Identifikační biometrické prostředky

Roman Ondrůšek

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2005/2006

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Roman ONDRŮŠEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Identifikační biometrické prostředky**

Zásady pro vypracování:

1. **Historie vývoje biometrických údajů**
2. **Základní členění biometrických údajů a jejich použití**
3. **Techniky zpracování biometrických údajů**
4. **Současný stav a perspektivy požadavků na využití biometrických údajů**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

Laucký L. Technologie komerční bezpečnosti I. Skripta UTB
Čandík M. Objektová bezpečnost II. Skripta UTB
Jan Uhlář Technická ochrana objektů II. Díl – Elektrické zabezpečovací systémy Skripta Policejní akademie České republiky
Stanislav Křeček a kol.: Příručka zabezpečovací techniky Tiskárna Blatná, vydání 2.

Vedoucí bakalářské práce:	**Ing. Mgr. Milan Kvasnica, CSc.** Ústav elektrotechniky a měření
Datum zadání bakalářské práce:	**14. února 2006**
Termín odevzdání bakalářské práce:	**13. června 2006**

Ve Zlíně dne 14. února 2006

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Bakalářská práce pojednává o přístupových systémech používaných na identifikaci osob, kterých použití v současné době je v souvislosti s nárůstem terorizmu vysoce aktuální. V práci se pojednává o současném stavu v oblasti biometrických systémů, zejména jakými způsoby je možné identifikovat osobu pomocí biometrických údajů. Jsou uvedeny metody, které se v současné době zatím jen testují, ale nicméně je jim věnována velká pozornost. Závěrem je uvedeno několik novinek v oblasti biometrie, které se využívají k ochraně osobních údajů a ochraně proti zneužití mobilních telefonů.

Klíčová slova: Přístupové systémy, biometrie, biometrické údaje, identifikační systémy.

ABSTRACT

This bachelor thesis deals about the access systems for the identification of competent persons, highly up date due to increased danger of terrorism. There is described current state of the art in the field of biometric systems, namely, the methods for the identification using biometric data. Final, there are described perspective methods, just tested in current time due to significant impact, namely the use of biometric data for the protection of personal database systems and against the misuses of mobile phones.

Keywords: Access systems, biometrics, biometric data, identification systems.

Tímto si dovoluji poděkovat svým rodičům za morální a finanční podporu při studiu. Také vyjadřuji své poděkování Ing. Mgr. Milanu Kvasnicovi, CSc. za kvalitní odborné vedení, připomínky a poskytnuté konzultace při zpracování mé bakalářské práce.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Problematika spolehlivé identifikace neboli rozpoznávání osob patří v současné době, zejména v souvislosti s ochranou osobních dat a narůstajícím terorizmem k vysoce aktuálním tématům. Identifikace osob se používala již v dávných dobách, ale za použití jednoduchých metod, které spočívaly především v rozpoznávání osob podle vzhledu a obličeje. Postupem času došlo v této oblasti k několika zdokonalením jednotlivých identifikačních metod a tím některé z nich získaly svoji současnou podobu. V souvislosti s rozvojem lidské civilizace potřeba spolehlivé identifikace osob výrazně vzrostla a dnes při použití počítačů, se tento problém dotýká každého z nás.

Cílem této práce je přiblížit současné možnosti využití identifikace osob pomocí identifikačních biometrických prostředků, které se stále víc stávají součástí každodenního života.

1 PODSTATA A POJEM BIOMETRIE

Biometrie či biometrika jsou pojmy v poslední době frekventovaně používané zejména v souvislosti s identifikací osob při zajištění vnitřní bezpečnosti, ochrany osob, majetku, různých objektů a identifikací osob oprávněných ke vstupu či k ověření totožnosti při kontrolách na hranicích. Pokud si klademe otázku, co to vlastně biometrie je, jednoduchou úvahou a volným překladem slova složeného z řeckých základů „*bios*“ a „*metric*“ dojdeme k závěru, že se jedná o pokus měřitelnosti živých organismů, resp. v živých organismech. Obecně lze tedy říci, že biometrická identifikace je využití jedinečných měřitelných fyzikálních nebo fyziologických znaků (tzv. markantů) nebo projevů člověka k jednoznačnému identifikaci nebo verifikaci jeho identity.

Zatímco při ***verifikaci*** uživatel nejprve zadá svoji totožnost (např. pomocí identifikační karty), poté se sejmou jeho biometrická data, ze kterých se extrahují charakteristické rysy a ty se následně porovnají s referenční šablonou uloženou v systému pro daného uživatele; při ***identifikaci*** uživatel nepředkládá svoji totožnost, ale rovnou se sejmou a zpracují jeho biometrické charakteristiky. Poté je na systému, aby prohledal svoji databázi, každou uloženou šablonu porovnal s aktuálně získaným vzorkem a pokusil se nalézt shodující se záznamy. Je zřejmé, že identifikace jako proces porovnávání dat je časově i výpočetně mnohem náročnější proces než verifikace, který představuje uložení dat.

Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik a jejich následné porovnávání s údaji obsažených v předem vytvořené databázi. Realizace biometrických identifikačních metod vyžaduje jednak hardware (čtecí zařízení, kamery, mikrofony, optická čidla atd.), který snímá biometrické charakteristiky a převádí je do elektronické podoby, a jednak software, který sejmutá data převádí do žádané podoby, která zajišťuje technologičnost identifikačního zpracování a provádí vyhodnocení. Biometrické systémy se skládají z několika logických bloků, které jsou znázorněny na obr.1. Současné biometrické systémy využívají nejrůznější snadno rozlišitelné znaky pomocí kterých lze rozpoznat jedince od množiny ostatních lidí. Biometrické technologie jsou nyní prostředkem k dosažení rychlé a uživatelsky pohodlné autentizace s poměrně vysokým stupněm přesnosti. Jejich předností je skutečnost, že ověření identity osoby

s vysokou pravděpodobností nelze přenést na nikoho jiného, ukrást nebo oklamat. Na základě měřitelnosti těchto vlastností je proto možné osoby od sebe navzájem rozeznat.

