktické posouzení je potřeba znát celý průběh křivek těchto hodnot v závislosti na prahu citlivosti. Příklad takové aplikace si můžeme prohlédnout na obrázku, který je níže (Obr. 12.). Z něho odečteme podle hodnoty prahu citlivosti procentuální hodnoty FRR a FAR. Například prahu citlivosti 50 odpovídá FAR = 6,4% a FRR = 0,8%, což znamená, že při tomto nastavení do objektu pronikne 6,4% neoprávněných osob a 0,8% oprávněných osob bude odmítnuto.

Jak jsem již řekl, jde především o účel aplikace a naše priority. Ideální zařízení, v němž jsou obě hodnoty rovny 0, bohužel zatím neexistuje.



Obr. 12. Příklad biometrické aplikace s křivkami FAR a FRR a bodem EER. [1]

2.2.5 Další pojmy

Zde následuje výčet a popis několika dalších pojmů vztahujících se k dané problematice.

Biometrie – soubor vědních poznatků, založených především na statistickém a analytickém přístupu, jejichž předmětem je zkoumání a následné praktické využití měřitelných charakteristik živých organismů s cílem jejich následné jednoznačné identifikace nebo verifikace. Nejčastějším objektem tohoto zkoumání je člověk. [1]

Biometriky – jsou to měřitelné biometrické charakteristiky živého organismu, které se snímají, zpracovávají, vyhodnocují a uchovávají v procesu identifikace nebo verifikace. [1]

Biometrický vzorek – stopa zanechaná na vnějším světě člověkem (otisk prstu, slina atd.).

Biometrické charakteristiky – jakékoliv měřitelné údaje pocházející z biometrického vzorku (různé obrazce, data a jiné).

Biometrické markanty – ty údaje, které jsou důležité pro identifikaci (verifikaci) člověka.

Tab. 1. Běžně používané biometrické metody a jejich běžně extrahované markanty [1]

Biometrická metoda	**Extrahované charakteristické markanty**
Otisky prstů	Umístění a směr charakteristických bodů otisku (rozdvojení papilárních linií, jejich tvar apod.).
Hlas	Frekvence, intonace, trvání jednotlivých hlasových charakteristik.
Tvář	Relativní pozice a tvar nosu, očí, lícních kostí.
Ucho	Velikost, tvar ucha, vzdálenost anatomických bodů vnějšího boltce.
Oční duhovka	Rýhování a proužkování duhovky, geometrické obrazce.
Oční sítnice	Tvar markanty krevního řečiště v sítnici.
Geometrie dlaně a prstů	Délka a šířka kostí a kloubů dlaně a prstů.
Podpis	Rychlost a směr jednotlivých tahů, dynamika, vzhled podpisu.
Dynamika psaní na klávesnici	Pořadí kláves, časové intervaly mezi jednotlivými úhozy.

Biometrická šablona – souhrn minimálního počtu markantů z biometrického vzorku, na jehož základě je provedena identifikace či verifikace člověka.

Equal Error Rate (EER) – bod, kde se FRR rovná FAR, což se v překladu označuje jako míra se shodnou chybou.

Failure to Enroll (FTE) – možnost, že uživatel nebude moci být zaregistrován v biometrickém systému (nevidomí – oči, těžce pracující – otisky prstů aj.).

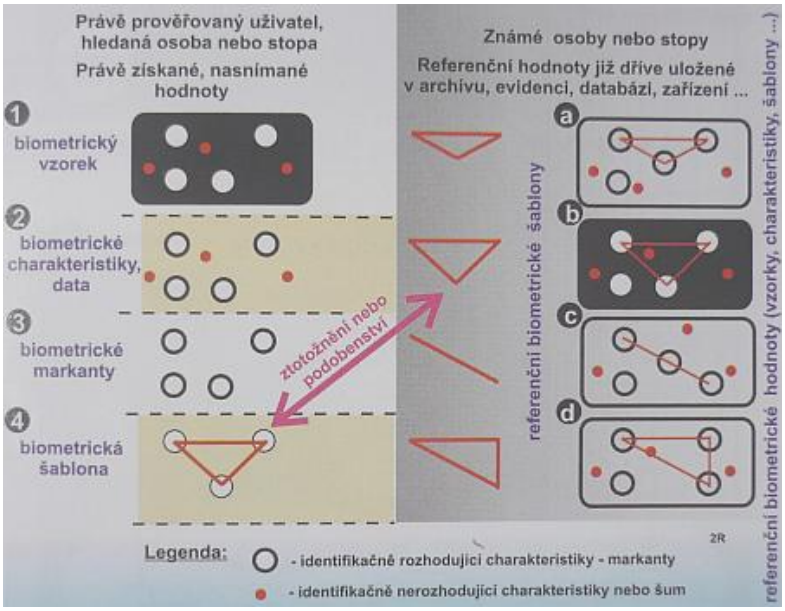
Failure to Acquire (FTA) – situace, kdy získaná biometrická data nejsou dostačující pro další zpracování.

False Match (FM) – situace, kdy dojde k nesprávnému ztotožnění při tom, když se vstupní data porovnávají s biometrickou šablonou.

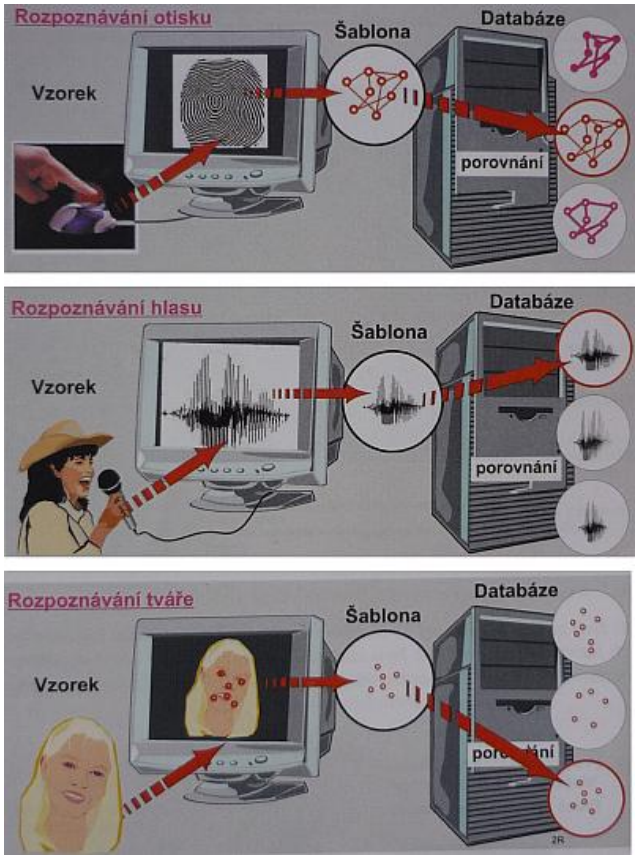
False Non-Match (FNM) – situace, kdy dojde k nesprávnému neztotožnění při tom, když se vstupní data porovnávají s biometrickou šablonou.

Autentizace – synonymum slova verifikace.

Automatizované systémy – systémy provádějící biometrickou identifikaci/verifikaci automatizovaně pomocí výpočetní techniky.



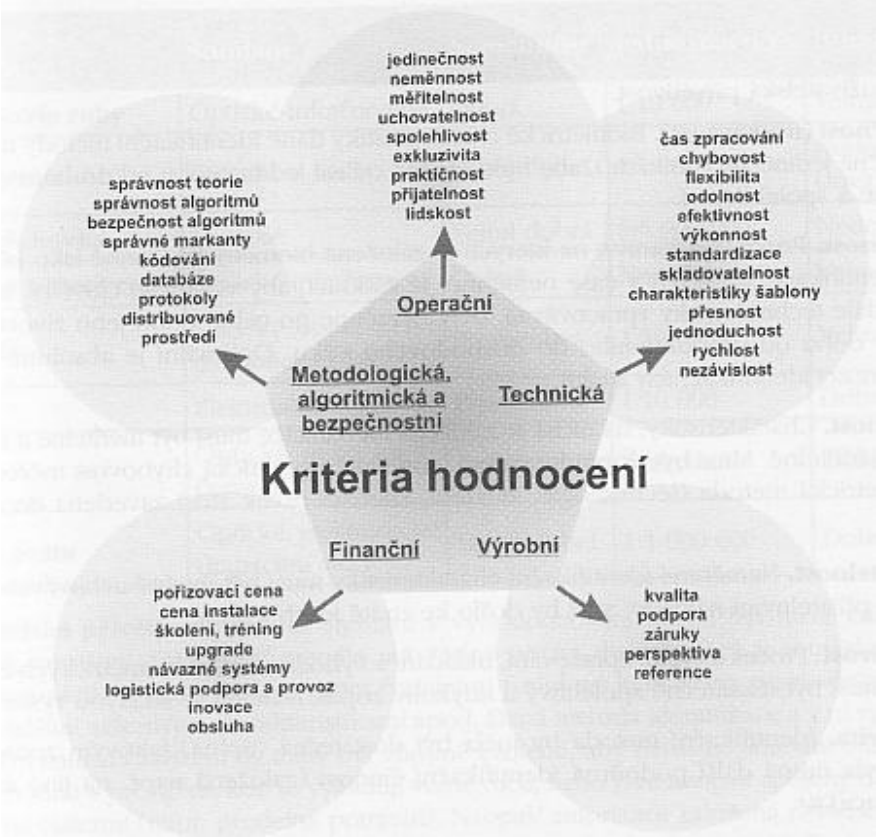
Obr. 13. Základní filozofie porovnávání vzorku uživatele s údaji uloženými v databázi. [1]



Obr. 14. Ukázky porovnávání u 3 biometrických metod. [1]

2.3 Kritéria hodnocení biometrických systémů

Aby bylo možné biometrické technologie vhodně nasadit, musí splňovat určitá kritéria pro splnění funkčních náležitostí. Dělení těchto kritérií je vidět na následujícím obrázku.



Obr. 15. Kritéria hodnocení biometrických technologií. [1]

2.3.1 Operační kritéria

a) jedinečnost – biometrické charakteristiky dané metody musí být jednoznačné, tzn. takové, které umožňují jednoznačnou identifikaci subjektu.

b) neměnnost – biometrické charakteristiky dané metody musí být s časem neměnné, tzn. stálé.

c) měřitelnost – biometrické charakteristiky dané metody musí být měřitelné a dostatečně symbolicky vyjádřitelné.

d) uchovatelnost – naměřené hodnoty lze ukládat bez ztráty kvality.

e) spolehlivost – proces identifikace musí být spolehlivý a kdykoliv opakovatelný.

f) exkluzivita – metoda musí sama stačit na identifikaci (není třeba další metody na její potvrzení).

g) praktičnost – metoda by měla být co nejvíce praktická (jednoduchost použití, rychlost atd.).

h) přijatelnost – proces identifikace by neměl porušovat osobní, společenské, sociální, náboženské, politické či etické požadavky.

i) uživatelská přívětivost – proces identifikace by neměl působit rušivě a měl by být co nejvíce pohodlný pro běžné použití.

2.3.2 Technická kritéria

Jako každé technologické zařízení i to biometrické musí splňovat určité technické požadavky. Důraz je kladen hlavně na rychlost celého procesu identifikace, technologické zpracování a odolnost vůči rušivým vlivům jako je prach, elektromagnetické záření, kouř, vlhkost, teplo apod. Samozřejmě i ostatní předpoklady jsou velice významné. Výčet všech požadavků na technické řešení biometrických zařízení je znázorněn na uvedeném obrázku (Obr. 15.) z knihy autora Raka.

2.3.3 Výrobní kritéria

Neméně podstatným hlediskem jsou výrobní faktory. Posuzujeme nejen jednotlivé položky vypsané výše v obrázku (Obr. 15.), ale i ostatní informace o dodavateli či firmě, která daný systém vyrábí.

2.3.4 Finanční kritéria

Snad nejvíce porovnávaným kritériem mezi biometrickými technologiemi a samozřejmě nejen mezi nimi, je finanční hledisko. Každý zákazník žádá od výrobku co nejvíce, za co nejméně peněz. Nejinak je tomu i zde. Musíme ale posoudit nejenom krátkodobé hledisko, ale i to dlouhodobé. Tzn., kolik jiných finančních prostředků nám instalovaný biometrický systém uchrání. Všechna kritéria související s finanční otázkou jsou vyobrazena v obrázku (Obr. 15.) na začátku kapitoly.

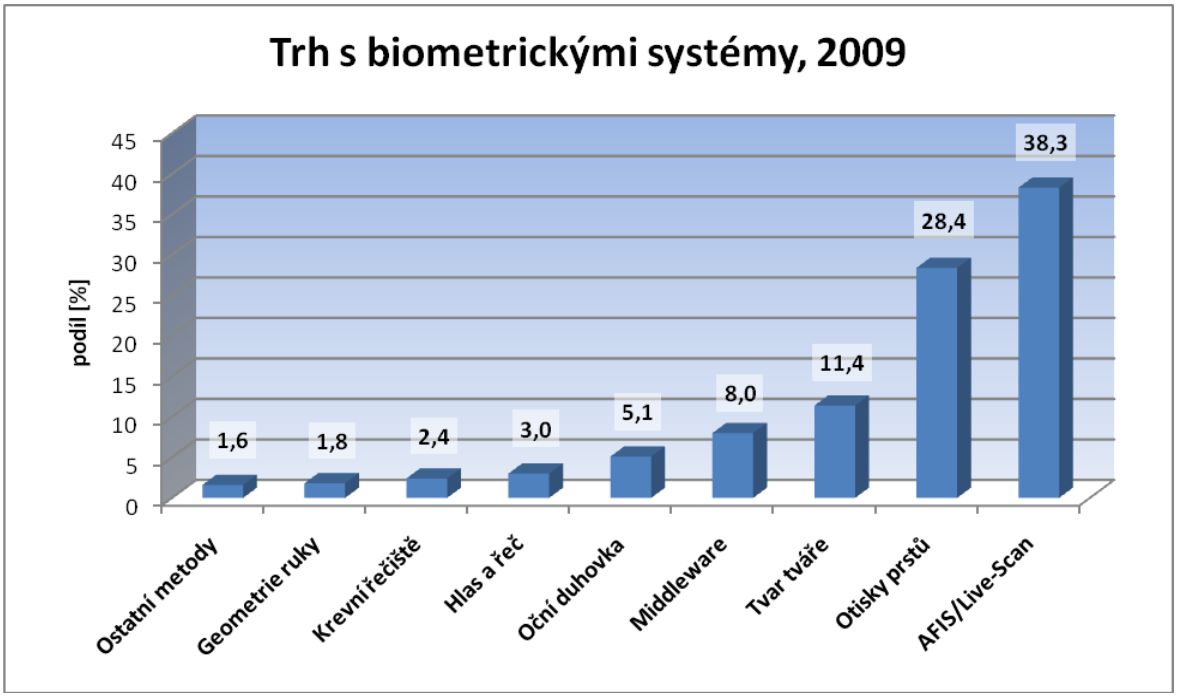
2.3.5 Metodologická, algoritmická a bezpečnostní kritéria

Každá metoda biometrické identifikace využívá různé druhy algoritmů ke svému zabezpečení či fungování a stejně tak tyto algoritmy jsou založeny na odlišných matematických teoriích. Jestliže je špatně teorie, je i algoritmus chybný. Každý algoritmus má svůj stupeň bezpečnosti a obecně lze říci, že pokud je cena za překonání bezpečnostního opatření (algoritmu) větší než cena chráněných dat, je tato technologie bezpečná. Z pohledu bezpečnosti a spolehlivosti mohou být kódující algoritmy buď absolutně bezpečné (v praxi nemožné) nebo bezpečné s vypočítanou mírou rizika.

Biometrické algoritmy z matematického hlediska můžeme rozdělit na statistické metody modelování, dynamické programování a neuronové sítě. Jednotlivá kritéria, která zde patří, jsou jasně zřetelná na již uvedeném obrázku (Obr. 15.).

3 JEDNOTLIVÉ METODY BIOMETRICKÉ IDENTIFIKACE

V této kapitole uvedu přehled a popis jednotlivých druhů biometrické identifikace a jejich možné použití. Také je vložena obrazová dokumentace, která zachytává jednotlivé metody, jak fungují a jak probíhají. Tato část je velmi důležitá pro její informační hodnotu, která dá čtenářům přehled o minulých a hlavně současných používaných biometrických metodách.



Obr. 16. Objem biometrických aplikací na trhu podle jejich druhu, 2009. [49]

3.1 Antropometrická metoda, tzv. bertillonáž

Jedná se o první skutečně vědecké identifikování lidí. Před příchodem této metody byla identifikace spíše vizuálního charakteru, a jelikož gramotnost i evidence byla na velmi malé úrovni, chycená osoba vždy tvrdila, že se ještě nikdy ničeho nedopustila a protože žádné pečlivé záznamy neexistovaly, tak jí toto tvrzení i prošlo. Takovéto jednání trápilo nejednoho policejního vyšetřovatele a tak bylo potřeba nějak tento problém odstranit.

S řešením přišel až francouzský vědec, antropolog a etnolog Alphons Bertillon (24. 4. 1853 – 13. 2. 1914) a protože se jedná o první krok v biometrické identifikaci, popíši v kostce i

život této historicky významné osoby. Narodil se do vzdělané rodiny a touha po vědění jej doprovázela celý život. Již od mládí sledoval výzkum svého otce Dr. Louise Adolpha Bertillona a svého dědy, matematika a přírodopisce Achilla Guillarda, kteří zkoumali výzkum statistika Lamberta Quételeta. Ten tvrdil, že neexistují dva jedinci, kteří by měli shodné míry všech částí těla a končetin.