Je také nutné si také říci, že autentizace, neboli ověřování totožnosti uživatele před povolením vstupu, má tři podoby, a to:

- **Autentizace heslem** – založená na znalosti hesla, které uživatel musí zadat přístupovému systému, žádá-li o povolení vstupu do chráněného prostoru. Výhodou této autentizace je její jednoduchá technická a programová realizace. Avšak mezi největší nevýhody patří zejména možnost snadného odchycení hesla, a proto se tento přístup používá hlavně v prostorách s minimálními bezpečnostními prvky.
- **Autentizace předmětem** – založená na vlastnictví určitého identifikačního předmětu, obecně nazývaného token, jenž by měl být jedinečný a obtížně padělatelný. Autentizace předmětem poskytuje z hlediska bezpečnosti vyšší úroveň zabezpečení než autentizace heslem. Mezi největší nevýhody však patří zejména to, že autentizační předmět může být odcizen, čímž se může kdokoliv vydávat za někoho jiného. Z hlediska používaných autentizačních předmětů je možné tokeny rozdělit na:
  - *tokeny paměťové* – magnetické, elektronické nebo optické karty, které jsou obdobou mechanických klíčů
  - *tokeny udržující heslo* – vydají určený kvalitní klíč po zadání jednoduchého uživatelského hesla
  - *tokeny s logikou* – umějí zpracovávat jednoduché podněty typu: vydej následující klíč, vydej cyklickou sekvenci klíčů, apod.
  - *inteligentní tokeny* – tzv. smart cards - mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu, mohou šifrovat, generovat náhodná čísla, apod.
- **Biometrická autentizace** – založená na biometrických charakteristikách člověka

Dříve než lze pomocí biometriky ověřit identitu jedince, je nutné nejprve sejmout šablonu (etalon) zvolené charakteristiky. Tato šablona je uložena v databázi a slouží jako referenční údaj pro účely následného porovnání se vzorkem sejmutým v okamžiku

identifikace. Bývá sejmuto větší množství šablon (obvykle tři), aby bylo možné vytvořit reprezentativní vzorek (např. jejich zprůměrováním). Následně je k šabloně přiřazen identifikátor, který je zpravidla v podobě rodného čísla, PIN kódu, čísla čipové karty nebo počítačového přihlašovacího jména (loginu). Tento proces sejmutí a ukládání šablon je klíčovým faktorem v celém procesu a má zásadní vliv na úspěšnost aplikace biometrických metod. Při ukládání šablon je důležitou otázkou, jakým způsobem jsou tyto šablony ukládány.

V zásadě existují čtyři možnosti:

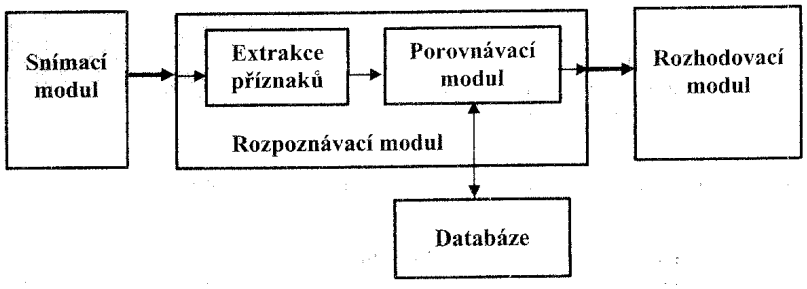
- **Uložení šablon v biometrickém čtecím zařízení**
  - výhodou této možnosti je rychlá reakce a nezávislost na externích procesech
  - nevýhodou je, že šablony jsou závislé na přítomnosti a funkčnosti daného čtecího zařízení
- **Uložení šablon v centrální databázi**
  - u této možnosti je potřeba myslet na to, že jakmile je síť mimo provoz, je biometrický systém vyřazen z činnosti a je třeba mít pro tento případ v záloze náhradní systém
- **Uložení šablon v přenosném prvku (např. čipová karta)**
  - tato možnost nevyžaduje žádné lokální nebo centrální ukládání šablon, protože uživatel si nosí svoji šablonu s sebou a může ji použít všude tam, kde má povolen autorizovaný přístup
  - nevýhodou je vyšší pořizovací cena a složitost biometrického systému
- **Libovolná kombinace předchozích způsobů**
  - tato možnost může poměrně efektivně eliminovat nevýhody jednotlivých samostatných možností a používá se všude tam, kde je kladen důraz na funkčnost systému za všech okolností

Biometrické identifikační systémy pracují ve dvou režimech:

- **registrační režim** – biometrická data jsou získána použitím biometrických detektorů a jsou uložena do databáze. Uložená identifikační data jsou označena identifikací uživatele (např. jméno, identifikační číslo…) pro umožnění autentizace uživatele.

- **autentizační režim** – slouží k identifikaci osoby na základě porovnání snímaných biometrických dat s biometrickými daty uloženými v databázi.

Tradiční techniky, např. přístupové heslo nebo čipová karta, jsou založeny na znalosti hesla nebo vlastnictví určité věci. Biometrie naproti tomu využívá k autentifikaci uživatele anatomicko - fyziologické (otisk prstu, sítnice) nebo jiné, např. behaviorální charakteristiky (podpis, řečová analýza). Tím se získají nejenom charakteristiky vztahující se k dané osobě, ale charakteristiky přímo s ní svázané. Důvody, proč se lidé snaží předstírat jinou než vlastní identitu, jsou různé. Ve většině případů se především jedná o prospěch finančního charakteru, snahu o získání citlivých informací nebo skrytí vlastní identity. S využitím biometrických metod je možné tuto bezpečnostní mezeru vyplnit. Biometrické metody identifikace se mohou stát vzhledem k nákladům a výkonnosti alternativou k jiným zabezpečovacím mechanismům nebo je vhodným způsobem mohou doplňovat. Cílem je rovněž postupně vytvořit komplexní biometrický bezpečnostní systém založený na současné analýze několika různých biometrických charakteristik.



Obr. 1: *Princip činnosti biometrických identifikačních systémů*

Popis jednotlivých logických bloků biometrických identifikačních systémů:

- **Snímací modul** – slouží k snímání biometrických dat uživatele
- **Rozpoznávací modul** – obsahuje:
  - *modul pro extrakci příznaků* – pro identifikaci uživatele se neužívají všechny snímané informace, ale jen některé jejich významné části (tzv. příznaky). S extrahovanými příznaky se uskutečňují různé matematické operace, na jejichž základě se uskutečňuje jednoznačná identifikace osoby.

  - *porovnávací modul* – na základě získaných příznaků biometrických dat uživatele se uskutečňuje porovnání s daty uloženými v databází.
- **Rozhodovací modul** – uskutečňuje závěrečné rozhodnutí o tom, zda-li jsou snímaná biometrická data uživatele totožná s biometrickými daty uloženými v databázi.