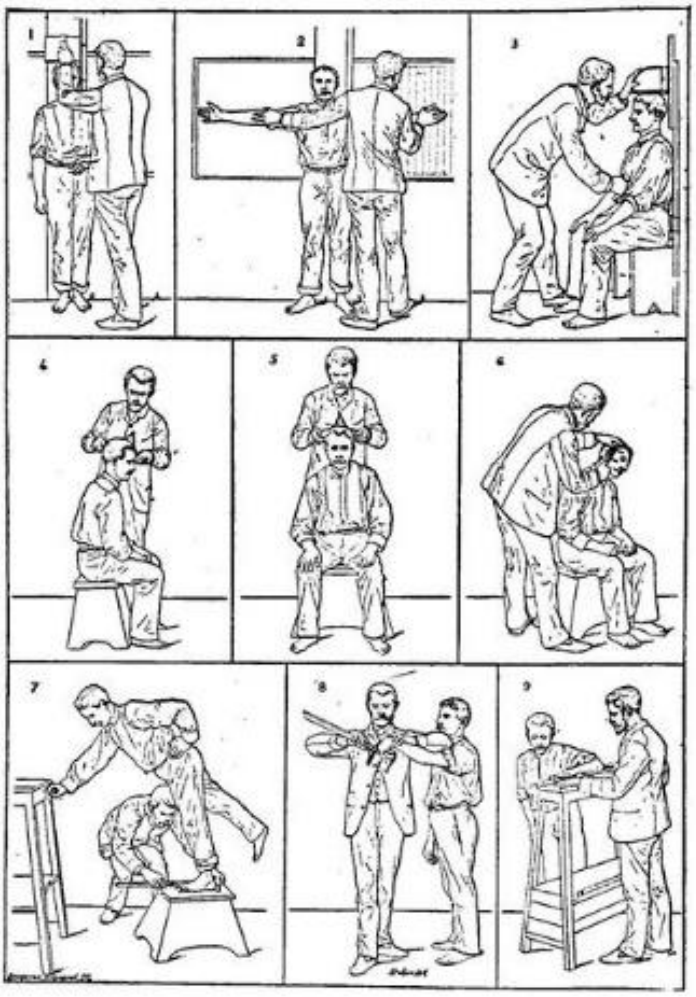
Mladý Alphons začal studovat matematiku a fyziku, ale ze studií brzy odešel a našel si práci v bance. Později, v jeho 25 letech, mu jeho otec sehnal místo pomocného úředníka v archívech v prefektuře policie. Práci měl stereotypní, kdy zapisoval údaje o zatčených zločincích do identifikačních karet.

3.1.1 Podstata metody

Zlom nastal v červenci roku 1879, kdy si při každodenním vyplňování karet uvědomil, že každého člověka lze odlišit od jiného právě mírami různých částí těla. Bylo jasné, že dva či tři údaje mohly mít dvě osoby stejné, ale třeba pět už nikoliv. S tímto tvrzením se mu nejdříve od ostatních dostávalo výsměchu, ale nakonec bylo vyhověno jeho žádosti o jeho vlastní přeměřování zatčených zločinců při jejich registraci. Při té měřil jejich výšku, délku a obvod hlavy, délku paží a prstů nohou.

Celý měsíc shromažďoval údaje a na konci shrnul své výsledky a v písemné zprávě ji odeslal policejnímu prefektovi Paříže. Ten její myšlenku nepochopil a ani o ni neměl zájem. Tak zpráva putovala dál k šéfovi Sűreté[3]. Ten, ač měl lepší znalosti daného tématu, opovrhoval teoriemi a teoretiky vůbec a tak se zprávou dále nezabýval. Posun znamenalo až přečtení výsledků práce Alphonsovým otcem, který geniální myšlenku pochopil a pomohl tuto věc „protlačit“ dále pomocí svých známostí. Nakonec dostal Alphons dva pomocníky a tříměsíční lhůtu na dokázání svých tvrzení. To se mu i podařilo, když 20. 2. 1883 identifikoval pomocí své metody zloděje lahví, který se stejného prohřešku dopustil již v prosinci roku 1882, kdy byl poprvé změřen Bertillonem.

[3] Brigade de Sűreté – první moderní policejní organizace ve Francii

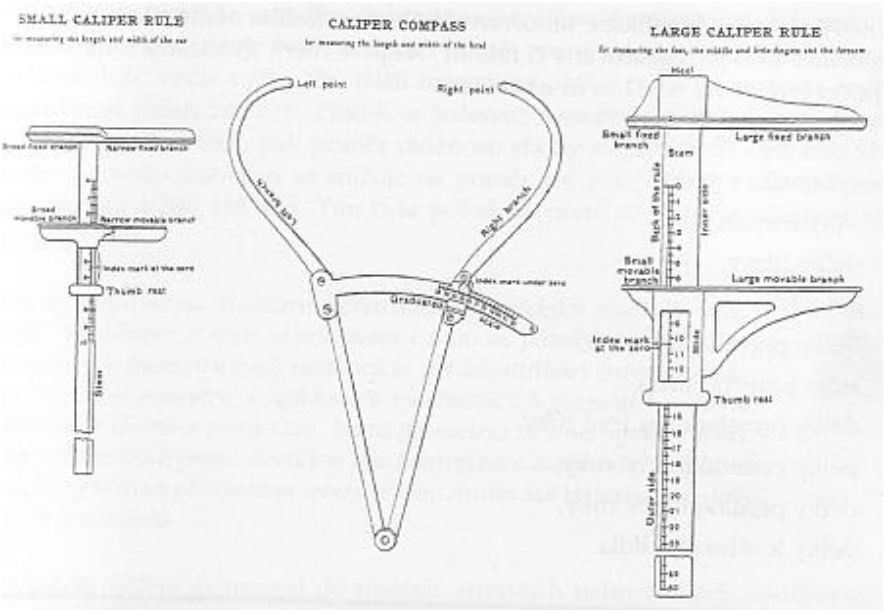


Obr. 17. Ukázka měření Bertillonovou metodou. [23]

K identifikaci podle své metody vytvořil:

- metodický návod k měření jednotlivých části lidského těla,
- speciální záznamovou kartu pro zanášení jednotlivých údajů,
- postup, jak řadit jednotlivé záznamy a rychle vyhledávat v již vytvořených záznamech.

Metodu dále její autor zdokonalil tím, že začal měřit 11 charakteristik lidského těla (pravděpodobnost shody 1:4191304).



Obr. 18. Nástroje, které Bertillon používal ke svým měřením. [1]

Alphons Bertillon svá měření rozlišoval do malých, středních a velkých podskupin a v důsledku toho mohla být každá osoba zařazena do jedné z 243 kategorií. Následným členěním podle barvy očí a vlasů vzniklo neuvěřitelných 1701 skupin.

Obr. 19. Bertilloneho identifikační karta i s vyplněnými údaji. [24]

I když Bertilloneho metoda slavila úspěch nejen v Evropě, ale i v zámoří, používala se pouze zhruba 25 let, podle lokality. Měla totiž několik negativ, např. se nedala dostatečně použít k identifikaci mladistvých. Druhým a zároveň podstatnějším faktorem, který ji odsunul do pozadí, bylo náročné a zdlouhavé získávání biometrických údajů v porovnání s rychle nastupující daktyloskopií, tedy identifikací podle otisků prstů.

3.2 Daktyloskopie

Jak jsem již na začátku práce uvedl, otisky prstů se používaly již dávno v historii lidstva, ale opravdovou vědou se stala daktyloskopie až v 17. století n. l. Jako první si nepravidelných tvarů na prstech všiml italský profesor anatomie Marcello Malpigni. Další poznatky přinesl v 18. století český lékař Jan Evangelista Purkyně, který rozlišil 9 základních daktyloskopických vzorů. Následovali další jako Angličani W. J. Herschel a H. Faulds, kteří dále rozpracovali teorii otisků. Koncem 19. století na základě předešlých výsledků sepsal další Angličan F. Galton práci „Fingerprints“, kde blíže rozšířil vědomosti o otiscích prstů.

Na základě všech zjištěných a dokázaných skutečností se v Anglii v roce 1894 mimo antropometrických údajů začaly do identifikačních karet zanášet i otisky prstů. To samé se stalo za podpory E. R. Henryho v Kalkatě. Nezávisle na Galtonovi přišel na podobné závěry Argentinec J. Vucetich, který jako první i usvědčil vraha za pomoci daktyloskopie a to bylo v roce 1892. Postupně, díky svým pozitivům (rychlé a snadné pořízení, vyhledání a méně náročná evidence) zcela nahradila identifikace podle otisků prstů Bertilloneho metodu a to doslova všude.

S vývojem výpočetní techniky a s rostoucím počtem daktyloskopických záznamů (karet) se dospělo k názoru, že bude lepší papírovou evidenci nahradit digitální. Jako první se zrodil tzv. AFIS v USA v 80. letech 20. století. Souběžně se tam používala i klasická papírová evidence, ale s příchodem nového milénia přešla pouze do digitální podoby v generačně novém počítačovém systému IAFIS (Integrated Automated Fingerprint Identification Systems). V České republice (ČR) se počítačově zpracovávají otisky od roku 1994 a systém se nazývá AFIS 2000 od americké firmy Printrak, který v současné sestavě pojme na 800 000 daktyloskopických karet (záznamů). Momentálně je kapacita systému více jak

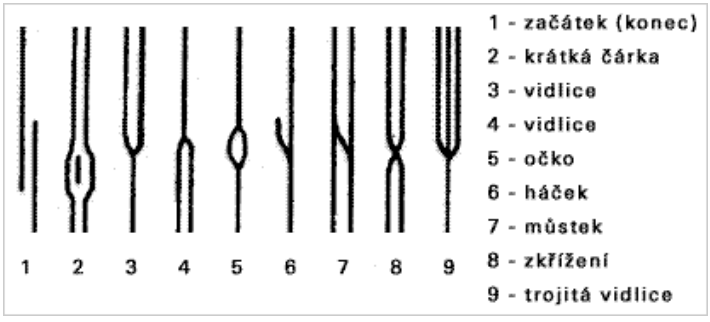
z půlky zaplněna. Centrála je v Kriminalistickém ústavu Praha a na tu jsou napojena jednotlivá pracoviště Odborů kriminalisticko-technických expertíz (OKTE).

Všeobecný rozvoj výpočetní techniky, vývoj skenerů pro přenášení daktyloskopických karet do PC a vývoj nových aplikací společně s nízkou cenou koncem 90. let určily daktyloskopii identifikací pro běžné použití jak v policejně-soudní, tak i v bezpečnostně-komerční sféře.

3.2.1 Podstata metody

Daktyloskopie vychází z toho, že člověk má na vnitřní straně prstů a dlaní a na chodidlech určité typické rýhování, tzv. papilární linie, které se u člověka začínají formovat již od 4. měsíce embryonálního vývoje a během prvního roku života člověka jsou již zformovány. Papilární linie vytváří specifické obrazce, podle nichž je možné ztotožnění člověka. Obrazce brané v potaz při identifikaci v České republice jsou linie, začátek a konec linie, můstek, křížení, háček, zdvojení, dvojitá a trojitá vidlice, posunutí, očko, tečka a ostrůvek s čárkou. Každý tvar má specifickou identifikační hodnotu podle toho, jak často se vyskytuje. Důležitým faktorem je i to, že papilární linie se vyskytují pouze u člověka a ne u zvířat či jinde. Papilární linie souvisí s hmatovou a úchopovou funkcí lidských končetin a jako taková vychází daktyloskopie z těchto tří základních zákonitostí:

- na světě nejsou dva jedinci se shodnými obrazci papilárních linií,
- obrazce papilárních linií zůstávají po celý život člověka relativně neměnné,
- papilární linie jsou relativně neodstranitelné (pokud se neodstraní i zárodečná vrstva kůže).



Obr. 20. Některé ze základních markantů používaných k daktyloskopické identifikaci. [25]

V policejně-soudní praxi se rozlišují tři základní typy otisků (*plastický* – obrazec vytvořen v plastické hmotě; *odvrstvený* – částečky podkladu ulpí na papilárních liniích; *navrstvený* – látky na papilárních liniích se otisknou na podklad, většinou se jedná o pot, který je složen z vody, solí, tuků a bílkovin, voda se odpaří a ostatní látky utvoří otisk). Někdy mohou být otisky skryté, okem neviditelné a proto se podle podkladu používají metody a látky na jejich zviditelnění. Kriminalistika pak rozlišuje otisky na tři druhy podle počtu charakteristických vzorů, tzv. markantů na *upotřebitelné pro identifikaci* (10 a více), *částečně upotřebitelné* (7-9) a *neupotřebitelné* (méně jak 7). Na životnost daktyloskopických stop mají vliv různé faktory jako je vlhkost, prašnost, teplota, déšť, mráz, vítr, světlo atd., ale i vlastnosti nosiče stop, který by měl být ideálně hladký, suchý, nesavý, nezaprášený a neměl by být vystavován venkovním vlivům.

Obr. 21. Znázornění některých markantů v otisku prstu. [26]

3.2.2 Bezpečnostně-komerční aplikace

Pro účely systémů, které jsou založeny na výpočetní technice, jsou typické tři kroky a to:

1. snímání otisku prstu – provádí se pomocí live skenerů, které snímají otisky s použitím senzorů, které dělíme na kontaktní (optické, elektronické, opto-elektronické, kapacitní, tlakové, teplotní) a bezkontaktní (optické, ultrazvukové). Obecně vzato jsou bezkontaktní lepší, protože nedochází ke kontaktu se snímací plochou, která může být špinavá či jinak poškozená a tím znehodnotit výsledek snímání. Z hlediska kvality se zdá jako výborná metoda ultrazvuková, která je velice přesná, má vysoký kontrast a výsledný obraz je trojrozměrný (3D). Tzn., že zabraňuje použití zfalšovaného či přeneseného otisku jiné osoby, který bývá většinou pouze dvojrozměrný (2D). Ovšem nasazení té či oné technologie závisí na tom, kde a na co daný biometrický systém chceme používat. Jak rychle a které senzory nasadit záleží zejména na ceně zařízení, velikosti aplikace a také na rozlišovací schopnosti senzoru.

2. počítačové zpracování otisku – sejmutý otisk se před zpracováním digitalizuje a následně komprimuje do souboru Wavelet Scaler Quantization (WSQ), který má vynikající komprimační schopnosti při minimální ztrátě komprimovaných dat. Také je rychlý, na rozdíl od klasického souboru typu Joint Photographic Experts Group (JPEG). Dalším krokem je předzpracování získaného obrazu, kdy se kontrastní metodou zvýrazní papilární linie a poté se odstraní nežádoucí vlivy, např. šum, jizvy, znečištění atd. Dále se pomocí extrakčních algoritmů vyhledávají jednotlivé markanty v otisku (uloží se jejich typ; x, y souřadnice; směr) a jejich následným spojeným pak vzniká šablona (ukládá se do databáze), která se používá v automatizovaných systémech k porovnávání otisků. Její velikost je v řádech stovek bytů.

3. závěrečné vyhodnocení – jde o porovnání šablony otisku uloženého v databázi a šablony právě sejmutého otisku uživatele. Výsledkem je podle hodnoty match score (míry ztotožnění) buď to, že se otisky shodují (přístup povolen) nebo ne (přístup zamítnut).

V současné době se biometrické identifikační systémy založené na otisku prstu používají zejména pro přístup do chráněných objektů, ke zvýšení ochrany platebních, identifikačních a jiných karet, pro přístup k různým informacím a zařízením (PC, mobilní telefon, notebook atd.) či k ochraně před zneužitím důležitých a nebezpečných technologií (např. zbraně).

Obr. 22. Vybraná zařízení používající jako ochranu otisk prstu. Zleva doprava je čtečka pro přístup do PC, pistole, čtečka pro přístup do objektu, mobilní telefon, zbraňové pouzdro. [27] [28] [29] [30] [31]

3.3 DNA

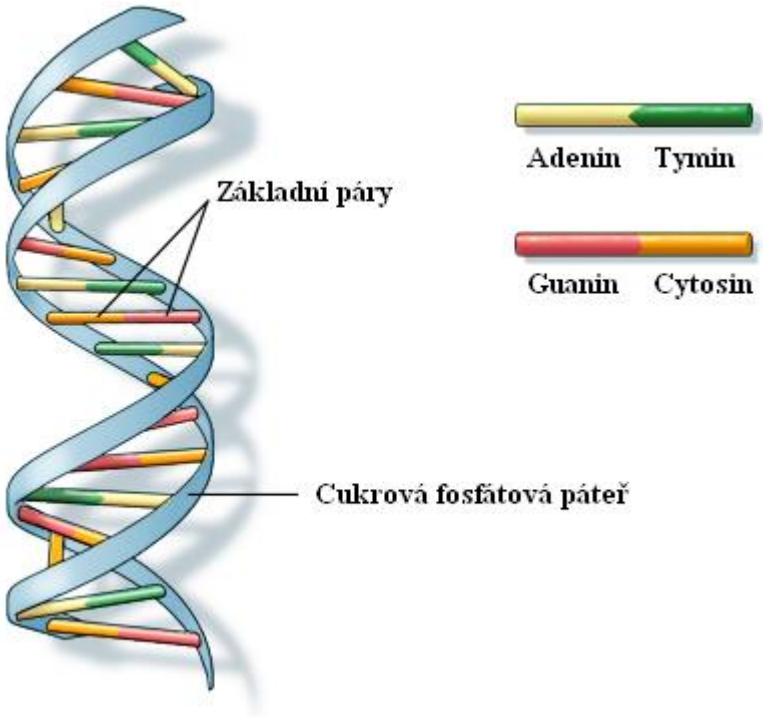
Z identifikačního pohledu se jedná se o celkem mladou metodu, jejíž počátky sahají do 80. let 20. století. Jako první však strukturu DNA (dvojitou šroubovici či točité schodiště) objevili vědci Američan James D. Watson a Brit Francis Crick, kteří položili základ výzkumu DNA. Průkopníkem v identifikaci pomocí DNA byl anglický genetik Alec Jeffreys, který v roce 1985 jako první popsal možnost této identifikace. Jeho metoda byla o rok později použita v případě znásilnění a vraždy a po hromadném testování několika tisíc mužů byl nalezen pachatel a tak se identifikace podle DNA proslavila.

Dalším přínosem byl objev polymerové řetězové reakce americkým chemikem Karym Mullisem v roce 1986, díky němuž bylo možné analyzovat i minoritní množství sporného materiálu.

V 90. letech minulého století vznikají díky rozvoji výpočetní techniky rozsáhlé databáze profilů DNA národního charakteru. První byla britská, kterou vytvořily dvě tamější státní organizace (Association of Chief Police Officers, The Forensic Science Service).

V následujících letech vzniká v USA databázový systém CODIS, který je po splnění podmínek nabízen zdarma i ostatním státům, zejména kvůli snadné kompatibilitě předávaných dat a získání dalších partnerů. V současnosti ho používá několik desítek států včetně ČR (červen 2002). V současnosti je v databázi naší republiky přes 40 000 genetických profilů, z nichž 2/3 patří osobám obviněným a odsouzeným a 1/3 patří neztotožněným stopám z míst činu. Existují i jiné systémy, které využívá např. již zmíněná VB nebo Německo či Rakousko.

Díky obrovským možnostem, co lze z DNA zjistit, roste počet jak státních, tak zejména soukromých subjektů, které se zkoumáním DNA zabývají. S tímto zájmem rostou i poznatky a díky převratnému rozvoji výpočetní techniky se očekávají další významné objevy na poli DNA.



Obr. 23. Složení dvojité šroubovice DNA. [32]

3.3.1 Podstata metody

DNA je jednou ze dvou informačních biopolymerů, které se nachází v 99% organizmů. Soubor informací nesených DNA nazýváme genom a tyto informace jsou stejné pro všechny tkáně a také jsou relativně stálé v čase. Druhým typem jsou bílkoviny (proteiny), ale ty jsou odlišné pro různé tkáně a mění se v závislosti na čase. Soubor informací nesených bílkovinami nazýváme proteom. Z těchto důvodů je pro identifikaci vhodnější DNA.

DNA si můžeme představit jako lineární nerozvětvený řetězec, tvořený střídáním 4 prvků (nukleotidů) – A (adenin), C (cytosin), G (guanin) a T (tymin). 99% DNA je uloženo v jádře buňky (tzv. jaderná DNA) a zbytek se v podobě malé kruhové molekuly (tzv. mitochondriální DNA) nachází mimo jádro. DNA se skládá z kódujících úseků tedy genů (10%, nesou informace o stavbě člověka) a nekódujících úseků (90%, žádná známá funkce pro vývoj člověka). Pro identifikační účely se využívají prozatím pouze nekódující úseky, především z etického hlediska. Prozatím proto, že v současnosti se intenzivně zkoumá i to, jak z kódujících úseků zjistit např. barvu očí či vlasů a jiné fyzické informace důležité k identifikaci jedince. Jestliže se toto podaří, bude to znamenat další revoluci v oblasti DNA identifikace.

Můžeme konstatovat, že genetická informace, kterou každý člověk nese, je kompletní v okamžiku oplodnění ženského vajíčka mužskými spermiemi, pokud tedy nedojde k její mutaci, která může mít malé i velké důsledky pro celý nově se utvářející organizmus.

Celý proces DNA identifikace lze rozdělit do několika kroků. Prvotním je sběr vzorků. DNA je obsažena ve všech tkáních člověka (krev, svaly, kosti, sperma atd.), v menší míře i ve slinách, vlasech a chlupech. Červené krvinky jako jediný objekt v lidském těle DNA neobsahují. Stopy uvedených tekutin a tkání se hledají na místě činu. Od osoby se dnes většinou odebírá vzorek DNA pomocí tyčinky s vatičkou a to z vnitřní strany tváře. Jednoduché, neinvazivní, neintimní, to je výhoda tohoto způsobu.

Dalším krokem je izolace čisté DNA, tzn. vzorek očištěný od nežádoucích látek jako bílkoviny, některé ionty atd. Existuje několik metod biochemických či fyzikálně chemických, z nichž na konci vždy vzejde tzv. izolát.

Následuje kvantifikace DNA, která se provádí v případech, kdy je nutno určit množství DNA v izolátu. Záměr je určit, kterou vhodnou metodu analýzy DNA použít.

Posledním krokem je analýza DNA sekvence. Ta se v dnešní době provádí nejvíce pomocí metody STR-typing, tzn. analýzou krátkých tandemových repetic. Po všech krocích je vytvořen genetický profil, který je uložen do databáze.

3.3.2 Bezpečnostně-komerční aplikace

Využití DNA v aplikacích bezpečnostního charakteru je v současnosti prakticky nemožné. Problémem je to, že i přes velice výkonnou výpočetní techniku a vyspělý software nelze spolehlivě provést rozbor a následnou identifikaci/verifikaci uživatele dostatečně rychle. Vždy je to otázka několika hodin.

Avšak dá se předpokládat, že další rychlý vývoj v této oblasti umožní v budoucnosti identifikační DNA zařízení nasadit i v bezpečnostně-komerčních aplikacích. Dá se však očekávat, že cena těchto zařízení bude příliš vysoká ve srovnání s jinými biometrickými metodami.

Dalším problémem může být to, že uživatelé budou tuto technologii bojkotovat, protože v budoucnu se dá očekávat, že z jedné jediné buňky DNA budeme moct vyextrahovat kompletní biologické informace o konkrétní osobě (zdravotní stav, fyzický vzhled, genetické predispozice atd.). V souvislosti s klonováním bude snaha ochránit svou DNA ještě větší. Ale to již předbíhám.

DNA se využívá spíše v policejní praxi a to k přímé identifikaci osoby, zjišťování příbuzenských vztahů (bratranci, otec a dcera atd.) a k identifikaci mrtvol.

Další použití může být v civilním životě: určování otcovství a rodičovství, kontrola DNA sportovců při dopingových testech či archeologické výzkumy.

Obr. 24. Práce kriminalistického technika v laboratoři při analýze DNA. [33]

3.4 Oční duhovka

Duhovka se u člověka začíná vyvíjet už ve třetím měsíci těhotenství a z velké části jsou všechny její vzory vytvořeny již v osmém měsíci těhotenství. V dalších letech po narození ještě může probíhat usazování pigmentu v duhovce.

Identifikační metoda podle oční duhovky je záležitostí zejména posledních 10 let. Na myšlenku, že každý člověk má jinou oční duhovku přišel sice již v roce 1936 americký oční chirurg Frank Burch, ale až s příchodem výpočetní techniky se tohoto podařilo využít v praxi. Převratem byly algoritmy britského profesora Johna Daugmana, které sloužily a stále slouží ke kódování a rozpoznávání různých vzorů duhovek.

Duhovku má každý člověk jedinečnou. I podle matematických výpočtů je prakticky nemožné, aby dva lidé měli stejné oční duhovky. Ta je jiná taktéž v každém oku člověka a různá je i u jednovaječných dvojčat, v porovnání například s DNA. To potvrzují i zprávy z praktického použití, kdy bylo zaznamenáno přes 9 milionů skenů očních duhovek držiteli licence těchto algoritmů v USA, Velké Británii, Japonsku a Koreji a žádné dvě duhovky nebyly identické.

Obr. 25. Oční duhovka a zornice. [34]

3.4.1 Podstata metody

Oční duhovka obsahuje různé charakteristické vzory a body, podle nichž je možné ji odlišit od jiné. Mohou to být různé rýhy, hřebeny, klikaté čáry, korány atd. Oko duhovky je nasnímáno infračervenou monochromatickou CCD[4] kamerou ze vzdálenosti zhruba jeden metr. Poté je v zachyceném obraze pomocí lokalizačních algoritmů vyhledána duhovka a následně je zaznamenáno rozmístění pigmentu a charakteristických tvarů v duhovce. Výhodou je, že duhovka má kulatý tvar a tak je vyhledání jednodušší než třeba u rozpoznání tváře. Pokud je duhovka na obraze viditelná méně jak z 50%, považuje se obraz za nepřijatelný. Následně je vzor duhovky demodulován (abychom získali jeho fázovou informaci) pomocí 2D Gaborových waveletů, které se používají pro svou optimálnost a komplexnost. Pro porovnávání duhovek se používají pouze fázové informace, protože

[4] CCD – Charge Coupled Device

amplitudová složka není příliš diskriminativní. Dalším jejím negativem je to, že závisí na vnějších faktorech (osvětlení, kontrast či typ kamery).

3.4.2 Bezpečnostně-komerční aplikace

Rychlost rozpoznávání je v současnosti na vysoké úrovni. Pro představu například RISC[5] procesor pracující na frekvenci 3GHz vykoná 1 000 000 porovnání za sekundu, což činí tuto metodu velice účinnou a vhodnou pro databáze velkého rozsahu. Lze také databázi prohledávat paralelně a to tak, že celou databázi rozdělíme na několik menších a ty systém prohledává najednou. Také můžeme využít místo jednoho výkonného procesoru několik spojených PC s nižšími takty, což ještě sníží naše výdaje. To, že je tato metoda takto rychlá navíc znamená, že můžeme práh citlivosti nastavit tak, abychom dosáhli nulové míry neoprávněného přijmutí a tím ani nijak zásadně nesnížíme výkonnost celého systému. Další výhodou je bezkontaktní způsob identifikace, což je uživatelsky velice přívětivé. Použití je možné jak pro identifikaci, tak pro verifikaci.

Systém může být náchylný na oklamání pomocí fotografie a tak je vhodné pro stoprocentní výsledek, aby u procesu skenování byla přítomna i nějaká fyzická ostraha, která toto hlídá, popř. snímání prostoru kamerovým systémem. Na tomto nedostatku se v současnosti ve světových laboratořích usilovně pracuje.

Využití je momentálně různé, ale vesměs podobné jako u ostatních metod biometrické identifikace. Zejména se této metody využívá na letištích pro odbavování odlétajících pasažérů, imigrační kontrolu přilétajících osob, vstup pilotů, letušek a jiného personálu do vyhrazených prostor a ke kontrole přilétajících osob, zda nejsou v seznamu dříve vyhoštěných osob.

Jedna z největších aplikací (cca 500 000 osob) je provozována Komisí pro uprchlíky Organizace spojených národů (UNHCR), která identifikaci podle duhovky využívá k rozdělování humanitární pomoci afghánským uprchlíkům v Pákistánu.

---

[5] RISC – Reduced Instruction Set Computer (procesor s redukovanou instrukční sadou)

Asi největší aplikace tohoto druhu funguje ve Spojených arabských emirátech. Na všech vstupech do země je každá osoba podrobena skenu oka, zda není v seznamu již vyhoštěných osob. Databáze obsahuje přes půl milionu vzorků a čas, který potřebuje systém k jejímu prohledání je 1 sekunda. Celkem posuzovanému člověku zabere procedura 2 sekundy. Každý den je uskutečněno přes 3,5 miliardy porovnání.

Další využití může být pro přístup do důležitých objektů, jako jsou jaderné elektrárny, nukleární sila, banky, trezory, přístup do informačních systémů (IS) apod. I ve věznicích se začíná tato metoda uplatňovat, protože vězni nejčastěji utíkají z vězení převlečení za návštěvu či zaměstnance a tímto je jim útěk znemožněn. Tento systém je také zaváděn například v Japonsku a těší se tam velké oblibě. Při příchodu do nájemního domu je osoba skenována a systém posuzuje, zda dotyčný v domě bydlí. Pokud ano, je mu vstup dovolen a dokonce je mu přivolán automaticky výtah a je vyvezen do patra, kde má osoba byt.

Obr. 26. Ukázka dvou biometrických snímačů oční duhovky na trhu. Vlevo Panasonic BM-ET200 a vpravo OKI IrisPass-M. [35] [36]

3.5 Oční sítnice

Počátky vědomostí o obrazu cév v oku můžeme datovat do roku 1935, kdy dva oční lékaři Isidore Goldstein a Carleton Simon přišli při výzkumu očních vad na to, že každé oko má zcela jedinečný obraz očních cév. Další výzkum přišel s Paulem Torerem v 50. letech,

který studoval oči jednovaječných dvojčat. Jeho předpoklad, že dvojčata budou mít stejné rozmístění cév v oku, byl chybný. Následoval další rozvoj poznatků o oku a jeho sítnici a cévách.

První plán zařízení, které mohlo snímat sítnici a identifikovat tak člověka byl k dispozici v roce 1975. V roce 1976 založil Robert Hill firmu EyeDentify (ED), která téma identifikace podle oční sítnice dále rozpracovala. Zpočátku vycházel přístroj z přístrojů očních lékařů, ale tyto byly velice drahé a těžké na obsluhu. Ke snímání se používalo viditelné světlo, které ale bylo v procesu získání obrazu nepříjemné uživateli a tak se začalo používat světlo infračervené (IR). První skutečně automatizovaný systém se podařilo vyrobit v roce 1981. První sériově vyráběný systém jménem EyeDentification System 7.5 se dostal na trh v roce 1985. Posledním systémem od fy ED byl ICAM 2001 (rok 2001), který byl ale stažen z prodeje pro svou vysokou cenu a hlavně uživatelskou nepřívětivost.

Současnými významnými hráči na trhu s těmito systémy jsou firmy EyeKey a Retica Systems, která má patentovanou biometrickou technologii založenou na kombinaci rozpoznání oční sítnice i duhovky.

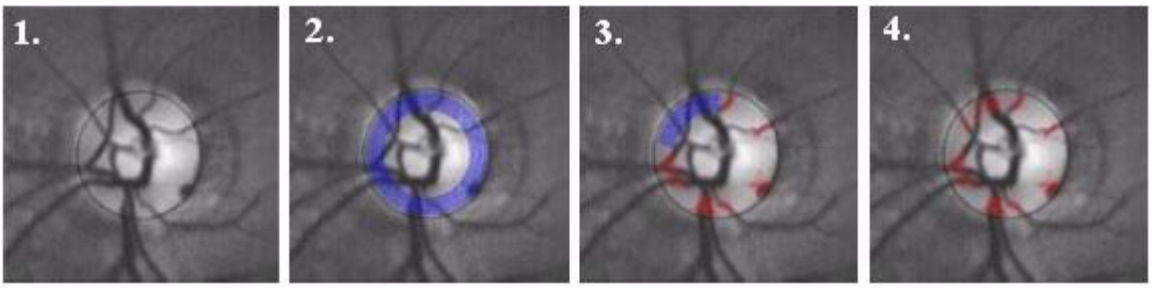
3.5.1 Podstata metody

V průběhu 20. století přišlo několik lékařů a jiných vědců nezávisle na sobě, že vyživující cévy na zadní stěně oční sítnice vytváří u každého člověka relativně stálé a jedinečné obrazce.

Tyto se nejdříve snímaly pomocí viditelného světla, ale později se přešlo na IR světlo. Proces probíhá tak, že uživatel se ze vzdálenosti několika centimetrů dívá do kamery, v níž je znázorněno několik bodů v různých optických vzdálenostech tak, aby byly úspěšně sejmuty i osoby krátkozraké a dalekozraké. Osoba musí sundat brýle, ale kontaktní čočky nevadí. Obraz se pak čistí pomocí filtru, aby se odstranil šum, odraz a zvýraznil se kontrast.

Referenční snímek se skládá z několika snímků sítnice, které se mezi sebou porovnávají pro ověření, zda může být daná osoba zanesena do systému. Pokud je shodnost snímků vyšší jak cca 0,8, je osoba schválena a referenční vzorek je zanesen do databáze. Míru otočení koriguje rotační algoritmus.

Pro porovnávání se používá pouze mezikruží tak, jak je znázorněno na následujícím obrázku (Obr. 27.).



Obr. 27. Proces sejmutí obrazu oční sítnice: ***1.*** *Extrakce a zaostření části sítnice;* ***2.*** *Sken mezikruží;* ***3.*** *Lokalizace cév v mezikruží;* ***4.*** *Vytváření kruhové šablony. [11]*

3.5.2 Bezpečnostně-komerční aplikace

Použití této metody identifikace/verifikace je podobné jako u metody používající jako identifikační prvek oční duhovku. Díky svým nevýhodám je nasazena pouze tam, kde je bezpečnost na prvním místě a uživatelská přívětivost až na druhém. Jedná se o vládní laboratoře, jaderná sila, důležité světové komunikační body atd.

K již zmíněným nevýhodám patří zatím drahé snímací zařízení, nedůvěra uživatelů (nebezpečné snímací světlo), uživatelská nepřívětivost (délka skenu, pozice při skenu, sundávání brýlí atd.) či nemožnost použití ve venkovním prostředí kvůli množství okolního světla.

Metoda má i výhody. Jsou to zejména rychlost a vysoká přesnost identifikace/verifikace. Přes všechny své vlastnosti je biometrický systém založený na oční sítnici považován za jeden z nejbezpečnějších.

Obr. 28. Zleva doprava vidíme: EyeDentification System 7.5 (1985), EyeDentify ICAM 2001 (2001), systém fy Retica Systems, Inc. (2004) [11] [37]

3.6 Tvar tváře

Identifikace podle tváře je každému z nás velice blízká, protože je to základní věc, podle které rozeznáváme ostatní lidi kolem nás. Lidský mozek si pamatuje obrazy nám známých lidí a v případě setkání se s někým hned hledá obraz, který zná a podle toho vyhodnotí, zda danou osobu známe. Jedná se o složité procesy, které ani zdaleka nejsou zatím objasněny.

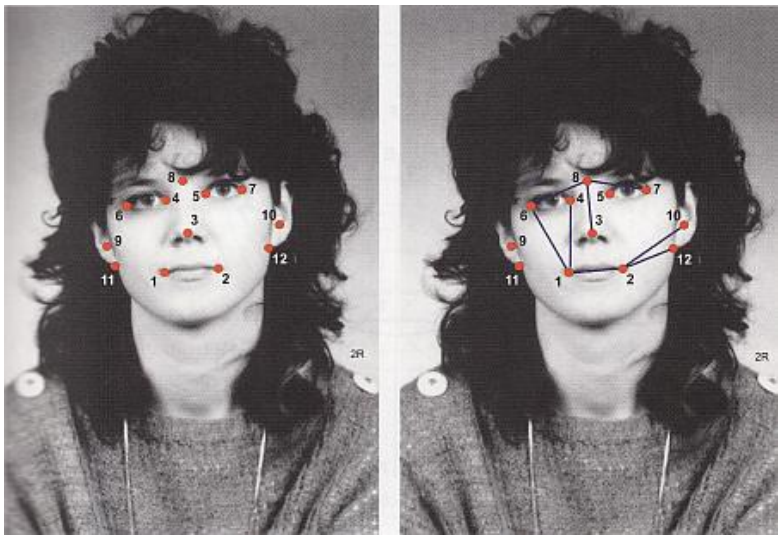
Pro identifikační účely se začala tvář studovat až během 20. a 21. století a to bezpečnostními složkami, které popis tváře využívaly pro celkový popis zájmových lidí (pohřešovaných, pachatelů atd.). Tento popis musí vždy dělat kriminalistický technik, který přesně zná danou metodu jak tento popis (obraz) tváře osoby zhotovit. Při tvorbě požadovaného obličeje bere v potaz ***tvář jako takovou*** (tvar, plnost, barvu, vrásky, různé důlky, jizvy a jiná zranění či vady), ***vlasy*** (tvar, hojnost, barvu, účes a střih, další zvláštnosti), ***vousy*** (barvu, tvar, hustotu, střih, jakost), ***obočí*** (hustotu, tvar), ***oči*** (tvar, vzdálenost očí, tvar horních víček) a dále popisuje ***čelo***, ***uši***, ***bradu***, ***nos***, ***rty*** či ***zuby*** (barvu, velikost, průběh, tvar, polohu atd.). Jednotlivé popisky realizuje buď subjektivně anebo za pomoci vzorníků. Metod tvorby obrazu tváře bylo a je stále několik. V dnešní době se ale s výhodou používá tvorba na PC, která nevyžaduje velké zkušenosti obsluhy a je velice jednoduchá. Jednotlivé části tváře se vybírají z již vyobrazených příkladů a sestavení tváře tak nezabere více jak hodinu. V ČR se používají dva programy a to domácí PORIDOS –

PORtrétní IDentifikace OSob (PC s OS Windows) a německý FACETTE (pro počítače Apple Macintosh).