1.1 Proč zvolit právě biometrickou identifikaci?

Stávající biometrické systémy „identifikují“ přímo člověka, nikoli předměty, kódy či hesla. Používají se všude tam, kde je třeba zajistit vysokou spolehlivost, transparentnost, bezpečnost a zároveň jednoduchost a komfort. Biometrický průmysl se proto stále více zaměřuje na počítačově snazší a poměrně rychlou verifikaci oprávněných osob. Magnetické nebo čipové karty, identifikační karty i klasické domovní klíče mohou být ztraceny, odcizeny nebo zkopírovány. Hesla nebo PIN kódy mohou být zapomenuty, odpozorovány nebo sdíleny více uživateli. U všech biometrických systémů je nutné, aby procesu identifikace nebo ověření identity byla daná osoba fyzicky přítomna. V případě, že je vyžadována vysoká úroveň zabezpečení systému, lze biometrii s výhodou použít i v kombinaci s jinými metodami autentizace, jako je heslo/PIN nebo čipová karta. Ovšem největší předností biometrie oproti jiným metodám je její jednoznačnost. Charakteristické rysy každého člověka jsou unikátní a žádní dva lidé nemají například shodné otisky prstů, a to ani v případě, že se jedná o jednovaječná dvojčata. Mimo to jde především o rychlost, určitý stupeň spolehlivosti daný nezaměnitelností vlastností toho kterého jedince, ale také neustálá možnost zdokonalování od systémů založených na jedné vlastnosti až po kombinaci několika z nich.

Spektrum použití biometrických systémů je značně široké a uplatnění nacházejí v nejrůznějších oblastech (obr.2). Nejběžnější jsou systémy pro fyzické přístupy do budov (například jako náhrada za klasické klíče a sloužit tak k otevření dveří domů, bytů či kanceláří) nebo k informacím (tj. autorizaci přístupu do počítačových sítí, pracovních stanic nebo pro zpřístupnění klientského účtu v bankomatech), dále jako kontrola totožnosti nebo ochrana dat. Biometrii lze využít i v souvislosti s elektronickým podpisem, kde může sloužit k omezení přístupu k soukromému klíči uživatele. Ve státní správě nachází biometrie uplatnění v soudnictví a soudním vyšetřování při identifikaci pachatelů, při zabezpečení věznic nebo na letištních terminálech. Příklady využití biometrických

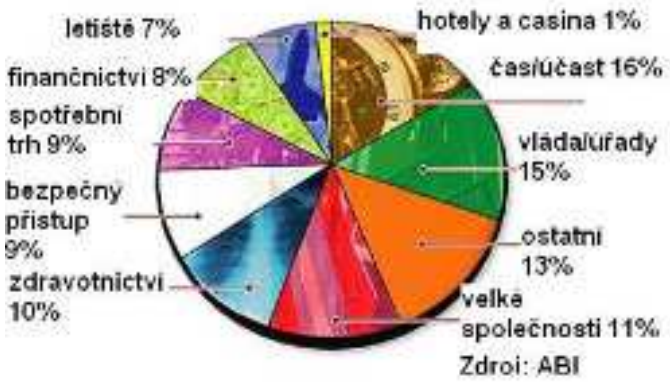
identifikačních systémů v bezpečnostní i civilní oblasti jsou uvedeny v tab. 1. Biometrický systém, který vyhovuje pro jednu aplikaci, však nemusí být vždy vhodný pro aplikaci jinou. Naštěstí existuje více typů biometrických systémů, i když s jejich rostoucí složitostí klesá ve světě počet výrobců, kteří se zabývají výrobou příslušných systémů.

Bezpečnostní oblast	**Oblast státní správy**	**Výpočetní technika obecně a komerční sféra**
• Kriminalistika • Boj proti zločinu obecně • Osoby v pátrání a pohřešované • Vězeňství • Sledování zájmových osob • Fyzická ostraha a zabezpečení strategických objektů (letiště, přístavy, nádraží, vojenské nebo režimové objekty, nákupní centra, pošty, banky, vládní instituce) • Zpravodajství	• Vydávání řidičských oprávnění, osobních dokladů, ID karet, pasů a víz • Zdravotní pojištění • Sociální pojištění • Oprávněnost přistupovat k volbám, účastnit se referenda, sčítání lidu atd. • Zdravotnictví • Školství	• Bankovnictví, finančnictví a pojišťovnictví • Personální agendy • Přístup k prostředkům počítačových informačních systémů a telekomunikačních zařízení • Obecná ochrana proti podvodům a zpronevěrám • Řízení přístupu k platebním kartám a bankomatům • Identifikace zákazníků, zaměstnanců, návštěvníků • Zvýhodněné služby pro stálé zákazníky • Elektronické transakce, elektronický podpis • Různé služby a marketing

Tab. 1: *Oblasti využití biometrických identifikačních systémů*

I přes všechny tyto vlastnosti mají biometrické systémy jedno společné, a to, že v současné době ještě neumožňují stoprocentní jistotu při rozpoznání. Člověk se totiž v průběhu života mění, a tomuto procesu podléhají i zdánlivě neměnné znaky. Při poměrně nízké hladině tolerance systému stačí i malá změna k tomu, aby systém hlásil chybu. Z

některých zkoušek současných biometrických systémů vyplývá, že míra jejich chybovosti může dosahovat až dvouciferný procentuální podíl.



Obr. 2: *Oblasti využití biometrických systémů*

1.2 Biometrie a EU

Před nedávnem EU rozhodla, o povinnosti standardní implementace čipů s biometrickými daty do pasů, konkrétně otisky prstů a obraz (sken) oční duhovky. Evropa tímto krokem také splnila požadavek americké strany, která od zemí bez vízové povinnosti požaduje biometrické identifikátory v pasech od října roku 2005. Podobně EU bude od následujícího roku požadovat od všech návštěvníků pocházejících ze zemí mimo EU otisk prstu ve vízu a také v povolení k pobytu, pokud cizinci žijí na území některé členské země. Pomocí kombinace otisků prstů a fotografie se má zamezit zneužití dokladů a také zvýšit bezpečnost. Proti přepsání nebo smazání budou tato citlivá data zajištěna elektronickým podpisem. Znamená to také nutnost sjednotit používané biometrické systémy v souladu s jednotnou evropskou politiku.