3.6.1 Podstata metody

V závislosti na faktech, které byly zjištěny o tváři, se analyzovala možnost, jak porovnat dva fotografické snímky osob pomocí výpočetní techniky. Nakonec se vyvinulo několik metod, z nichž nejrozvinutější byly v 60. a 70. letech 20. století tyto dvě:

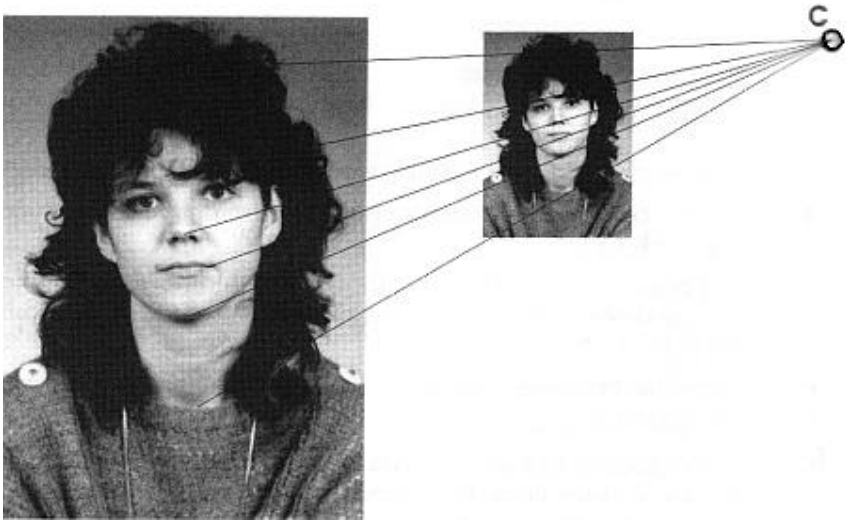
a) **metoda analyticko-statistická** – bylo dokázáno, že pro ztotožnění stačí ve tváři určit 12 markant, které se každá s každou spojí a výsledný obrazec se porovnává s jinými. Pokud je tvář pokaždé sejmuta z jiného úhlu či pozice, musí se použít ještě prostorová transformace, která výsledný obrazec otočí dle potřeby.



Obr. 29. Ukázka analyticko-statistické metody. Pro zjednodušení jsou spojeny jen některé markanty. [1]

Na obrázku (Obr. 29.) výše je vidět 12 bodů, které jsou pro srovnání nejdůležitější. Jedná se o koutky úst (1, 2), špičku nosu (3), vnitřní a vnější koutky očí (4, 5, 6, 7), místo, kde nos přechází v čelo (8), místa na chrupavce ucha chránící vnější sluchovod (9, 10) a místa, kde ušní lalůčky přechází do tváře (11, 12).

b) metoda grafická – jedná se o to, že určité body (markanty) každého snímku jsou shodné s body na jiném snímku, který je určitým způsobem zmenšen, zvětšen, popř. pootočen.



Obr. 30. Ukázka grafické metody. [1]

Obrázek (Obr. 30.) jasně ukazuje, že přímky spojující jednotlivé identifikačně významné body se protínají v jednom bodě (C). Tzn., že osoby jsou totožné. Pokud by jenom jedna přímka neprotínala tento bod, bude výsledkem neztotožnění obou osob.

Největším problémem je strojově tvář vyhledat. Samozřejmě v situacích, kde osoba prochází určitým daným stanovištěm nebo pokud se chce dostat do objektu nebo získat přístup do IS, tento problém neřešíme, protože tvář je vždy orientována stejným směrem a ze stejné vzdálenosti a tak i její zachycení není větším problémem. V opačných případech je musí algoritmy počítačového softwaru složitě detekovat a lokalizovat (např. hromadné foto, identifikace z dálky, záznam v reálném čase atd.). Metod je vícero a základní dělení je na ***statisticky orientované*** (metoda podprostoru, metoda neuronových sítí) a ***znalostní*** (metody založené na odstínech šedi, na rozpoznávání obličejových obrysů, na informaci o barvách, na informaci o pohybu na scéně, na symetrii). V praxi se pro přesnější určení používají kombinace těchto metod.

Nalezený obličej je poté podroben softwarové analýze k vyhledání důležitých charakteristik. Jejich druh vyplývá z typu použité aplikace. Tzn., jak pracuje. Snímání může být 2D nebo 3D, černobílé, barevné, popř. infračervené a může být prováděno

z čelního nebo bočního pohledu. I zde se uplatňuje několik metod jak dané charakteristiky získat (metody založené na rozložení odstínů šedi v obraze, na geometrických tvarech a identifikačních markantech, metoda optických toků, metoda deformačních modelů, metody neuronových sítí, metoda Eigenhead).

Jako taková má každá metoda svoje pro a proti a nejvíce se v praxi využívalo a stále využívají metody založené na geometrických tvarech a identifikačních markantech. Velké výhody mají ale i metody založené na neuronových sítích, které jsou schopny sami se „učit“. Určitou výhodu má snímání obličeje v IR světle, které není závislé na vnějším osvětlení. Funguje na stejném principu jako u identifikace podle krevního řečiště hřbetu ruky, kdy se zaznamenává obraz, který vytváří cévy v obličeji. Ty přirozeně vystupují, jelikož rozvádí teplou krev po hlavě a tím pádem jsou teplejší než jejich okolí.

3.6.2 Bezpečnostně-komerční aplikace

Počátek komerčního využití je datován do roku 1999, kdy se na trhu objevily první programy na identifikaci podle tváře. Vzápětí vzrostla obliba nasazování této metody a neustále také stoupá díky svým vlastnostem jako je bezkontaktní snímání (možnost skrytého snímání), možnost hromadného snímání, rychlost identifikace a taktéž lze snímat obličeje na velkou vzdálenost (dle vlastností snímacího zařízení – kamery).

Pokud se uživatel přihlašuje (verifikuje) do systému je pro něj tato metoda velice přívětivá, neboť nezasahuje do jeho prostoru a pro identifikaci nemusí takřka nic udělat. Pro nasazení těchto systémů je také to, že lze využít stávající kamerové systémy a k těm dodat pouze příslušný software (SW). Taktéž pro potřeby identifikace mohou být použity již vyfocené fotografie. Na druhou stranu to, že na trhu s biometrickými systémy není tato metoda zase tak moc zastoupena může být způsobeno několika faktory. Jednak je někomu nepříjemné být focen či filmován, jiným to nedovoluje náboženství (Islám a jejich burky) a jiní ji prostě neberou jako standardní a spolehlivou metodu identifikace. Moderní systémy si již poradí i s brýlemi, klobouky, změnou světelných podmínek či změnou účesu.

Využití identifikace podle tváře může být jednak v identifikaci lidí ke zjištění, kdo je daná osoba, čehož se hromadně začalo využívat po teroristických útocích v září 2001 v USA. Tohoto se využívá zejména na letištích a také na dalších veřejných prostorech (např.

metro). Další oblastí může být ochrana hranic či určitých zájmových prostor jako jsou banky, kasina, hotely, obchodní domy, sportovní stadiony, nemocnice, důležité průmyslové komplexy či vládní budovy rozmanitého druhu. Prostě všude tam, kde je potřeba prověřit množství lidí (s nebo bez jejich vědomí). Zkušebně se také uvažuje využití této metody pro rozpoznání řidiče, který se dopustil například překročení rychlosti. Obviněný sice tvrdí, že vozidlo neřídil, opak je ale pravdou. Systém obličej projede registrem řidičů a najde odpovídající osobu. Také se může tato metoda používat pro klasickou verifikaci, kdy je potřeba ověřit identitu dané osoby (přístup do budovy, do IS, docházkové systémy apod.). Biometrická šablona tváře má velikost v řádech desítek kilobytů (kB).

Obr. 31. Možné použití identifikace podle tváře. Osoba je před turniketem sejmuta kamerou a systém vyhodnotí, zda může vstoupit či ne. Výsledek procesu se také ukáže na druhé straně zařízení. Dále rozhoduje obsluha vstupu do chráněných prostor. [38]

3.7 Geometrie ruky

Historický vývoj této metody nesahá příliš daleko do minulosti, jelikož se jedná o poměrně „mladou“ biometrickou metodu. První zařízení (jednorozměrné) bylo vyvinuto v 70. letech minulého století v Standfordském výzkumném institutu Robertem. P. Millerem a měřilo

pouze délku prstů ruky. Jak se technologie rozvíjely, přišly na řadu 2D a v současné době i 3D snímací (zatím ve fázi vývoje a vylepšování) zařízení k měření geometrie ruky. 2D zařízení pracuje s obrazem ruky shora, popř. z boku, kdežto 3D identifikuje uživatele na základě 3D modelu celé ruky. Za hlavního průkopníka dneška a budoucnosti je považována americká firma Recognition Systems, Inc. sídlící v USA v Kalifornii.

Obr. 32. Systém identifikující podle geometrie ruky od fy Recognition Systems, Inc. [39]

3.7.1 Podstata metody

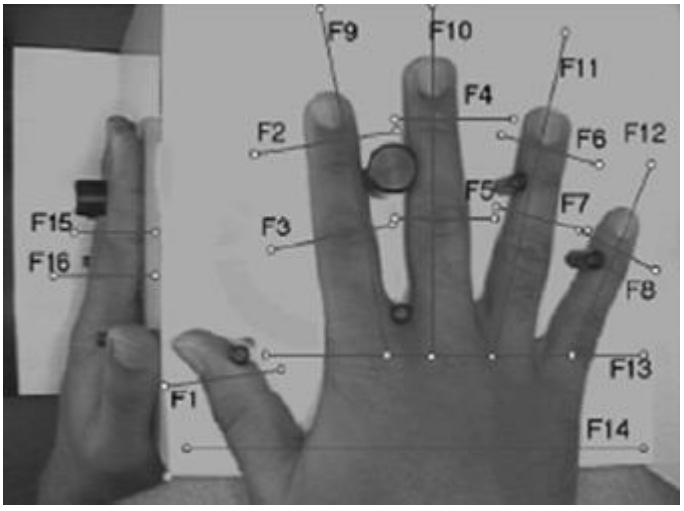
Každá ruka je zcela individuální na základě délky, šířky a výšky jednotlivých prstů a taktéž svým tvarem. Na tomto principu rovněž tato metoda pracuje. Většinou se jedna ruka vloží do přístroje na určené místo a určeným způsobem a ta je poté osvětlena pomocí infračervených LED[6] diod. Podložka pod ruku je z leštěného materiálu s vysokou odrazivostí a obraz je snímán pomocí digitální kamery s CCD čipem. Dříve se používala

[6] LED – Light Emitting Diod

metoda tzv. přímá, kdy snímací kamera byla přímo kolmo nad rukou, ale posléze se začalo využívat systému zrcadel, který obraz odráží do kamery, která již není umístěna nad rukou a toto má za následek zhruba o polovinu menší rozměry přístroje. Snímat se může ruka buď jenom shora, nebo i z boku.

Z nasnímaných geometrických dat se vytvoří šablona o velikosti několika bytů a do identifikačních zařízení se tak bez problému vejde až několik desítek tisíc šablon, což umožňuje tuto metodu používat i ve velkých aplikacích, např. různé výrobní, průmyslové a obchodní objekty (areály). Další výhodou je i to, že u každého vchodu do areálu či budovy může být umístěno jedno zařízení (stand-alone verze) a ty mezi sebou nemusí být nijak propojeny, protože do každého se mohou uložit referenční šablony všech zaměstnanců. Samozřejmostí je i sesíťování jednotlivých zařízení s centrálním stolním osobním počítačem (PC). Většinou se tato metoda používá v kombinaci s PINem či identifikační kartou. Klávesnice na zařízení neslouží ale jen k zadávání PINu, ale i k jeho administraci (kalibrace, vložení a smazání šablony, nastavení prahu citlivosti, autotest atd.).

Pokud nasnímaná šablona odpovídá referenční, je uživateli dovoleno projít. V opačném případě nikoliv. I zde figuruje tzv. match score a práh citlivosti.



Obr. 33. Ukázkové rozložení prstů při identifikaci na základě geometrie ruky. [40]

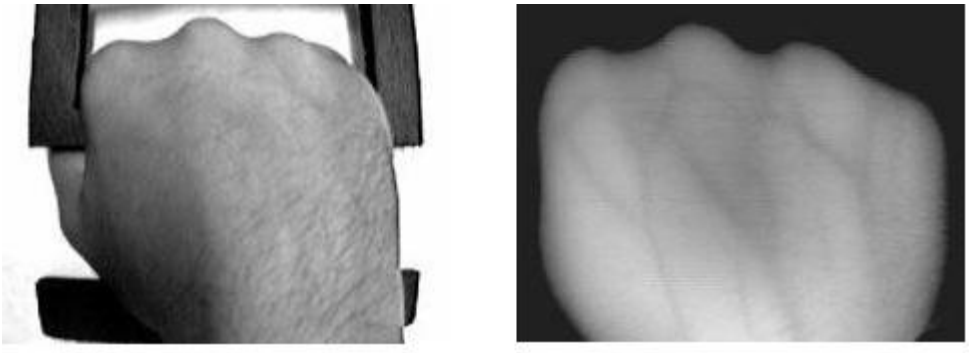
3.7.2 Bezpečnostně-komerční aplikace

Identifikace podle geometrie ruky se využívá pouze v bezpečnostně-komerčních aplikacích, jelikož nám dává málo informací pro identifikaci v policejně-soudní. Tímto je dána i sféra použití. Jde zejména o vstup do objektů různého charakteru (průmyslové, výrobní, vojenské atd.) mnohdy spojené s docházkovými systémy. Nemusí jít nutně o komerční objekty, ale i o věznice, školy, hraniční přechody, letiště, nemocnice, kasina, různé VIP kluby a jiné. Taktéž se této metody používá např. při ovládání nebezpečných technologií (atomové elektrárny, dálkově řízené rakety apod.).

Výhodami této metody je rychlost, snadnost identifikace z pohledu uživatele, malá velikost šablony, přijatelnost metody širokou veřejností a také to, že proces není ovlivněn nečistotami ruky. Nevýhodami pak jsou lehce nižší přesnost, využití zejména pro verifikaci, vyšší cena a omezené použití ve venkovním prostředí.

3.8 Krevní řečiště hřbetu ruky

Tato metoda se vyvinula z biometrické metody identifikace podle geometrie ruky. Jedná se o moderní metodu, která využívá obraz cév (tepny, žíly, vlásečnice) lidské ruky a to buď na jejím hřbetu anebo dlani. Výsledný obraz je unikátní pro každou ruku a pro každého člověka, i pro dvojčata.



Obr. 34. Hřbet ruky ve viditelném světle (vlevo) a v infračerveném (vpravo). [41]

3.8.1 Podstata metody

Ruka je položena na skenující zařízení a následně je nasvícena v infračerveném světle. Jelikož cévy rozvádí po lidském těle teplou krev, jsou cévy zřetelně vidět. Tímto se může zabezpečit i neoprávněné skenování (test živosti). Obraz je zaznamenán černobílou kamerou pomocí CCD čipu s 256 odstíny šedi. Výsledný snímek obsahuje ruku včetně mapy rozpoznaných cév. Pomocí algoritmů následuje úprava obrazu, kdy se odstraňuje šum a jiné negativní faktory a zvýrazňuje se kresba tepen a žil. Dalšími algoritmy je pak z obrazu vyextrahována biometrická šablona, na základě níž probíhá identifikace/verifikace.

3.8.2 Bezpečnostně-komerční aplikace

V porovnání s identifikací podle geometrie ruky nemusí uživatel pokládat ruku na stejné místo, ale šablona je prostorově orientována až při samotné identifikaci/verifikaci. Metodě nevadí vlhkost, poranění rukou či její nečistoty. Jedná se o bezkontaktní metodu a zařízení, které tento způsob identifikace používají, mají daleko větší potenciál miniaturizace než v případě geometrie ruky, kde je velikost dána velikostí lidské ruky. I proto se tato metoda rychle dostává do praxe a očekává se její nasazení např. u zámku dveří automobilů. Momentální nasazení je podobné jako u biometrické identifikace podle otisku prstu nebo geometrie ruky, tzn. zejména vstup do objektů, přístup k informačním systémům či zjišťování docházky osob. Pro nemalou část uživatelů jde ale o přijatelnější metodu než v případě geometrie ruky, protože nevyžaduje velké soustředění na způsob položení ruky a hlavně se nemusí dotýkat podložky, které se dotklo mnoho uživatelů před nimi.

Obr. 35. Ukázka přístrojů na skenování hřbetu ruky (vlevo) a dlaně (vpravo). [42]

3.9 Tvar ucha a jeho otisky

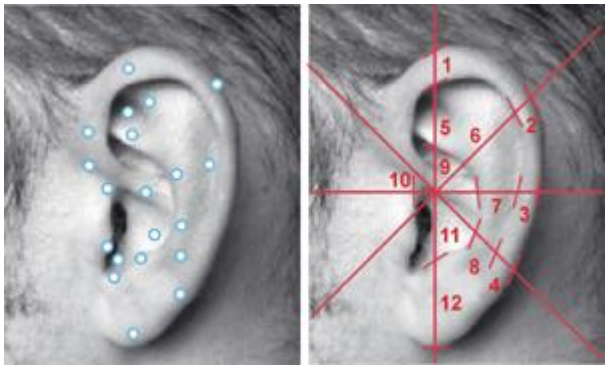
Domněnka, že každé ucho je unikátní, vznikla již dávno v lidské historii. Snažil se ji prokázat i Čech R. Imhofer, který zkoumal 500 otisků a došel k názoru, že stačí určit 4 markanty ucha k individuální identifikaci osoby. To byl začátek 20. století. Ve stejné době se v Anglii začala používat tato metoda k identifikaci novorozeňat v nemocnicích, aby nedošlo k jejich záměně.

Následovaly další studie a zkoumání např. Švýcara Hirschiho, Němců Georga, Langeho, Hungera, Hammera, Nizozemce Duboise a dalších, kteří shodně přišli k závěru, že otisk ucha je stejně jako otisk prstu zcela individuálním znakem každého člověka. Těmto závěrům zase oponovaly názory, že nebyly provedeny rozsáhlejší empirické výzkumy v tomto oboru a tak jejich tvrzení nemusí být zcela pravdivé. Postupem času se opravdu přišlo na to, že ucho má každý jedinečné a to dokonce levé od pravého.

V současné době se věnuje otiskům uší podobná pozornost jako otiskům prstů.

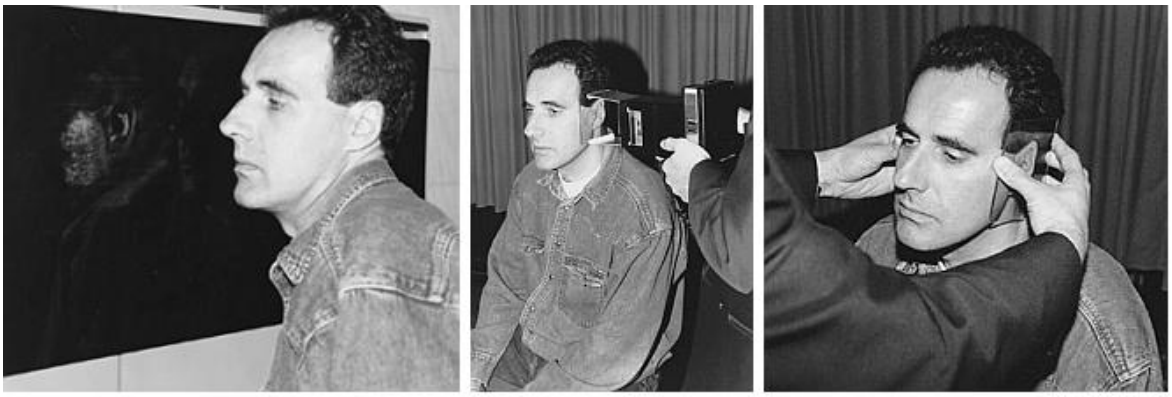
3.9.1 Podstata metody

Ucho se skládá z vnějšího, středního a vnitřního ucha. Pro identifikaci se používá tvar a otisk vnějšího ucha. Jeho konečná podoba je vytvořena již po 70 dnech vývoje plodu člověka a jeho vzhled se nemění až do smrti (kromě velikosti). Každé ucho a jeho optimální (plný) otisk má 20 základních anatomických znaků (markantů), podle kterých se otisky srovnávají.



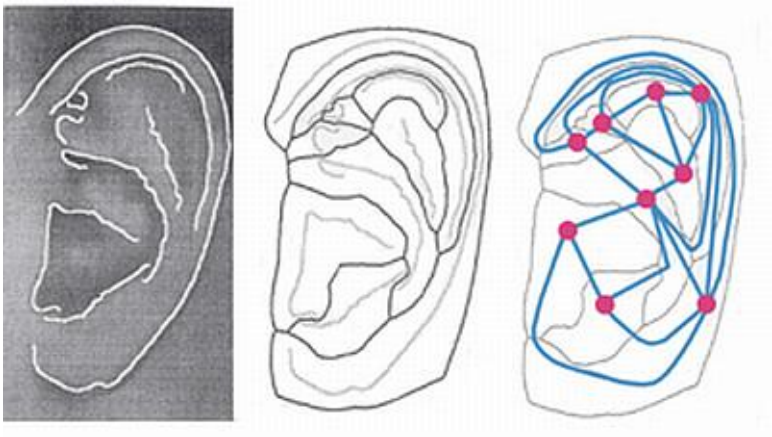
Obr. 36. Vlevo jsou základní markanty ucha a vpravo udávané geometrické charakteristiky (měří se velikosti úseček). [43]

Rozeznáváme 4 základní tvary ucha: kulaté, oválné, obdélníkové a trojúhelníkové. Jednotlivé druhy jsou u každé rasy zastoupeny v jiném počtu a na jeho základě se provádí základní kategorizace otisku. Na výsledný otisk má vliv působící tlak a směr působící síly a každý otisk je vždy jiný. Proto se také dělá vícero referenčních otisků při identifikaci jedince. Referenční otisky se provádí buď klasickou daktyloskopickou metodou, fotografickou nebo kombinovanou. Všechny tři jsou vidět na následujícím obrázku (Obr. 37.).



Obr. 37. Metody získání referenčního otisku ucha. Zleva daktyloskopická, fotografická, kombinovaná. [43]

K porovnávání uší se také začínají používat automatizované systémy, kde je ovšem strategie trošku odlišná. Toto porovnávání má několik kroků a to: pořízení snímku ucha (stačí černobílé), lokalizace vnějšího ucha a detekce hran pomocí matematických algoritmů, extrakce identifikačních křivek a sestavení grafického modelu – rozdělení ucha do oblastí, v kterých jsou poté určeny body ležící v jejich těžištích. Identifikace/verifikace pak probíhá na základě sítě, která vzniká spojením vytvořených bodů. Problémem může být již první fáze, protože osoba může mít ucho překryto vlasy a v tom případě se s výhodou používá snímání pomocí IR světla.



Obr. 38. Proces automatizovaného vytvoření šablony ze snímku ucha. Vlevo vidíme nalezené hrany v původním snímku. Uprostřed je ucho rozčleněno do několika oblastí a vpravo jsou vyznačeny body, po jejichž spojení je vytvořena síť potřebná k identifikaci či verifikaci osoby. [43]

3.9.2 Bezpečnostně-komerční aplikace

Bezpečnostně-komerční využití této metody je zatím poměrně malé. Může být ale nasazena všude tam, kde již jsou instalovány kamery pro snímání tváře a které mají schopnost rozeznávat tvary a různé objekty. Nevýhodou je možnost zakrytí ucha. Obecně ale zatím tato metoda rozšířena moc není, i když má velký potenciál, podobně jako otisky prstů.

Tato metoda je zejména využívána v policejně-soudní praxi, kdy na místě činu je celá řada stop vedoucích k pachateli a někdy i otisky uší. Otisky se nachází většinou na dveřích či oknech objektů, v důsledku poslouchání osoby, zda v daném prostoru někdo není. Zviditelňují se pomocí klasických daktyloskopických prášků. Před samotným porovnáváním otisků si musíme nejdříve ověřit, zda sejmutý otisk obsahuje dost charakteristických bodů pro identifikaci. Pokud ne, je nám takový otisk prakticky k ničemu.

3.10 Hlas a řeč

Obor rozpoznávání hlasu se rozvíjí již od 60. let minulého století (západní Evropa, USA). S první metodou založenou na trojrozměrném spektru řeči, tzv. sonogramu přišel Američan

L. G. Kerst v roce 1962. Poprvé provedl konkrétní experimenty na lidech a výsledky identifikace přes 99% rozdmýchaly velkou diskusi mezi fonetiky té doby. Objevily se metody založené na poslechové analýze a na instrumentálním zpracování řeči, které mezi sebou soupeří dodnes. S postupem času se poznatky o hlasových projevech rozrůstaly zejména kvůli využití v soudnictví a kriminalistice. V následujících letech přibývaly další empirické poznatky související s lidským hlasem a rozvoji vědomostí také nahrával prudký rozvoj informačních technologií, které podstatně vylepšují možnosti identifikace na základě instrumentálního měření.

Stále se zvyšující zájem o tuto identifikaci může být narůstající počet telefonních hovorů a odposlechů, rozmach telefonování přes Internet či zvyšující se počet bezpečnostních kamer zaznamenávajících kromě obrazu i zvuk. Obor, který se touto problematikou zabývá, se nazývá audioexpertíza. Pro její potřeby se využívá poznatků fonetiky, akustiky, audiotechniky atd.

Rozpoznání hlasu se využívá buď k verifikaci (bezpečnostní aplikace) nebo k identifikaci, která se provádí hlavně pro kriminalistické účely. Tam je potřeba zjistit podle získané nahrávky, čí zachycený hlas je. Jedná se o složitý proces, na jehož konci není zaručen odpovídající výsledek ani za použití moderního SW a hardwaru (HW) kvůli technické a jazykové kvalitě záznamu. Podle kvality se nahrávky dělí na zpracovatelné, obtížně zpracovatelné a nezpracovatelné.

3.10.1 Podstata metody

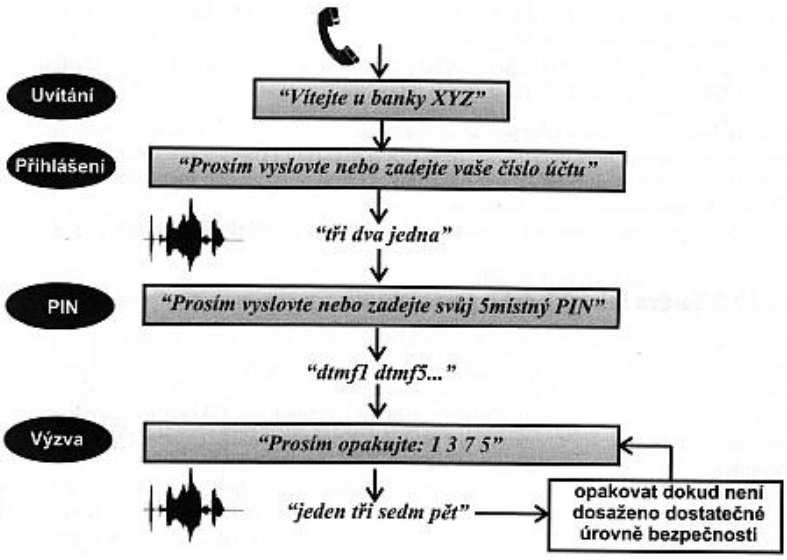
Metoda vychází z toho, že v mluveném projevu každého člověka jsou určité znaky, které má jenom on. Vychází se z toho, že každá osoba má anatomicky jinak vyvinuté mluvící ústrojí a z toho vyplývá, že každý jedinec má svůj jedinečný hlas (organické rozdíly). Další v čem se hlasy lidí odlišují, jsou získané charakteristiky řeči, tj. jak se osoba projevuje (naučené rozdíly). Na oba druhy odlišností musíme při porovnávání klást důraz, přičemž oba dva faktory se při identifikaci vzájemně prolínají. Lidská řeč je velice variabilní hned z několika důvodů. Mluvící orgány lze různě „nastavovat“ tak, abychom docílili různých druhů řeči. Můžeme používat buď speciální zařízení na změnu hlasu nebo také primitivní pomůcky jako kapesník, předmět v ústech, změna tónu nebo akcentu atd. V průběhu života se styl řeči mění také v závislosti na prostředí, kde člověk vyrůstá, stupni vzdělání,

výchově, popř. pokud dlouho člověk svou rodnou řečí nemluví. Na slovní projev má dále vliv jak momentální psychický a fyzický stav, tak i časový faktor. Dalším problémem v nahrávce může být zachycení různých ruchů a šumů. Můžeme sice použít různé filtry, ale i přesto není výsledek nijak zvlášť dobrý. Všechny tyto argumenty jasně ukazují, proč je identifikace na základě hlasu problematičtější v porovnání např. se stálými otisky prstů.

Vlastní zkoumání hlasu probíhá, jak jsem již řekl, dvěma metodami a to akustickým poslechem a instrumentálním zpracováním dnes převážně realizovaného na počítačích. V počítačovém zpracování se analyzují dva parametry (dlouhodobé spektrum řeči, spektrální rozložení formantů). Jinak řečeno, v prvním případě se graficky a číselně zaznamenává spektrum mluvené řeči, a v druhém případě frekvence a hladina zvuku v závislosti na čase.

3.10.2 Bezpečnostně-komerční aplikace

V této oblasti se identifikace podle hlasu využívá převážně k verifikaci, tj. k ověření identity osoby. Jako u většiny biometrických systémů se jí využívá k přístupu do objektu, či spíše do určitého prostoru, např. místnosti v bance, laboratořích a jiných významných objektech. Taktéž může hlasová verifikace sloužit k ovládání startování auta či k přístupu k tajným informacím v IS. Další oblastí, kde se využití této metody přímo nabízí, jsou bankovní transakce prováděné prostřednictvím telefonního přístroje. Zde však hrozí problém zkreslení mikrofonem a komunikačním kanálem.



Obr. 39. Typická aplikace telefonního bankovnictví. [1]

Jedná se o metodu přijatelnou pro uživatele, protože se jedná o bezkontaktní způsob verifikace a také proto, že řeč je pro nás samozřejmá a tak nás neobtěžuje. Problémem by ale mohl být pro němé či postižené lidi. Další výhodou je nižší cena aplikací, kdy stačí PC se zvukovou kartou, mikrofon a příslušný SW. Také odolnost vůči neoprávněným uživatelům je na dobré úrovni.

Mezi ostatními biometrickými metodami se jedná o středně přesnou metodu, protože hlas může být velice variabilní a v případě třeba nachlazení je možnost, že systém oprávněnou osobu odmítne. Dále je systém náchylný na chybu v případě dvojčat, kdy mluvící orgány mají velice podobnou stavbu. Posledním problémem v přesnosti je existence ruchů a šumů při verifikaci. Do budoucna se předpokládá velký pokrok v oblasti automatického a přesného rozpoznání hlasu a tak se dá očekávat jeho širší využití.

Obecně existují 3 systémy rozpoznání hlasu. Jsou to textově závislé systémy, systémy s textovou výzvou a textově nezávislé systémy. Textově závislé verifikují osobu na základě určeného sledu slov a jsou náchylné na oklamání pomocí nahrávky uživatele. S textovou výzvou požadují od osoby verifikovat se sledem slov, který náhodně vybere sám systém. Verifikace u poslední skupiny probíhá podle jakéhokoliv sledu slov, který uživatel vysloví. Zase je zde možnost obelhání systému nahrávkou. Dá se říci, že nejlepší jsou textově závislé, kde je EER v rozsahu 0,1 – 2%. Výkonnost systému ovlivňuje také spolupráce uživatele, variabilita hlasu mluvčího, podmínky záznamu a množství registračních a testovacích dat.

Verifikace probíhá tak, že osoba odříká text (podle druhu systému) a jeho biometrické charakteristiky jsou poté srovnány se šablonou uloženou v databázi. V případě shody je uživateli přístup povolen, v opačném odmítnut. Velikost šablony bývá 1500 – 3000 bytů.

3.11 Chůze

Jedná se o jednu z nejmladších způsobů biometrické identifikace, jejíž výhodou je zejména bezkontaktnost. V domácí literatuře se otázkou využití pohybů lidského těla zabývá až práce V. Porady a V. Karase a to v roce 1977. Uvádí možnosti teoretického i praktického využití pro kriminalistickou identifikaci.

První experiment ale uskutečnil až G. Johansson a to pomocí světel umístěných na těle člověka. Když se osoba pohybovala, vytvářela pomocí světel typické křivky, které se u každého jedince lišily.

Další zkoumání u nás i ve světě potvrdily na přelomu tisíciletí velký potenciál této metody pro identifikační/verifikační potřeby. Budoucí osud závisí zejména na rozvoji výpočetní techniky, která bude rozhodující pro její využitelnost v běžných bezpečnostních aplikacích.

Vítanou výhodou je schopnost přidat tuto technologii do již nainstalovaných kamerových a monitorovacích systémů, kde může fungovat společně s rozpoznáním tváře či ucha. Oproti těmto dvěma ale nabízí chůze způsob, jak identifikovat osobu, která má maskovaný obličej nebo v případě nedostatečného osvětlení snímané scény.

Samozřejmě, kde jsou výhody, musí být zpravidla i nevýhody. Největší nevýhodou této metody je mnoho individuálních specifičností chůze každého člověka. Tyto specifika jednak pomáhají vlastnímu využití pro identifikační účely, ale na druhou stranu ztěžují automatizovanému systému samotnou identifikaci/verifikaci.

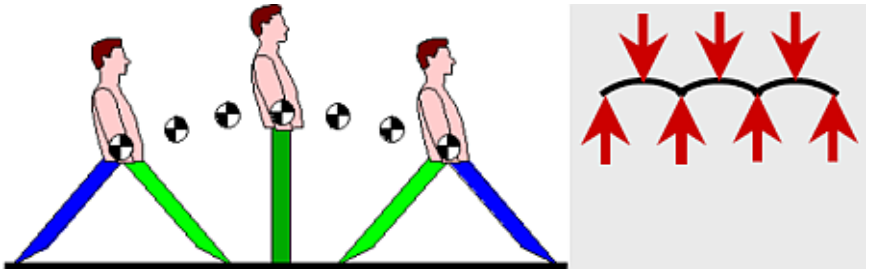
3.11.1 Podstata metody

Při pohybu člověka vznikají díky jeho funkčním a dynamickým vlastnostem určitě stopy. Těchto pohybů může být celá řada, např. skákání, běh, chůze, lezení, plazení i volný pád. Pro biometrické potřeby je v současnosti vhodná chůze a běh. Na projevy těchto pohybů mají vliv jak psychologické aspekty, tak i anatomické (výška, hmotnost, zdravotní stav, různé odchylky – zakřivení páteře, zranění, různé pohybové návyky, drogy, těhotenství atd.). Změna chůze může být samozřejmě i účelová.

Chůze i běh člověka je poměrně stereotypní, ale značně proměnlivý vzhledem k vnějším i vnitřním činitelům, které na ní působí. Rozhodující je tempo, zátěž, náročnost cesty, stres, únava a mnoho dalších faktorů. I technické vlivy jsou zde neopomenutelné. Identifikační systém založený na rozpoznání podle chůze musí počítat s různým oblečením, světelnými podmínkami či úhlem snímání a toto všechno ovlivňuje výsledný obraz pohybujícího se člověka.

Historicky prvním zkoumaným způsobem identifikace byl podle měnícího se těžiště při chůzi. Tento byl dále doplňován dalšími složkami chůze (ohyb v kolenech, kyčlích

kotnících, rotace hrudníku a pánve a další) a tak se výsledná křivka neustále zjemňovala. Dalšími sledovanými body jinými vědci bylo temeno hlavy či střed ucha.