1.3 Biometrická identifikace policejně-soudní, bezpečnostně-komerční a ezoterická

Podle přesnosti, spolehlivosti a objektivnosti metody identifikace a z ní vyplývajícího způsobu použití, lze biometrické identifikační metody rozdělit na identifikaci (verifikaci):

- policejně-soudní (forenzní)
- bezpečnostně-komerční
- ezoterickou

1.3.1 Policejně-soudní (forenzní) identifikace

Metody policejně-soudní (forenzní) identifikace patří k nejnáročnějším a nejspolehlivějším a jsou dlouhodobě prověřené na základě velkého množství zkoumaných vzorků. Používané metody zaručují jednoznačnou totožnost osoby mezi stamiliony jedinců. Ke zpracování se používají laboratorní a počítačové technologie se speciálním softwarovým vybavením. **Základním rysem policejně-soudní identifikace je, že výsledek vždy vyhodnocuje člověk.**

Vědecká policejně-soudní identifikace je používána zhruba sto let a byla odstartována a dále intenzivně rozvíjena až kriminalistickými potřebami a vědeckými poznatky 20. století. Mezi používané metody biometrické identifikace patří daktyloskopie (identifikace na základě otisků prstů, dlaní a chodidel), analýza DNA a analýza lidského hlasu. Ve forenzních aplikacích **převažuje identifikace nad verifikací**.

Softwarové a hardwarové vybavení je finančně nákladné a náročné na provozní údržbu, a proto je koncentrováno pouze do několika málo centralizovaných pracovišť (kriminalistické ústavy, soudně-laboratorní instituce apod.). Všem oprávněným uživatelům je však umožněn vzdálený přístup pro vkládání i vyhodnocování informací.

1.3.2 Bezpečnostně-komerční identifikace

Bezpečnostně-komerční identifikace je historicky odvozena od identifikace policejně-soudní. Slovo *bezpečnostní* zde vyjadřuje obecné bezpečnostní potřeby, pro které je identifikace používána (zejména počítačová bankovní bezpečnost a ochrana citlivých osobních údajů). Slůvko *komerční* pak znamená, že používané biometrické technologie jsou dostupné na specializovaném trhu.

Řada metod používaných v kriminalistice a dalších bezpečnostních oborech byla upravena pro bezpečnostní a komerční využití. Některé z nich byly podstatně zjednodušeny, některé naopak zase více hlouběji rozpracovány. Důvodem bylo jejich široké průmyslové a komerční nasazení. Důsledkem toho v komerční sféře vzniká velké množství aplikací, které jsou zpětně využitelné i pro policejně-soudní identifikační potřeby.

Na rozdíl od policejně-soudní identifikace, **jsou bezpečnostně-komerční aplikace zcela automatizované.** U těchto aplikací spíše **převládá verifikace nad identifikací**. Přesnost (citlivost) bezpečnostně-komerčních metod je obecně nižší než u metod policejně-soudních.

V bezpečnostně-komerční biometrické identifikaci se v současné době používají metody založené na poznatcích o daktyloskopii, o oční duhovce a sítnici, anatomických rozměrech a závislostech dlaně a prstů, tvarech obličeje, projevech hlasu a dovednosti psaní (především podpis a psaní na klávesnici). Tyto technologie jsou díky svému plošnému nasazení podstatně levnější než technologie policejně-soudní.

1.3.3 Ezoterická identifikace

Pod označením „ezoterická identifikace“ je uvedena poslední skupina biometrických identifikačních metod. Patří sem metody, které v praxi nejsou zatím běžně známé, či rozšířené a dostatečně prověřené na rozsáhlém souboru testovaných případů. Prozatím se nepoužívají pro bezpečnostně-komerční aplikace, ale v určitých případech jsou v zahraničí využívány pro policejně-soudní potřeby. Nicméně jsou to metody, kterým je věnována mimořádná pozornost a časem se mohou stát rovnocennými partnery pro soudní nebo bezpečnostně-komerční identifikaci.

Mezi ezoterické identifikační metody se řadí lokomoce (typické rysy lidské chůze), tvar vnějšího ucha, otisky rtů a pórů, topografie žil, termovizní obrazy, pach lidského těla, obsah solí v lidském těle a v poslední době zejména identifikace na základě podélného rýhování nehtů ruky, které lze vyhodnocovat podobně jako čárové kódy.

1.4 Propojení biometrie a bezpečnosti

Dnes je stále více patrné, že rostoucí obavy z bezpečnostních rizik, zejména mezinárodního terorizmu vedou mezinárodní, národní (vládní) i soukromé instituce k využívání co nejkvalitnějších systémů zabezpečujících přístupy na svá území a jiná teritoria, do různých objektů či informačních systémů obsahujících strategické údaje. Z tohoto pohledu jsou za nejmodernější způsob k ověřování totožnosti a „identifikace“ oprávněných osob považovány právě moderní biometrické identifikační systémy.

Ovšem je nutné si také říci, že u všech existujících biometrických systémů, tzv. měření fyzických znaků, ať ve formě manuální nebo ve formě plně automatizované, vždy souvisí i s určitými omezeními osob na jejich právech. Všechny původní i stávající biometrické systémy jsou spojeny nejen s tělesnými a behaviorálními znaky člověka, ale také s jeho osobními údaji. Proto ve spojitosti s biometrickými systémy zákonitě vystupují do popředí vždy i problémy související s ochranou osobních údajů. S rozšiřujícím se zaváděním a využíváním biometrických systémů v každodenním životě je stále více diskutována otázka zásahů do soukromí, a s tím spojená omezení základních práv občanů.

Názory na to jsou různé. Buď chceme zaručit bezpečnost, pak je ovšem třeba něco slevit ze svých práv. Anebo si svá práva a svobody chceme ponechat, ale pak bohužel nebude možno zaručit bezpečnost. Oba tyto názory mají svá pro i proti a je těžké z nich vybrat to nejsprávnější rozhodnutí. V této souvislosti i biometrie bude muset na své cestě nacházet řadu kompromisů. Jde především o rozumný kompromis mezi tím, čemu zpravidla slouží (tedy např. kriminalistice, boji proti kriminalitě a terorismu, ochraně bezpečnostních systémů apod.), a mezi právem občanů na soukromí a na ochranu osobních údajů, které někdy může být biometrií narušeno. Tento problém je při současném rozmachu biometrie na jedné straně a při růstu terorismu na straně druhé stále naléhavější.

Naprosto nebývalý ohlas jsme v této oblasti mohli zaznamenat, takřka ve všech sdělovacích prostředcích, po teroristických útocích na Světové obchodní centrum v New Yorku 11. září 2001. Z tohoto pohledu je nyní využití biometrie a na jejím principu založených plně automatizovaných systémů považováno mnohými světovými specialisty na bezpečnost a některými politiky za jeden z nejmodernějších a nejúčinnějších prostředků strategie boje proti terorismu.

V rámci protiteroristických opatření v celém světě proto podmínky pro zavádění a využívání biometrie našly oporu také v řadě národních či mezinárodních dokumentů (deklarací, smluv, zákonů, opatření apod.). Současně s tím se obecně zvýšil i zřetelný tlak na to, aby technické prostředky založené na využití biometrie byly co nejrychleji a nejintenzivněji zaváděny do praxe.

Opatření v oblasti strategie boje proti terorismu a všeobecné zajištění vnitřní bezpečnosti za použití technik rozpoznávání fyziologických znaků osob, odstartovala nebývalý boom ve vývoji a využívání nových biometrických systémů a prostředků v

komerční sféře. Někdy se v této souvislosti dokonce hovoří i o „biometrickém průmyslu“. Firmy, které se specializují na vývoj a výrobu biometrických systémů reagovaly na vzniklou situaci okamžitě a připravují realizace nových projektů a testují nové technologie. Z toho všeho je nepochybné, že mezinárodní terorismus a teroristé tak svými akcemi nevědomky odstartovali mimořádný rozvoj biometrie.

Z hlediska vnitřní bezpečnosti, ochrany života a zdraví osob, ochrany majetku a objektů představuje dnes biometrie skutečně významný fenomén v životě téměř každé země. V boji proti terorismu může sehrát jako jedno z opatření dosti podstatnou roli. Přitom je však třeba respektovat skutečnost, že i když se pojmy biometrika, biometrie nebo biometrické systémy v kriminalistice v podstatě nevyskytují, hraje měření znaků osob i dnes v kriminalistice a především v kriminalistické identifikaci rozhodující poslání. Pokud se v souvislosti se zajištěním uvedených hodnot a svobod občanů rozhodne o zavedení a „měření“ nějakého nového biometrického znaku, nelze tak učinit bez odpovídajícího zajištění vybavenosti těch policejních pracovišť, která provádějí důkazní kriminalistickou identifikaci.

1.5 Některé aspekty zavádění biometrie v ČR

V květnu roku 2003 pojala vláda ČR biometrii jako součást postupu v boji proti terorismu v souladu s evropskými opatřeními. Obecně nelze vyloučit, že v důsledku požadavků na zajištění vnitřní bezpečnosti může dojít k zavedení některých nových a efektivnějších biometrických systémů. V aktualizovaném Národním akčním plánu boje proti terorismu (usnesení Vlády ČR č. 479 z 19. 5. 2004), resp. v jeho příloze, proto mimo jiné ukládá ministerstvu vnitra a ministerstvu zahraničních věcí *„zkušebně provést snímání biometrických údajů. V první etapě se jedná o digitální sejmutí podoby žadatele a digitální sejmutí podpisu ze žádosti. Ve druhé etapě pak vláda stanoví, v návaznosti na doporučení EU, zajistit možnost digitálního sejmutí otisku prstu, popřípadě dalšího doporučeného biometrického údaje žadatele o cestovní doklad“*. Posledním úkolem je *„na základě doporučení EU zajistit změnu příslušných zákonů a následně i konstrukci příslušných dokladů tak, aby umožnily bezkontaktní kontrolu biometrických údajů“*.

Takový doklad by pak měl obsahovat digitální fotografii obličeje (ve formátu JPG) a otisk prstu svého držitele. Otisky prstů mají pořizovat pracovníci na obecních úřadech obcí s rozšířenou působností, avšak žádná centrální databáze na tomto základě zřizována nebude.

Digitální podoba obličeje by se měla snímat nejpozději v srpnu letošního roku, otisky prstů pak do poloviny roku 2008. Nařízení se týká pouze nově vydávaných dokladů, stávající pasy zůstanou v platnosti po dobu, která je v nich uvedena. Tyto pasy lze samozřejmě používat až do konce doby jejich platnosti. Nadále by bylo možné žádat o cestovní pas platný maximálně jeden rok, který by úřady vydávaly ve zkrácené lhůtě. Takový doklad již biometrické prvky obsahovat nebude.

Zavedení cestovních pasů s biometrickými údaji patří také mezi podmínky, které stanovily Spojené státy americké pro rozhodování o tom, zda bude pro občany České republiky cestujících do zámoří zaveden bezvízový styk.

Principiální otázkou zásad a vlastního zavedení biometrie však je to, jak bude případně v praxi řešen problém, když při kontrole cestovního dokladu s biometrickými údaji (uloženými na RFID čipu) bude zjištěn rozdíl mezi těmito údaji a znaky osoby, která doklad předložila. Pak je tedy zřejmé, že musí nastoupit porovnání jiné, a to klasická kriminalistická identifikace.

Závěrem je tedy nutné si říci, že i když se neustále bezpečnostní opatření zdokonalují, stále ještě neexistuje žádná záruka proti jejich zneužití. Proto si musíme položit otázku, jak budou tato bezpečnostní opatření přijata veřejností a zda i přesto všechno je lidé přijmou a budou jim důvěřovat.

2 HISTORIE BIOMETRICKÝCH IDENTIFIKAČNÍCH PROSTŘEDKŮ

Přestože se v poslední době o biometrii hovoří převážně v souvislosti s počítačovou bezpečností, její počátky sahají hluboko do minulosti. Z literatury je například známo, že první poznatky o biometrii a používání tohoto termínu jsou odbornou veřejností

registrovány již v první polovině 19. století, avšak její jasné definování jako pojmu je spojeno až s rozvojem statistiky a biologie koncem 19. století.