Obr. 40. Metoda založená na pohybu těžiště. [12]

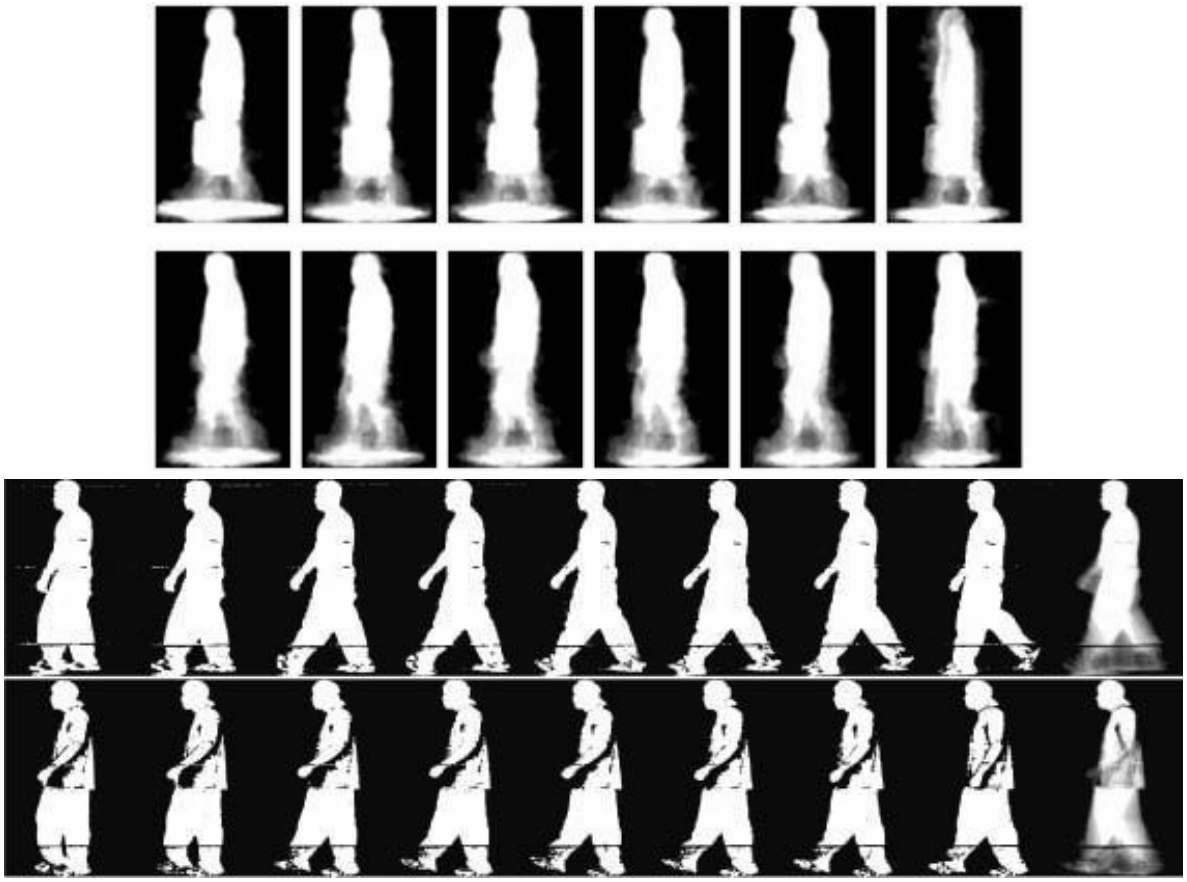
Jelikož sledování jednoho bodu na těle neposkytovalo dostatek informací, setkáváme se s tzv. sagitální[7] kinematikou. Jedná se o to, že při pohybu člověka měříme měnící se úhel mezi určitou částí končetiny a kloubem směrem dolů od předozadní osy procházející sledovaným kloubem.

Prvním větším krokem v automatizovaném rozpoznávání chůze byl počin Agentury pro výzkum pokročilých obranných projektů (DARPA), která jako první začala shromažďovat data o chůzi lidí a na jejich základě začala vyvíjet první algoritmy pro jejich rozpoznání.

V současnosti se metody používané k identifikaci chůze dělí do dvou základních směrů: [1]

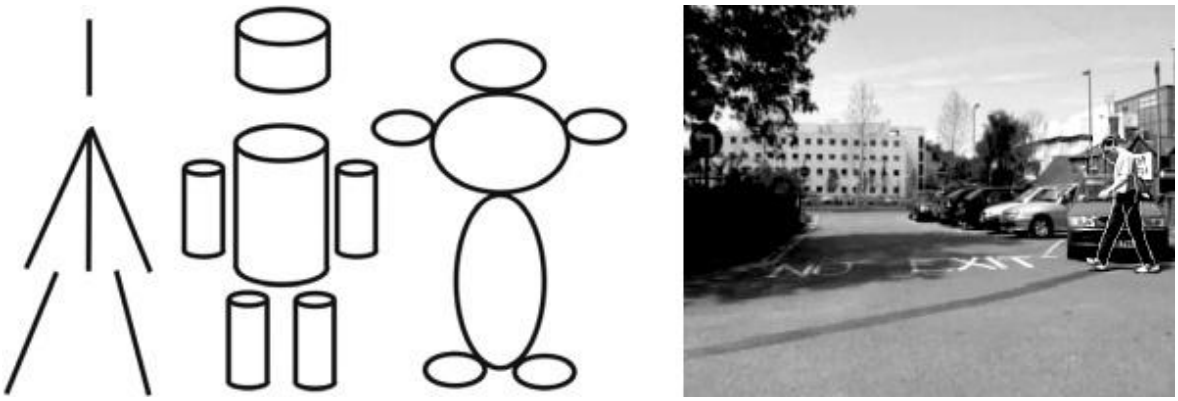
a) **metody založené na zpracování siluety pohybujícího se objektu** – silueta osoby, rozpoznané podle chůze, je vyčleněna z pozadí a ta se sleduje a vyhodnocuje.

[7] sagitální – rovnoběžný se střední (mediální) rovinou těla, předozadní



Obr. 41. Fázové pohyby siluety chodce snímané kamerou a počítačově zpracované. Nahoře osoba nesoucí kufřík a dole osoba bez kufříku. [48]

b) metody využívající modelování (rozpoznávání) pohybu – sledují a vyhodnocují dynamiku pohybu. Konkrétně se věnují pohybu horní části těla nebo nohou a zohledňují délky a úhly při chůzi. Hlavní modely jsou drátěný, cylindrický a oválný.



Obr. 42. Vlevo vidíme základní modely lidského těla pro analýzu pohybu – drátěný, cylindrický, oválný. Napravo je vidět ukázka drátěného modelu v reálné situaci. [13]

3.11.2 Bezpečnostně-komerční aplikace

Jak už bylo řečeno, jestliže je možné metodu přidat do již instalovaných systémů, jedná se vždy o výhodu, která není nezanedbatelná. Navíc se jedná o bezkontaktní metodu, která nijak neobtěžuje uživatele. Nabízí se také skryté nasazení.

Je asi patrné, že více než pro verifikaci se bude tato metoda využívat pro identifikaci. Bylo by asi náročné a odrazující, aby osoba po každé, když bude chtít vstoupit do objektu, pochodovala před kamerou sem a tam. Na druhou stranu by bylo možné tuto technologii uplatnit například při vstupu do svého domu, kdy by kamera zabírala určitou část cesty (chodníku), která vede ke dveřím, a po rozpoznání naší osoby by se dveře automaticky odemkly. Tohoto by ale šlo teoreticky zneužít, že by do domu někdo neoprávněný v nepozorované chvíli (otočení oprávněné osoby) vstoupil. Také by ale mohl být tento systém jen součástí celého zabezpečení domu. To je otázka k zamyšlení.

V identifikaci má tato metoda daleko lepší využití. Jde zejména o sledování a rozpoznávání osob na veřejných místech stejně jako u metody založené na tvaru tváře. Tzn., jednalo by se o důležité tranzitní uzly jako letiště, nádraží či velké prostory jako haly, stadiony, kde je velké množství lidí. Může jít také o bankovní prostory, hotely a jiné objekty. Dalším způsobem použití může být sledování pohybu konkrétních osob po městě či v určitém prostoru, který je pokryt kamerovým systémem.

Zájem bezpečnostních složek po způsobech skryté identifikace lidí stále sílí. Je to dáno hlavně strachem z dalších teroristických útoků, které do budoucna hrozí.

3.12 Ruční písmo a podpis

Problematika písma je velmi stará. Předchůdcem dnešního písma byly již v době okolo 4500 let př. n. l. tzv. piktogramy, kde jeden znak vyjadřoval celou větu. Další rozvoj následoval v podobě tzv. ideogramů (písmo klínové či hieroglyfické), kde jeden znak vyjadřoval jedno slovo. Kolem roku 1000 n. l. vzniká Fénická abeceda, která se rozšířila do celého světa. Z ní se odvíjela abeceda v Řecku, která se stala základem abecedy i písma latinského, používaného v různých obměnách do dnes. Z tohoto písma pak vznikla cyrilice a hlaholice, jež daly základ azbuce, dnes používané zejména v postsovětských státech. S dalším rozvojem latinky se objevilo psací písmo, které značilo potřebu rychlého psaní.

Toto písmo se také od roku 1932 stále učí na našich školách. Momentálně se v naší zemi hodně mluví o tom, že psací písmo je zastaralé a stejně všichni píší tiskacím písmem a tak je snaha určitých lidí výuku psacího písma nahradit písmem tiskacím, kterým by mělo být nově vytvořené písmo Comenia Script, jehož autorkou je Radana Lencová.

Obr. 43. Tiskací písmo Comenia Script Radany Lencové. [44]

3.12.1 Podstata metody

Každý rukopis je jedinečný a podpis je jeho menším vzorkem, který odráží jednotlivé vlastnosti celého rukopisu. Již století se zkoumají a porovnávají rukopisy a zejména podpisy, protože ty jsou používány k stvrzování různých listin, formulářů či dokumentů. Na základě rukopisů se také zkoumá psychický a fyzický stav jejího majitele.

Manuální porovnávání dvou výsledných podpisů nemusí být naprosto přesně, jelikož úplně přesný podpis žádná osoba nikdy dvakrát po sobě nenapíše a tak se spíše jedná o padělek. Zato moderní technologie jsou schopny nejenom rozeznat již výsledné podpisy, ale i průběh jejich vzniku, který ovlivňuje např. rychlost a směr tahů, tlak, pořadí písmen, sklon apod., což je pro identifikaci podpisu daleko podstatnější.

Rukopis každého člověka se také v průběhu života mění v závislostech na správném psaní písmen, znalosti gramatiky a schopnosti zdařile zobrazit jednotlivá písmena a styl jeho psaní může taktéž ovlivnit jeho momentální fyzická či psychická kondice. Další

individualizací mohou být podmínky při jeho psaní, např. poloha pisatele, osvětlení, ruch či stav psacího prostředku a podkladu nesoucího rukopis

Identifikace člověka na základě jeho písma je z dlouhodobého hlediska prokázána a v současnosti se k tomuto využívá již starší metoda nazývaná grafosynkritická analýza, která zkoumá jak grafickou, tak jazykovou stránku textu. Další vědou, která se zabývá písmem je grafometrie. Ta studuje znaky, jako je rychlost psaní, tlak, velikost písma, délky a šířky písmen atd. Psychologií písma a vším, co s ním souvisí, se v současnosti zabývá grafologie.

Všechny uvedené metody se využívají pro policejně-soudní potřeby. Z písma se zjišťují informace o pisateli (fyziologický a psychický stav, mentální a pohybové schopnosti a vnější podmínky při psaní textu). Praktické využití může být například u výhružných dopisů, dopisů na rozloučenou, závětí atd.

3.12.2 Bezpečnostně-komerční aplikace

V bezpečnostně-komerčních aplikacích se tato metoda identifikace používá s výhodou, neboť jde o údaj, který jen tak nezapomeneme a také je pro nás přívětivá, neboť jsme na podepisování zvyklý z každodenního života. V podstatě existují dva typy aplikací pro identifikačně-verifikační účely. Jsou to:

a) **off-line systémy (statické)** – osoba se podepisuje na papír. Poté je podpis digitalizován pomocí skeneru či kamery. Následuje porovnání mezi předkládaným podpisem a tím uloženým v databázi.

b) **on-line systémy (dynamické)** – osoba se podepisuje v reálném čase na speciální HW (tablet), pomocí speciálního HW (speciální pero) nebo jiným speciálním HW snímačem. Jsou zachycovány jak statické, tak dynamické charakteristiky podpisu a ten je poté porovnáván s referenčním podpisem, který je uložen v databázi.

Obr. 44. Ukázka speciálního tabletu pro snímání dynamiky podpisu od firmy Wacom. [45]

Samotný proces zpracování podpisu se u obou druhů systémů skládá ze tří podobných, ale různě náročných etap: předzpracování (vyhlazovaní a zjednodušování podpisu, odstranění šumu atd.), extrakce biometrických charakteristik a vyhodnocování (identifikace/verifikace).

Pro využití v bezpečnostních aplikacích se lépe hodí on-line systémy, které jsou méně náchylné na padělané podpisy, protože neporovnávají jenom finální podpis (statické charakteristiky), ale i dynamiku jeho vzniku (dynamické charakteristiky).

V reálu se setkáváme s různými typy padělaných podpisů a bránit se proti jejich přijetí můžeme správným nastavením prahu citlivosti. Tyto padělky rozdělujeme na ***jednoduché*** (podpis osoby je nevědomky chybně ztotožněn s podpisem jiné osoby, která je již v databázi), ***nahodilé*** (osoba zkouší různé podpisy a doufá, že některý bude uložen v databázi – nenapodobuje konkrétní podpis) a ***záměrně vytvořené*** (osoba se podepisuje jako konkrétní osoba).

3.13 Dynamika stisku počítačových kláves

Historie tohoto druhu identifikace sahá až do roku 1986, kdy si nechal první identifikační metodu patentovat Američan John D. Garcia. Jeho metoda využívá časových prodlev mezi stisky kláves při přihlašování k systému (zadání jména). Při tomto se vytvoří vektor, který je pak porovnán s referenčním vektorem a pokud se shodují, je přístup povolen.

Dalším zásadním dílem byla práce G. Gupty a R Joyceho, jejichž metoda pracovala na stejném principu, ovšem výpočet výsledného vektoru byl odlišný. Uživatel se přihlašuje pomocí uživatelského jména, jména a příjmení a hesla.

Důležitou prací je i ta od S. Blehy a kolektivu. Tito autoři preferují rozpoznání člověka na základě pouze přihlašovacího jména. Způsob je taktéž založen na časových odstupech stisknutí kláves, ale bere v potaz i průměr předchozích pokusů. Jejich způsob byl velice účinný a prakticky se jejich FRR rovnalo cca 4% při 529 pokusech a FAR cca 1% při 768 pokusech.

Jako taková je tato metoda v současnosti intenzivně zkoumána, jelikož počítačů a všeobecně informačních systémů přibývá a tak je ochrana informací v nich obsažených stále důležitější.

3.13.1 Podstata metody

Metoda využívá charakteristik při psaní textu na klávesnici počítače, které jsou pro každého individuální. Tyto charakteristiky se mohou postupem času měnit a to v závislosti na zkušenostech uživatele s psaním na PC. Z tohoto důvodu se může úspěšnost této metody v čase měnit. Využitelnými charakteristikami této metody může být:

- časová prodleva – doba mezi stisknutím různých kláves a délka jejich stisku,
- styl psaní velkých písmen – první je uvolněna klávesa Shift nebo příslušný znak?,
- rychlost psaní – měří se počet stisknutých znaků za určitou dobu,
- frekvence chyb – měří se počet překlepů a následného mazaní klávesou Backspace,
- síla použitá pro stisk klávesy – pomocí speciální klávesnice se měří tlak při psaní.

Novým trendem v tomto odvětví je tzv. kontinuální verifikace, která využívá pouze časy stisknutí kláves. Jedná se o vyhodnocování práce na PC po celou dobu jeho užívání. Při této se využívá „R“ hodnoty, která odráží současný psychický a fyzický stav člověka a tedy styl psaní. Dále se používá „A“ hodnota, která slouží k zaznamenání absolutní rychlosti. Z těchto hodnot potom vzejde výsledek přijetí či odmítnutí, např. v situaci, kdy uživatel odejde na toaletu a neoprávněná osoba si sedne k jeho PC.

3.13.2 Bezpečnostně-komerční aplikace

Zabezpečení pomocí této metody je aplikováno pro přístup do informačních systémů všeho druhu. Prostě tam, kde je žádoucí ochrana dat uložených v systému. Může se jednat jak o vládní IS, tak i čistě soukromé (ochrana osobních údajů, tajných informací, know-how atd.). Většinou se verifikace praktikuje na základě srovnávacího textu či loginu a hesla. Implementace této ochrany je velice snadná a finančně nenáročná. Celá biometrická ochrana je uskutečněna pomocí speciálního SW na běžném PC.

Jako příklad produktu na trhu můžeme uvést aplikaci BioPassword, která může zabezpečit buď jeden počítač či jiné počítače připojené v síti. Standardní obrazovka je nahrazena obrazovkou aplikace, kde probíhá identifikace uživatele. Míra citlivosti jde samozřejmě nastavit administrátorem. Registrace se provádí několikanásobným napsáním přihlašovacího jména a hesla (počet opakování nastavuje administrátor). Toto je poté vyhodnoceno a je sestavena referenční šablona určená ke srovnávání.

Celou metodu můžete zhlédnout a on-line si ji vyzkoušet například na této internetové stránce[8], anebo si můžete přímo stáhnout demo programu BioPassword do PC[9], abyste si udělali obrázek toho, jak takové přihlašování pomocí dynamiky stisku kláves vypadá v praxi.

---

[8] On-line vyzkoušení identifikace podle dynamiky stisků počítačových kláves je možná na internetové stránce *http://stage1.biopassword.com/democlient/*.

[9] Stahovatelné demo aplikace BioPassword (identifikace podle dynamiky stisku kláves) je možné získat například na této internetové stránce *http://packetstorm.linuxsecurity.com/Crackers/NT/biodemo.exe*.

Obr. 45. Přihlašovací okno aplikace BioPassword. Na obrázku vidíme korektní přihlášení (ověření) uživatele (mé osoby).