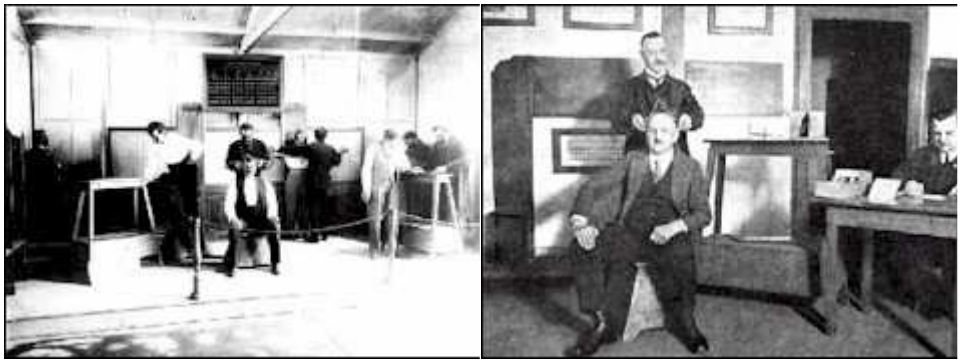
Ze všech dnes používaných biometrických technologií je nejznámější metodou otisk prstu. Znalost o existenci papilárních linií na lidské kůži se objevuje u celé řady civilizací. Například indiánské kmeny, které obývaly území dnešního státu Indiana v období několika tisíc let před naším letopočtem, za sebou zanechaly kameny s rytými obrazy, tzv. "**petroglyfy**", znázorňující lidskou ruku s vyznačenými papilárními liniemi (obr.3). Proč však tyto obrazy vznikly se doposud nepodařilo zjistit.

Také u Asyrské civilizace byly nalezeny pozůstatky otisků prstů, a to zejména ve zříceninách starověkého asyrského města Ninive, kde byla objevena část slavné Aššurbanipalovy knihovny založené již v 9. století před naším letopočtem. Na nalezených úlomcích hliněných tabulek se kromě rozličných textů nacházely také otisky prstů, ale v tomto případě se spíše jednalo o zamezení falzifikování tabulek, kdy autor pravděpodobně umístil svůj otisk vedle svého jména. Obdobné užití otisků prstů se prokázalo i na keramice nalezené při archeologických vykopávkách v Egyptě, v Řecku a na území Římského impéria.

Obr. 3: *Kámen datovaný do období kolem roku 2000 př. n. l. s naznačenými papilárními liniemi*

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

Moderní historie biometrie se však datuje od roku 1882. S tímto datem je především spjato jméno zakladatele vědecké kriminalistiky, průkopníka kriminalistické fotografie a první kriminalisticko - technické laboratoře policie na světě, antropologa a šéfa oddělení identifikace pachatelů pařížské Suréte (kriminální policie) Louise Alphonse Bertilliona (obr.5a). Jeho objevy, byť některé již dávno překonané, patří dnes neoddělitelně ke klasické vědecké kriminalistice. Bertillion hledal nějaký způsob, který by mu umožnil identifikovat již jednou odsouzené zločince. Problém s opakovaně vezněnými zločinci spočíval v tom, že při každém novém zatčení udávali nové falešné jméno a úřady tak nebyly schopny jim jejich opakovanou recidivitu prokázat. Bertillion vynalezl metodu, která spočívala v měření fyzických znaků člověka a byla po něm nazvána **bertilionáž**. Především jeho zásluhou se biometrie stala reálným předmětem studia. Uvědomil si, že některé charakteristické tělesné rysy jako je velikost lebky nebo délka prstů zůstanou stále stejné, i když si dané osoby změní jméno, přiberou na váze nebo si nechají ostříhat či narůst vlasy. Vycházel přitom ze závěrů A. L. Quételeta, který v rámci svého statistického měření a výzkumu dospěl např. k závěru, že najít dvě osoby naprosto stejné výšky, se jedná pravděpodobnosti v poměru 4:1. Bertillionův Systém antropometrické identifikace, jak se jeho metoda oficiálně nazývala, se rychle rozšířil a záhy ho používali policisté a vyšetřovatelé po celém světě. Měření, která se prováděla v antropometrických laboratořích (obr.4) a při nichž autor připouštěl menší chyby, se zaznamenávala na antropometrické karty, které se řadily podle délky hlavy do tří tříd. K nim byla později přiložena fotografie zločinců zhotovované jednotným postupem (za stejných světelných podmínek, stejné vzdálenosti a ze dvou stran) a otisky čtyř prstů. Později tuto metodu ještě doplnil o podrobný popis obličejů zločinců, tzv. **portrait parlé**, provedený na základě přesně definovaných kritérií a jednotné terminologie. Po čase se však zjistilo, že někteří lidé mohou mít měřené míry shodné, a tudíž dva jedinci by mohli být považováni za jednoho a toho samého člověka. Z tohoto důvodu se systém Alphonse Bertilliona přestal užívat téměř tak rychle, jak rychle se zavedl. Nicméně se tento systém identifikace a jeho principy staly základem některých dosud používaných kriminalistických metod a postupů.



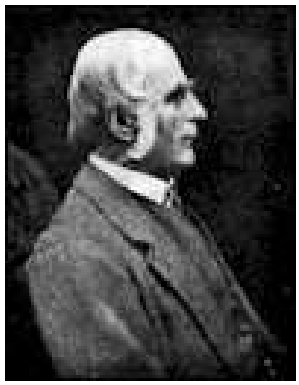
Obr. 4: *Ukázky měření v antropometrické laboratoři*

Biometrie samotná však v zapomnění neupadla. V květnu roku 1888 publikoval svoji práci anglický přírodovědec Francis Galton (obr.5b), v níž položil teoreticko - vědecké základy daktyloskopie, tj. vědy zabývající se otisky prstů. Galton, jako významný představitel a zakladatel moderní biometrie, je současně považován za tvůrce jednoho ze základních zákonů daktyloskopie, a to zákona o vyloučení možnosti výskytu dvou jedinců se stejným obrazem papilárních linií, k němuž došel na základě svých matematických propočtů, kdy vypočítal, že existuje celkem 64 miliardy různých variant uspořádání papilárních linií. Přitom vycházel pouze s obrazcem jednoho prstu. Daktyloskopie jako jedna z prvních a základních biometrických metod tak našla v kriminalistice, na rozdíl od bertilionáže, trvalé a nezastupitelné místo až do současné doby. Její postavení a využívání k identifikaci osob neohrozily ani takové nové biometrické technologie jako např. analýza DNA nebo scanování oční duhovky. Mimo to byl Galton také zakladatelem eugeniky (tj. vědy zaměřené na zlepšení genetické výbavy lidstva). S jeho jménem jsou spojeny i počátky výzkumu lidské inteligence a vnesení nového významného tématu do psychologie - studium individuálních rozdílů, a to především rozdílů ve schopnostech. Galton byl také jedním ze spoluzakladatelů časopisu Biometrika, založeného v roce 1901.