V současné době se také experimentuje u této metody identifikace s přidáním použití myši. Ukázkové video lze shlédnout na Internetu[10].

[10] Ukázka využití počítačové myši při identifikaci podle dynamiky stisků počítačových kláves je dostupná na internetové stránce *http://www.dcs.qmul.ac.uk/~pmco/biometric.rm*.

II. PRAKTICKÁ ČÁST

4 IDENTIFIKACE POMOCÍ TVARU TVÁŘE (VISIONACCESS)

Pro praktickou část mojí diplomové práce jsem si vybral biometrický systém založený na rozpoznání tváře uživatele. Vybral jsem si ho z důvodu zajímavého znázornění tváře člověka a jeho následné identifikace. Dalším důvodem mé volby bylo to, že tento systém je podle mého daleko více atraktivní pro čtenáře v porovnání například s otisky prstů. Tento systém máme momentálně k dispozici v jedné z laboratoří na Fakultě aplikované informatiky na Univerzitě Tomáše Bati ve Zlíně.

Systémy rozpoznání obličeje mají podle mě do budoucnosti velký potenciál zejména v bezpečnostně-komerčních aplikacích, kde bude kladen důraz hlavně na vysokou bezpečnost. Tyto aplikace budou sloužit k ochraně důležitých objektů a prostor jako jsou vládní budovy, vývojové laboratoře, bankovní trezory apod. Také využití pro hromadnou identifikaci osob na různých veřejných místech bude s rozvojem této technologie vzrůstat, jelikož se jedná v této oblasti o jedinečný způsob jak identifikace docílit.

4.1 Popis a parametry systému

Systém představila v roce 2007 kanadská společnost Bioscrypt, Inc. pod názvem VisionAccess. V ČR jej nabízí firma ADI Global Distribution (Honeywell, spol. s r.o.). Celý systém se skládá ze dvou hlavních částí a to **Enrollment Stationu** (stolní PC, 3D EnrolCam) a **FaceReaderu** (3D FaceReader Optical Unit, FaceReader Controller, Easy Install Box). V neposlední řadě k systému patří i SW, který celou funkčnost systému umožňuje. Zejména je to VisionAccess Enrollment Application k obsluze a nastavení první části systému a Vision 3DI k obsluze a nastavení druhé části systému.

VisionAccess pracuje na principu srovnání 3D modelů tváře. V jejich obrazech jsou nalezeny charakteristické body a referenční 3D model (šablona) sestávající se z těchto charakteristik se srovnává s 3D šablonou uživatele, který se dožaduje například vstupu do objektu.

Systém je odolný vůči změně barvy pleti, vousům a doplňkům (náušnice aj.). Není však schopen rozeznat tvář, kterou zakrývají brýle či jiné předměty (šály aj.).

4.1.1 Enrollment Station

Jedním prvkem této části je klasické **stolní PC**, na němž je nainstalován SW pro obsluhu a nastavení 3D EnrolCam.

Pro bezchybné fungování celého systému musí počítač splňovat tuto minimální konfiguraci:

- procesor Intel Pentium 4 na frekvenci 3,0 GHz nebo vyšší,
- minimálně 1 GB RAM operační paměti,
- minimálně 100 MB volného místa na pevném disku,

  Poznámka**:** V tomto místě není zahrnuto místo potřebné pro databázi. Pro každou šablonu je potřeba cca 2,5 MB místa na pevném disku.
- grafická karta podporující zobrazování na dvou monitorech, která disponuje kompozitním či s-video výstupem (Nvidia GeForce 4 a vyšší, ATI Radeon 9700 a vyšší),
- dále CD-ROM, síťová karta, sériový port (COM), USB 2.0,
- SW: Windows 2000 Professional nebo Windows XP Professional, Internet Explorer 6.0, DirectX 9.0b a vyšší.

Druhým prvkem je **3D EnrolCam**. Jedná se o speciální kamerový systém umístěný na tripodu (stojanu), který je doplněn o již zmíněný SW na připojeném stolním PC. Tato jednotka slouží k zavádění nových referenčních šablon uživatelů do systému.

Základem zařízení je barevná kamera doplněná projektorem, který vytváří pomocný zdroj osvětlení. Tvář uživatele je tak osvícena nejenom okolním světlem, ale i projektorem. Tímto snímáním se rekonstruuje 3D obraz lidské tváře. Prvek je také vybaven IR kamerou, která kontroluje, zda je před zařízením živý objekt a ne pouze objekt podobný tváři člověka. Tak je celý systém odolnější vůči oklamání.

Pro snímání obličeje je využíváno až 40 000 identifikačních bodů a pozornost je zaměřena hlavně na čelo, okolí očí a hřbet nosu.

Obr. 46. Provedení 3D EnrolCam. [8]

Postup sejmutí tváře je následovaný:

- nasnímání 3D video dat pomocí 3D stereometrie,
- rekonstrukce povrchu tváře,
- vyhlazení a interpolace dat,
- body 3D modelu tváře jsou uložený jako 3D síť,
- 3D síť se dále zpracovává za účelem vyhledání charakteristických znaků tváře, které se uloží do databáze.

Objekt snímání musí během referenčního snímání splnit několik podmínek. Jsou to tyto:

- tvář musí být v zorném poli kamery a ve vzdálenosti cca 80 cm od ní,
- osoba se nesmí pohybovat a měla by zaujmout neutrální výraz ve tváři,
- osoba musí mít sundané brýle a jiné předměty zakrývající tvář.

Základní parametry	
Biometr. technologie	rozpoznávání obličeje 3D
Technologie snímače	IR kamera
Způsob ověření identity	identifikace (1:N) / verifikace (1:1) - nastav.
Ověřované prvky	obličej / karta+obličej / PIN+obličej
Vestavěná čtečka	ne
Kapacita paměti vzorů	-
Připojení k PC	videosignál (RCA), USB
Software pro správu	AdminManager 3Di
Napájení	12 Vss
Odběr	1000 mA
Výstup	videosignál (RCA)
LED	ne
Bzučák	ne
Pracovní teplota	5 - 40 °C
Použití v exteriéru	ne
Rozměry - výška	292 mm
Rozměry - šířka	119 mm
Rozměry - hloubka	152 mm
Další funkce	náhledový LCD, snímání 3D (IR) / 2D (barevný) obrazu, nastavitelný poměr FAR/FRR

Obr. 47. Základní parametry jednotky 3D EnrolCam. [46]

4.1.2 FaceReader

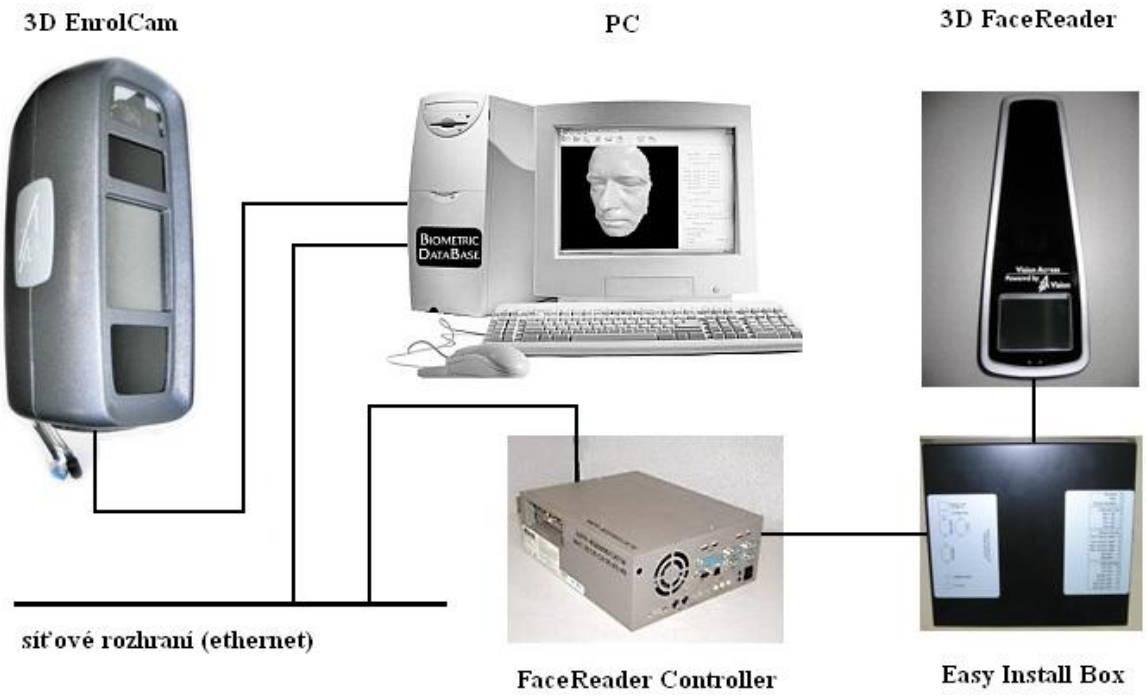
Základem této části systému je 3D FaceReader Optical Unit (FRO), jenž snímá tvář osoby a slouží tak k identifikaci uživatele (1:N, tzn. prohledání celé databáze) nebo k jeho verifikaci (1:1, tzn. ověření uživatele na základě PINu či identifikační karty). Tato jednotka je spojena prostřednictvím propojovacího pole zvaného Easy Install Box k FaceReader Controlleru (FRC). FR Controller je průmyslový počítač, který obstarává rozpoznávání tváří uživatelů a jejich srovnávání se šablonami v databázi. Může být na něho napojena jedna či více jednotek FRO.

Update databáze referenčních šablon uživatelů, kteří mají povolen vstup do systému se děje prostřednictvím softwaru Vision 3DI mezi stolním PC, na které je napojena 3D EnrolCam a jednotky FRC, ke které je napojen 3D FRO. Výměna informací se děje přes síťové rozhraní (ethernet).

K FRO může být také připojena čtečka karet pro znásobení zabezpečení přístupu a také dveřní kontrolér, který automaticky odemkne dveře po úspěšné identifikaci/verifikaci. FaceReader může fungovat buď síťově nebo jako stand-alone aplikace, tzn. samostatně.

Základní parametry	
Biometr. technologie	rozpoznávání obličeje 3D
Technologie snímače	IR kamera
Způsob ověření identity	identifikace (1:N) / verifikace (1:1) - nastav.
Ověřované prvky	obličej / karta+obličej / PIN+obličej
Vestavěná čtečka	ne
Kapacita paměti vzorů	1000 (identif.) / 60000 (verif.)
Připojení k PC	TCP/IP
Software pro správu	AdminManager 3Di
Napájení	24 Vss
Odběr	1500 mA
Výstup	Wiegand, TTL, RS-485, RS-232
LED	ne (barev. LCD)
Bzučák	ne (reprod.)
Pracovní teplota	5 - 35 °C
Použití v exteriéru	ne
Rozměry - výška	355 mm
Rozměry - šířka	132 mm
Rozměry - hloubka	116 mm
Další funkce	barevný dotykový LCD, konfigurovatelný hlasový výstup, navigace uživatele, volit. klávesnice na LCD

Obr. 48. Základní parametry jednotky 3D FaceReader Optical Unit. [47]



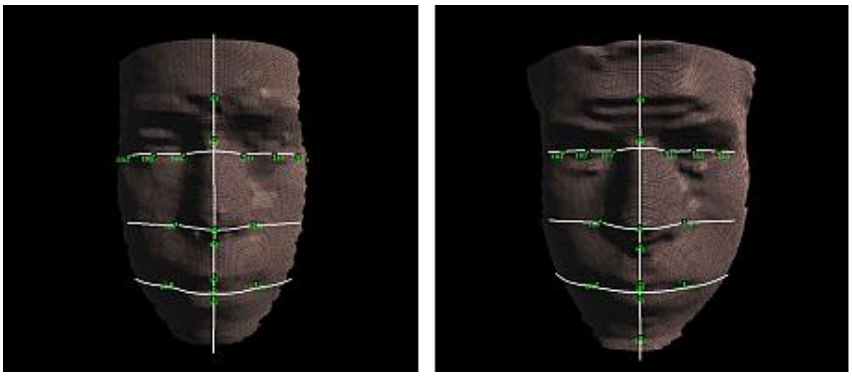
Obr. 49. Zjednodušené schéma možného zapojení systému VisionAccess. [8] [9]

4.2 Praktické cvičení

Na systému VisionAccess jsem provedl laboratorní úlohu, která měla za cíl odzkoušet jeho funkčnost a vlastnosti. K tomuto jsem si také přizval pomocníka-figuranta, kterému jsem poděkoval na začátku mojí práce. Celá úloha měla několik částí.

1. Nasnímání a uložení referenčních šablon. Po zapojení a zapnutí celého systému jsme oba dva provedli nasnímání a uložení šablon našich tváří. Jelikož nasvětlení scény nebylo ideální, bylo potřeba snímání párkrát opakovat, abychom docílili slušné kvality obrazu. I přes opakování ale nebyly výsledné obrazy úplně ideální. Obraz se hned pro kontrolu verifikuje, zda bude možná budoucí verifikace (identifikace). Při snímání jsme zjistili, že aby byl threshold nad 80%, je možné maximální horizontální natočení hlavy o cca 8,5° a vzdálenost tváře od kamery se může měnit v rozmezí cca ± 10 cm od stanovené hodnoty.

Obr. 50. Snímání tváře jednotkou 3D EnrolCam.



Obr. 51. Obrazy tváří s charakteristickými body. Vlevo je vidět obraz figuranta a vpravo můj. Rozdíl je jasně patrný.

2. Výpočet podobnosti. Po uložení obrazů jsem pro názornost vypočítal jejich podobnost, tzv. koeficient shody **m**. Vztah je určen sice pro 2D porovnávání, ale pro představu, jak takové porovnávání probíhá, bude dostačující a stále ještě pochopitelný. Koeficient shody **m** je veličina, kterou se v matematice hodnotí podobnost buď dvou vektorů, nebo spojitých signálů. V tomto případě jsou naměřené rozměry jednotlivých sémantických rysů složkami vektorů **a** a **b**.

Tab. 2. Jednotlivé sémantické rysy tváře a jejich hodnoty.

Jednotlivé sémantické rysy tváře	Hodnoty $A_1 - A_8$ [mm] pro 1. osobu (figuranta)	Hodnoty $B_1 - B_8$ [mm] pro 2. osobu (mě)	Výsledný vektor [mm] $\vec{\Delta} = \vec{a} - \vec{b}$
Velikost levého oka	34,49	32,12	2,37
Velikost pravého oka	36,86	28,86	8,00
Délka nosu	51,09	50,85	0,24
Levá část nosu	36,39	42,98	-6,59
Pravá část nosu	35,78	40,50	-4,72
Šířka nosu	43,00	44,03	-1,03
Výška nosu	14,93	16,96	-2,03
Velikost rtů	2,51	2,32	0,19

$$m = 0{,}5 + 0{,}5 \times \frac{\sqrt{\vec{\Delta} \cdot \vec{\Delta}}}{3 \times \sigma}, \tag{5}$$

kde σ (sigma) je směrodatná odchylka nebo typický rozptyl odlišnosti dvou jedinců.

$$m = 0{,}5 + 0{,}5 \times \frac{\sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2 + \ldots + (a_8 - b_8)^2}}{3 \times \Sigma}$$

$$m = 0{,}5 + 0{,}5 \times \frac{\sqrt{2{,}37^2 + 8^2 + 0{,}24^2 + 0{,}24^2 + (-6{,}59)^2 + (-4{,}72)^2 + (-1{,}03)^2 + (-2{,}03)^2 + 0{,}19^2}}{3 \times 10}$$

$$m = 0{,}5 + 0{,}5 \times \frac{\sqrt{140{,}5989}}{30} = 0{,}5 + 0{,}5 \times 0{,}395 = 0{,}6975$$

$$m \times 100 = \underline{\underline{69{,}75\%}}$$

Výsledkem je tedy to, že naše obličeje jsou si z 2D hlediska podobné z 69,75 procent.

3. Identifikace pomocí 3D FRO. Poslední částí byla identifikace pomocí FRO. Po spuštění příslušného SW jsme vložili své údaje do databáze a uložili. Poté jsme pomocí FRO provedli naši identifikaci. Po jejím úspěšném dokončení se na LCD displeji FRO objeví nápis Access Granted a tím je identifikace dokončena a „vstup“ povolen.

Obr. 52. Proces identifikace prostřednictvím FRO.

4.3 Zhodnocení

Při procesu snímání referenční šablony je důležité dodržet několik podmínek. Jde o to správně nastavit snímací zařízení z hlediska polohy (podle manuálu). Dalším bodem je vhodné nasvětlení celé scény a našeho okolí. V neposlední řadě je potřeba dodržet snímací vzdálenost, zachovat neutrální výraz a nehýbat se při snímání.

Pokud výše uvedené podmínky dodržíme, nic nebrání tomu, aby byl do 10 sekund zhotoven kvalitní obraz naší tváře.

Samotná verifikace (identifikace) je velmi spolehlivá a i při nastavení míry citlivost na 80% (vysoká bezpečnost) je porovnání otázkou pár sekund. Vše ovšem záleží na kvalitní referenční šabloně a okolním vlastnostem při identifikačním či verifikačním procesu.

Závěrem mohu říci, že systém rozpoznání tváře je velice přívětivý k uživateli, který se jenom „nastaví“ snímací kameře a během okamžiku je jeho identita rozpoznána. Nabízí také vysokou míru bezpečnosti, kdy i při přísném nastavení thresholdu je FRR velice nízké (např. při thresholdu 80% je to pouze 1,5% pro parametr FRR).

ZÁVĚR

Tato práce byla vytvořena pro potřeby předmětu Kriminalistické technologie a systémy. Je zpracována jako výukový materiál pro oblast biometrických systémů. Měla by v budoucnu sloužit posluchačům tohoto předmětu jako zdroj k získávání poznatků a vědomostí, vztahujících se k tomuto tématu. Zpracování jsem pojal jak teoreticky, tak i s praktickou ukázkou na vybraném biometrickém systému.

V teoretické části jsem jako první probral obecné hledisko identity a identifikace a samostatně popsal identifikaci člověka, což je zde významné, pro pochopení celého problému biometrické identifikace. Dále jsem se věnoval biometrii jako takové a popsal jsem její historický vývoj až do současnosti. Historie sahá až několik tisíc let před naším letopočtem, kdy se dají vypátrat první zmínky o využití biometrie k identifikaci.

Další část jsem věnoval vysvětlení důležitých pojmů jako je biometrie, biometrické charakteristiky, FAR, FRR atd. a hlavně jsem vysvětlil rozdíl mezi identifikací (ztotožněním) a verifikací (ověřením). Přesné vysvětlení a pochopení těchto termínů je stěžejní, aby se čtenáři zorientovali v tomto tématu a mohli díky nim jednoznačně identifikovat vlastnosti různých biometrických systémů.

Posluchači tohoto předmětu se taktéž seznámí s kritérii pro hodnocení biometrických systémů, které jim mohou pomoci při posuzování různých biometrických metod či při případném výběru takovýchto zařízení.

V poslední části teorie jsem rozebral jednotlivé metody biometrické identifikace a verifikace používané v současné době. Experimentální metody jsem záměrně vynechal. Většinou je popsána jejich stručná historie, podstata metody, tedy jak pracují a také jsem vylíčil jejich možné použití v praxi v bezpečnostně-komerčních aplikacích. Pokud se tyto metody neuplatňují momentálně v těchto aplikacích, je zmíněno jejich policejně-soudní využití.

V praktické části jsem provedl testování systému rozpoznání tváře, který je k dispozici na Fakultě aplikované informatiky na Univerzitě Tomáše Bati ve Zlíně. Toto testování jsem také zhodnotil a upozornil na různá rizika spojená se snímáním tváře tímto zařízením.

Všechny uvedené informace by měly posloužit k získání vědomostí o oblasti biometrie jako celku a také o jednotlivých biometrických metodách, které se v současnosti využívají k identifikaci či verifikaci osob v reálných aplikacích.

ZÁVĚR V ANGLIČTINĚ

This work was created to serve the subject Criminalistic technology and systems. It is prepared as a teaching material for the area of biometric systems. It should in the future serve students of this subject as a source of knowledge related to this subject. I have looked at processing both theoretically and practically – with practical example on selected biometric system.

In the theoretical part, I first focused on the general aspect of identity and identification, and then separately on human identification, which is important for understanding the whole problem of biometric identification. Then I focused deeper on biometrics and described its historical development until now. The history goes back several thousand years BC, when we can find the first references of biometrics being used for identification.

Next part is devoted to an explanation of important terms such as biometrics, biometric characteristics, FAR, FRR, etc. Mainly, I explained the difference between identification (ego-involvement) and verification (verification). Rigorous explanation and understanding of these terms is crucial for the readers to understand this topic and thanks to them to clearly identify the characteristics of different biometric systems.

Students in this course are also familiar with the criteria for evaluation of biometric systems that can help them in assessing various biometric methods or in choosing such devices.

In the last part of the theory I disassembled the individual methods of biometric identification and verification currently in use. I purposely left out experimental methods. Usually, their short history, principle or how they work is discussed, and I also described the possible use in practice in security-commercial applications. If these methods are not currently used in these applications, then police-court usage is mentioned.

In the practical part, I tested the system for identifying face, which is available at the Faculty of Applied Informatics of Tomas Bata University in Zlín. I also evaluated this testing and identified various risks associated with the sensing face with this device.

All of the above information should serve to gain knowledge about the area of biometrics as a whole and also about the individual biometric methods, which are currently used for identification or verification of individuals in real-world applications.

SEZNAM POUŽITÉ LITERATURY

[1] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk a kolektiv. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha : Grada Publishing, 2008. 631 s. ISBN 978-80-247-2365-5.

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

[3] PORADA, Viktor a kolektiv. *Kriminalistika*. Brno : CERM, 2001. 746 s. ISBN 80-7204-194-0.

[4] MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika*. 2. přeprac. a dopl. vyd. Praha : C.H. Beck, 2004. 583 s. ISBN 80-7179-878-9.

[5] NĚMEC, Miroslav. *Kriminalistická taktika pro policisty*. 1. vyd. Praha : Eurounion Praha, 2004. 328 s. ISBN 80-7317-036-1.

[6] STRAUS, J.: *Kriminalistika, kriminalistická technika : pro kvalifikační kurz kriminalistických expertů*. Praha : Policejní akademie České republiky, 2006. 301s. ISBN 80-7251-216-1.

[7] PORADA, Viktor. *Teorie kriminalistických stop a identifikace : technické a biomechanické aspekty*. 1. vyd. Praha : Academia, 1987. 328s, barev. obr. příl.

[8] A4VISION INC., Vision Access™. *Enrollment Station 2.0 : Installation Manual*. 4.0.0.060823. California, USA : A4Vision Inc., 2006. 35 s.

[9] A4VISION INC., Vision Access™. *Face Reader 3.0 : Installation Manual*. 4.0.0.060627. California, USA : A4Vision Inc., 2006. 25s.

[10] KAŠPAR, Karel. *Kriminalistika : (Úvod, technika, taktika)* [online]. Praha : 2008 [cit. 2010-06-08]. Dostupný z WWW: <http://www.vsrr.cz/pomucka/kriminalistika1.pdf>.

[11] DRYGAJLO, Andrzej. *Biometrics : Biometrics-Lecture-8-Part1* [online]. 2006 [cit. 2010-06-08]. Dostupný z WWW: <http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/08-Biometrics-Lecture-8-Part1-2006-12-11.pdf>.

[12] PATTON, James. *Gait Section, PartB, Kinesiology* [online]. 2002 [cit. 2010-06-08]. Dostupný z WWW: <http://www.smpp.northwestern.edu/~jim/kinesiology/partB_GaitMechanics.ppt.pdf>.

[13] Bratislavská vysoká škola práva. *Notitiae ex Academia Bratislavensi Iurisprudentiae : Rozbor možností identifikace osob na základě projevů jejích lokomoce (zejména chůze)* [online]. Žilina : 2008 [cit. 2010-06-08]. Dostupný z WWW: < http://www.uninova.sk/pf_bvsp/casopis/1-2008_Notitae.pdf >.

[14] TUČEK, Josef. *Oko jako důkaz místo otisku prstu - iDNES.cz* [online]. 12.7.2002 [cit. 2010-06-08]. Oko jako důkaz místo otisku prstu . Dostupné z WWW: <http://zpravy.idnes.cz/oko-jako-dukaz-misto-otisku-prstu-dra-/vedatech.asp?c=A020715_100635_vedatech_zem>.

[15] TOUFAR, Petr. *Historie RISC procesorů* [online]. 2002 [cit. 2010-06-08]. Oko jako důkaz místo otisku prstu . Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2002/xtoufar1.htm>.

[16] FreePatentsOnline.com. *Personal identification apparatus - Patent 4621334* [online]. c2004-2010 [cit. 2010-06-08]. Personal identification apparatus. Dostupné z WWW: <http://www.freepatentsonline.com/4621334.html>.

[17] VANČO, Emil. *Policie ČR nezneužívá DNA - Policie České republiky* [online]. c2010 [cit. 2010-06-08]. Policie ČR nezneužívá DNA. Dostupné z WWW: <http://www.policie.cz/clanek/policie-cr-nezneuziva-dna.aspx>.

[18] LORENC, Miroslav. *Zadání samostatných cvičení - Excel 4* [online]. c2007-2010 [cit. 2010-06-08]. Zadání samostatných cvičení - Excel 4. Dostupné z WWW: <http://lorenc.info/3MA381/sc-excel_4.htm>.

[19] RAMEŠ, Jiří. *Vstupní zařízení PC* [online]. 2002 [cit. 2010-06-08]. Čtečka čárových kódů. Dostupné z WWW: <http://vstupnizarizeni.rames.info/7code.html>.

[20] DOLEŽÁLEK, Jan. *DarkArt » Kevin Warwick* [online]. c2004 [cit. 2010-06-08]. Kevin Warwick. Dostupné z WWW: <http://www.darkart.cz/?page_id=416>.

[21] VACH, Martin. *Historie biometrik a jejich využití ve výpočetní technice* [online]. 2003 [cit. 2010-06-08]. Historie biometrik a jejich využití ve výpočetní technice. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm>.

[22] KRHOVJÁK, Jan; MATYÁŠ, Václav. *Autentizace a identifikace uživatelů* [online]. 2007 [cit. 2010-06-08]. Autentizace a identifikace uživatelů. Dostupné z WWW: <http://www.ics.muni.cz/zpravodaj/articles/560.html>.

[23] FÜRBACH, Martin. *Uříznout si bříška prstů nestačí. Vzor pro otisky se vám vrátí - iDNES.cz* [online]. 30.7.2008 [cit. 2010-06-08]. Uříznout si bříška prstů nestačí. Vzor pro otisky se vám vrátí. Dostupné z WWW: <http://technet.idnes.cz/uriznout-si-briska-prstu-nestaci-vzor-pro-otisky-se-vam-vrati-pb7-/tec_technika.asp?c=A080728_203638_tec_technika_fur>.

[24] The New York State Division of Criminal Justice Services. *Criminaljustice.state.ny.us* [online]. 1997 [cit. 2010-06-08]. The New York State Bertillon Bureau. Dostupné z WWW: <http://criminaljustice.state.ny.us/ojis/history/bert_ny.htm>.

[25] Společnost pro kriminalistiku. *Papilární linie, obrazce a markanty* [online]. c2010 [cit. 2010-06-08]. Obrazce a znaky kůže. Dostupné z WWW: <http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm>.

[26] JEDLIČKA, Miloslav. *Daktyloskopie* [online]. c2009 [cit. 2010-06-08]. Kriminalistická daktyloskopie. Dostupné z WWW: <http://www.vpsmvbrno.cz/osobni/jedlicka/daktyl/daktyl.html>.

[27] DAVIDÍK, Michael. *Gamesport.cz - PC Snímač otisku prstů od Microsoftu - informace, článek, download, galerie* [online]. 19.10.2004 [cit. 2010-06-08]. Snímač otisku prstů od Microsoftu. Dostupné z WWW: <http://www.gamesport.cz/clanek-snimac-otisku-prstu-od-microsoftu.html>.

[28] My Digital Life. *Armatix Pistol Offers Safety Mechanism Via Wristwatch » My Digital Life* [online]. 3.2.2010 [cit. 2010-06-08]. Armatix Pistol Offers Safety Mechanism Via Wristwatch. Dostupné z WWW: <http://www.mydigitallife.info/2010/02/03/armatix-pistol-offers-safety-mechanism-via-wristwatch/>.

[29] Eurosat CS. *Čtečka otisku prstů BioSwitch* [online]. c2010 [cit. 2010-06-08]. Čtečka otisku prstů BioSwitch. Dostupné z WWW: <http://www.eurosat.cz/410-bioswitch-ctecka-otisku-prstu.html>.

[30] Borgis a.s. *Mobily už mají i čtečku otisků prstů – Novinky.cz* [online]. 14.3.2008 [cit. 2010-06-08]. Mobily už mají i čtečku otisků prstů. Dostupné z WWW: <http://www.novinky.cz/internet-a-pc/135359-mobily-uz-maji-i-ctecku-otisku-prstu.html>.

[31] Ministerstvo vnitra ČR. *Ministerstvo vnitra - časopis Policista 2/2002* [online]. 2002 [cit. 2010-06-08]. Daktyloskopické pouzdro na pistoli. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/2002/02/pro4id.html>.

[32] LYLE, D. P. *Dirty DNA « The Writer's Forensics Blog* [online]. 18.11.2009 [cit. 2010-06-08]. Dirty DNA. Dostupné z WWW: <http://writersforensicsblog.wordpress.com/2009/11/18/dirty-dna/>.

[33] Home DNA Testing Kits.net. *Home DNA Testing Kit Reviews* [online]. 12.3.2008 [cit. 2010-06-08]. DNA Testing at Home. Dostupné z WWW: <http://www.homednatestingkits.net/>.

[34] SOVOVÁ, Veronika. *Přístroj zvaný oko* [online]. c2010 [cit. 2010-06-08]. Přístroj zvaný oko. Dostupné z WWW: <http://veronika.sovova.sweb.cz/interest/oko.htm>.

[35] Digitus s.r.o. *DIGITUS s.r.o. - identifikační systémy, biometrie* [online]. c1999-2009 [cit. 2010-06-08]. Kontrola vstupu a docházky / Panasonic BM-ET200. Dostupné z WWW: <http://www.digitus.cz/produkt_bm200.php>.

[36] Digitus s.r.o. *DIGITUS s.r.o. - identifikační systémy, biometrie* [online]. c1999-2009 [cit. 2010-06-08]. Kontrola vstupu a docházky / OKI IrisPass-M. Dostupné z WWW: <http://www.digitus.cz/produkt_irispassm.php>.

[37] MAINGUET, Jean-François. *Biometrics: retinal* [online]. c2004-2010 [cit. 2010-06-08]. Retinal / Rétine. Dostupné z WWW: <http://pagesperso-orange.fr/fingerchip/biometrics/types/retinal.htm>.

[38] GAT Solutions a.s. *OVI BlackBall | GAT* [online]. c2010 [cit. 2010-06-08]. OVI BlackBall. Dostupné z WWW: <http://www.gat-solutions.sk/sk/ovi-blackball>.

[39] Brigham Scully. *Ingersoll Rand Security Technologies Schlage biometrics Photos* [online]. c2010 [cit. 2010-06-08]. PHOTOS. Dostupné z WWW: <http://www.brighamscully.com/photos/prsi.html>.

[40] Vysoké učení technické v Brně, Fakulta informačních technologií. *STRaDe - Security Technology and Development* [online]. c2009 [cit. 2010-06-08]. Snímání geometrie ruky. Dostupné z WWW: <http://strade.fit.vutbr.cz/biometrie/snimani-geometrie-ruky.html>.

[41] DOBIÁŠ, Richard; HIRŠ, Petr. *(Snímek 2) BIOMETRIE - Technologie žil hřbetu / dlaně ruky* [online]. c2006 [cit. 2010-06-08]. Technologie žil hřbetu ruky. Dostupné z WWW: <http://bio.sonixdesign.net/snimky/snimek2.html>.

[42] DOBIÁŠ, Richard; HIRŠ, Petr. *(Snímek 2) BIOMETRIE - Technologie žil hřbetu / dlaně ruky* [online]. c2006 [cit. 2010-06-08]. Technologie žil hřbetu ruky. Dostupné z WWW: <http://bio.sonixdesign.net/snimky/snimek4.html>.

[43] Ministerstvo vnitra ČR. *Kriminalistika : Časopisy - internetové stránky resortních a partnerských tiskovin včetně nakladatelství Themis|archiv stranek mvcr.cz, cerven 2008* [online]. c2004 [cit. 2010-06-08]. Identifikace osoby na základě tvaru ucha a jeho otisků - II. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0402/ident_info.html>.

[44] LENCOVÁ, Radana. *Radana Lencová - Nová psací latinka - Comenia Script* [online]. c2002-2008 [cit. 2010-06-08]. Radana Lencová - Comenia script. Dostupné z WWW: <http://www.lencova.eu/cs/gal_latinka>.

[45] Fakulta informatiky Masarykovy univerzity. *Stránky laboratoře LaBAK | Fakulta informatiky Masarykovy univerzity* [online]. c2008 [cit. 2010-06-08]. Vybavení laboratoře. Dostupné z WWW: <http://www.fi.muni.cz/research/laboratories/labak/vybaveni.xhtml.cs>.

[46] ADI Global Distribution. *ADI - 3D EnrolCam - Registrační kamera 3D VisionAccess* [online]. c2010 [cit. 2010-06-08]. Registrační kamera 3D VisionAccess. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/w/72D5641E94DE16C7C12573B4005F81F6?OpenDocument>.

[47] ADI Global Distribution. *ADI - 3D FaceReader - Snímací a vyhodnocovací jednotka s kamerou 3D VisionAccess* [online]. c2010 [cit. 2010-06-08]. Snímací a vyhodnocovací jednotka s kamerou 3D VisionAccess. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/w/A3BDB41A497CF9A6C12573B4005F81F8?OpenDocument>.

[48] Visualization and Intelligent Systems Laboratory. *VISLab* [online]. c2010 [cit. 2010-06-08]. Current Projects. Dostupné z WWW: <http://vislab.ucr.edu/RESEARCH/sample_research/sampleres.php>.

[49] International Biometric Group, LLC. *International Biometric Group - Biometrics Market and Industry Report 2009-2014* [online]. c2003-2010 [cit. 2010-06-08]. Biometrics Market and Industry Report 2009-2014. Dostupné z WWW: <http://www.biometricgroup.com/reports/public/market_report.php>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D	Dvojrozměrný
3D	Trojrozměrný
AFIS	Automatizované systémy identifikace otisků prstů (Automated Fingerprint Identification Systems)
CODIS	Systém propojených DNA seznamů (Combined DNA Index System)
ČR	Česká republika
DARPA	Agentura pro výzkum pokročilých obranných projektů (Defense Advanced Research Projects Agency)
DNA	Deoxyribonukleová kyselina (Deoxyribonucleic Acid)
ED	EyeDentify, Inc.
FAR	Míra chybného přijmutí neoprávněného uživatele (False Acceptance Rate)
FBI	Federální úřad pro vyšetřování (Federal Bureau of Investigation)
FRR	Míra chybného odmítnutí oprávněného uživatele (False Rejection Rate)
HW	Hardware (technické vybavení PC)
IAFIS	Integrované automatizované systémy identifikace otisků prstů (Integrated Automated Fingerprint Identification Systems)
IR	Infračervené záření (Infrared)
IS	Informační systém
ISBN	Mezinárodní standardní číslo knihy (International Standard Book Number)
JPEG	Joint Photographic Experts Group
kB	kilobyte
MHD	Městská hromadná doprava
n. l.	Našeho letopočtu
OCR	Optické rozpoznávání znaků (Optical Character Recognition)
OKTE	Odbor kriminalisticko-technických expertíz

PC	Osobní počítač (Personal komputer)
PIN	Osobní identifikační číslo (Personal Identification Number)
př. n. l.	Před naším letopočtem
RFID	Identifikace na rádiové frekvenci (Radio Frequency Identification)
RZ	Registrační značka
SW	Software (programové vybavení PC)
UNHCR	Komise pro uprchlíky Organizace spojených národů (United Nations High Commissioner for Refugees)
USA	Spojené státy americké (United States of America)
VB	Velká Británie
VIN	Identifikační číslo vozidla (Vehicle Identification Number)
VIP	Velmi důležitá osoba (Very Important Person)
WSQ	Wavelet Scaler Quantization

SEZNAM OBRÁZKŮ

SEZNAM TABULEK