Další osobností, která se výrazně zasloužila o rozvoj biometriky, resp. daktyloskopie byl sir William James Herschel (obr.5c), který zavedl nový výplatní systém při svém pobytu v Indii, kdy každá vyplácená osoba musela potvrdit příjem peněz otiskem ukazováku a prostředníku pravé ruky na výplatní listinu. Zabránil tak podvodům a zároveň nasbíral množství materiálu ke zkoumání. Svoji metodu navrhl k využití ve věznicích, kde

by zamezila záměnám těžkých zločinců za tzv. lehké případy. Jeho návrhy však byly označeny za výplody fantazie a nikdy nebyly akceptovány.

(a) Louise Alphonse Bertillion (1853 -1914)



(b) Francis Galton (1822-1911)

(c) William James Herschel (1833-1917)

Obr. 5: *Významné osobnosti světové historie, které stály u počátků biometrických metod a zasloužili se o jejich vývoj*

Na problematice otisků prstů pracovalo mnoho dalších význačných osobností, mimo jiné Dr. Henry Faulds (1843-1930), Juan Vucetich (1838-1925) a také český přírodovědec Jan Evangelista Purkyně (1787-1869), který jako první popsal jednotlivé typy charakteristických kreseb papilárních linií na koncových článcích prstů a klasifikoval je do devíti různých vzorů. Rovněž upozornil na trojúhelníkové seskupení papilárních linií (tzv. deltu) jako na důležitý klasifikační znak.

V roce 1886 publikoval Joseph T. James z univerzity v Miami krátký článek s titulem *"Portrét palce"*, v němž vyvodil dvě hypotézy, na nichž dodnes stojí veškeré praktické využití metody otisku prstu. První předpokládala, že papilární linie na koncových článcích prstů se během života člověka nemění. Druhá hypotéza předpokládala, že žádní dva lidé nemají shodné obrazce papilárních linií. Ani pro jednu ze svých hypotéz však James neměl žádný konkrétní vědecky zdůvodnitelný důkaz.

I přes všechny počáteční problémy a odmítání se nakonec technika otisků prstů dočkala uznání a i po nástupu nových technologií, jako je DNA či oční duhovka, zůstává dodnes nejpoužívanější metodou při identifikaci a ověřování identity osob.

2.1 Genetika ve službách kriminalistiky

Kyselin deoxyribonukleová (dále jen DNA) se jako identifikační prvek používá v policejní praxi od druhé poloviny osmdesátých let. Vzorky DNA získané na místech činu ještě dnes v mnoha případech ovlivňují přešetření kriminálních případů starých desítky let. Struktura DNA je odlišná u všech lidí s výjimkou jednovaječných dvojčat a s věkem se nemění. Přesnost zkoumání DNA je důvodem pro stále širší využití této technologie i přesto, že získávání otisků DNA představuje poměrně náročnou a zdlouhavou proceduru. Tato metoda se zrodila jako vedlejší produkt výzkumu, zaměřeného na celkem jinou problematiku, a to na studium struktury lidského genetického materiálu, s využitím při diagnostice genetických onemocnění.

První písemnou zprávu o výsledcích genetických pokusů podal v roce 1866 profesor Johann Gregor Mendel, který již o rok dříve ukončil své pokusy a přednesl svou teorii na zasedání Přírodovědného spolku v Brně. Ve své době však jeho práce neměla vůbec žádný ohlas a byla dokonce zapomenuta. V roce 1953 byla objevena a vypracována chemická struktura DNA, jejímiž tvůrci byli americký biochemik a genetik James Dewey Watson a britský biolog Francis Harry Compton Crick. Oba vědci sestrojili strukturu DNA ve tvaru dvojité propletené spirály, spojené dvojicemi chemikálií, zvanými nukleotidy. Z jejich výzkumů později vyplynulo, že molekula je stále stejná bez ohledu na to, o jaký druh DNA jde.

V roce 1984 vypracoval britský genetik Alec Jeffreys metodu genetické identifikace známé pod hovorovým termínem "*DNA Fingerprinting*", neboli "*genetická daktyloskopie*" či "*genetické otisky*". Tato metoda byla vyvinuta s původní představou zjistit příznaky dědičných chorob, které by pak bylo možné s předstihem léčit. V roce 1986 byla poprvé Jeffersova metoda DNA Fingerprintingu využita také pro účely kriminalistiky.

Záhy se metoda analýzy lidské DNA pro kriminalistické účely rozšířila také do USA a dalších zemí. Na území České republiky byla poprvé uplatněna a později soudem akceptována v roce 1992. Pro kriminalistiku je významné, že zdroj DNA je specifický a nepodléhá žádným velkým změnám. To znamená, že z hlediska individuální identifikace lidského jedince jde o mnohem dokonalejší metody, něž metody, které pro tento účel dosud využívají znaky člověka dědičně podmíněné. V biologických stopách se DNA navíc zachovává v nedegradovaném stavu velmi dlouho, dokonce několik století.

V současné době umožňují metody analýzy DNA určit původ biologických stop s takovým stupněm jistoty, jaký poskytuje daktyloskopie a navíc je tato metoda identifikace jedním z nejrychleji se rozvíjejících oborů kriminalistické biologie. Vyvíjejí se stále citlivější a rychlejší techniky a vznikají další pracoviště, která je začínají používat. V kriminalistické praxi je pro tento druh zkoumání zaveden název "*molekulárně genetická expertiza a analýza DNA*".

Identifikace pomocí DNA, jedna z největších novinek moderní kriminalistiky, poněkud zastínila pozoruhodné pokroky klasické daktyloskopie. A snad i trochu neprávem. Otisky prstů totiž stále jsou a zřejmě i dlouho budou nejrychlejší a nejlevnější metodou identifikace osob.

Z dalších biometrických metod se v poslední době začíná rozšiřovat technologie založená na skenování oční duhovky. Algoritmus pro počítačové zpracování obrazu duhovky a pro jeho identifikaci vyvinul a v roce 1994 patentoval profesor John Daugman z Harvardské univerzity.

Mezi jedny z nejstarších a nejznámějších identifikací patří podpis. Ten je jako identifikační prvek používán celá staletí, ale do oblasti biometrických technologií spadá až metoda rozpoznání dynamického podpisu, která zkoumá způsob vytvoření autogramu, nikoliv jeho tvar.

V posledních letech se výzkum identifikace podpisu soustřeďuje na vícesložkové, nejvíce šesti-složkové silově-momentové snímače. Ty jsou schopné analyzovat dynamiku pohybu lidské ruky při podpisu pro tři osová posunutí a tří úhlová pootočení s podstatně vyšší spolehlivostí, než je tomu u klasického počítačového zpracování dvourozměrné obrazové informace získané pomocí videokamery s obrazovým CCD snímačem.

Identifikace založená na geometrii ruky patří k těm "starším" biometrickým technologiím. Původní systémy byly založeny na měření délky jednotlivých prstů, ale současné skenery vytvářejí 3D model ruky, který je následně redukován do devítibajtové podoby, která je porovnávána s uloženým vzorkem v databázi.

Vlastnosti cévního systému lidské sítnice jako možného identifikačního prvku jsou známy od třicátých let 20. století, ale první komerční produkt se podařilo uvést na trh až v roce 1984.

Známé a používané jsou také metody vycházející z rozpoznávání lidského hlasu, obličeje, dynamiky stisku kláves a mnoho dalších. Problémem těchto biometrických

technik, který brání jejich většímu rozšíření, zpravidla je, že nemusejí být zcela jedinečné a s větší či menší snahou je lze často obejít.

Biometrika má již nyní v informačních systémech své pevné místo. A v krátkém časovém horizontu se sní budeme setkávat stále častěji. Většina technických a technologických překážek je dnes již vyřešena, zbývá ještě dořešit a vyřešit vytvoření příslušných legislativních podmínek akceptovatelných veřejností.

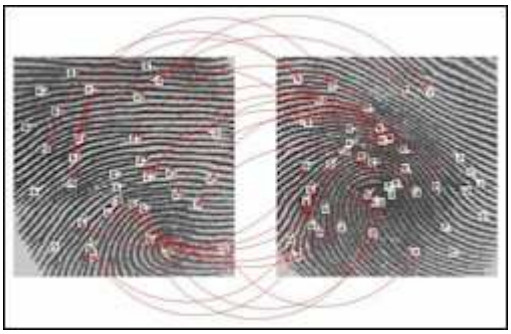
2.2 Počátky biometrie v kriminalistice

Biometrie si již ve svých raných počátcích našla nepopiratelné místo v řadě vědních oborů zabývajících se měřením živých organismů. Vedle pro ni tak typických oborů, zejména jako jsou statistika a biologie, je biometrie již od doby svého vzniku těsně spojena především s kriminalistikou. V této oblasti došlo za více jak sto let od vzniku biometrie a její implementace do tohoto vědního oboru k převratným změnám. Proto se také první poznatky o využívání metod moderní biometrie v kriminalistice datují zhruba do stejné doby jako její samotný vznik.

V tomto období se v kriminalistice využívaly biometrické metody nejčastěji ve formě měření zevních znaků těla osob poměrně jednoduchými měřícími metodami a prostředky, a to především pro účely identifikace osob (pachatelů) v souvislosti s trestním řízením. Účely využívání biometrie v kriminalistice se během doby v podstatě příliš nezměnily. Zcela jistě se ale změnily a rozšířily možnosti jejího využívání. Byla-li např. antropometrie a daktyloskopie při identifikaci pachatelů ve svých počátcích spojena s manuálními, velice pracnými, zdlouhavými a málo efektivními postupy, vývoj přinesl i v této oblasti zásadní kvalitativní změny. Ty jsou markantní zejména s rozvojem výpočetní techniky počátkem 60. let 20 století. Byly vyvinuty automatizované systémy pro identifikaci podle otisků prstů (obr.6) – tzv. systémy AFIS (Automated Fingerprint Identification Systems), které znamenaly výrazné zrychlení procesu identifikace podezřelých z rozsáhlých databází. První využití metody otisků prstů mimo sféru kriminalistiky umožnil až pokrok v oblasti osobních počítačů a optických snímačů v 80. letech minulého století. Začaly vznikat zařízení a aplikace, které kombinovaly techniku snímání otisků prstů s identifikačními kartami nebo zadáváním PIN kódu. K jejich masovému rozšíření v průběhu 90. let přispěl nástup levných optických snímačů a rychlých a spolehlivých srovnávacích algoritmů.

Komerční oblast se však zaměřila spíše na výpočetně snazší verifikaci uživatelů, zatímco mnohem náročnější identifikace zůstává doménou systémů AFIS.

Také metody, postupy a prostředky biometrie se samozřejmě v průběhu více než sta let postupně vyvíjely v závislosti na vědeckotechnickém pokroku a poznání v této oblasti. Některé z nich tak dnes poskytují svým způsobem nevídané možnosti.



Obr. 6: *Porovnávání jednotlivých charakteristických bodů dvou otisků prstů*

3 ROZDĚLENÍ BIOMETRICKÝCH IDENTIFIKAČNÍCH PROSTŘEDKŮ

Na základě biometrické identifikace osob lze biometrické charakteristiky každého jedince rozdělit na anatomicko - fyziologické a behaviorální (tj. týkající se chování):

Anatomicko-fyziologické biometrické charakteristiky – jsou využívány pro identifikaci nebo verifikaci osob na základě vědeckých poznatků o oční duhovce, oční sítnici, tváři, stavbě vnějšího ucha, otiscích prstů, dlaní a chodidel, geometrii prstů a ruky, topografii žil zápěstí, lidském tělesném pachu, obsahu solí v lidském těle, rozměrech a vahách lidského těla a skladbě DNA apod. Anatomicko-fyziologické biometrické charakteristiky jsou unikátní a časově stálé.

Behaviorální biometrické charakteristiky – jsou založeny na poznatcích o lidském hlase, pohybu těla – tzv. *lokomoce* (aktivní pohyb organizmů z místa na místo), o znalostech a dovednostech psaní. Rozlišuje se psaní souvislého textu, podpis osoby a dynamika psaní (úhozů) na počítačové klávesnici. Behaviorální biometrické charakteristiky

jsou unikátní a mohou být časově nestálé, mohou se změnit například po úraze, popřípadě po překonání některých onemocnění.

3.1 Základní rozdělení biometrických identifikačních prostředků

3.1.1 Identifikace podle otisků prstů

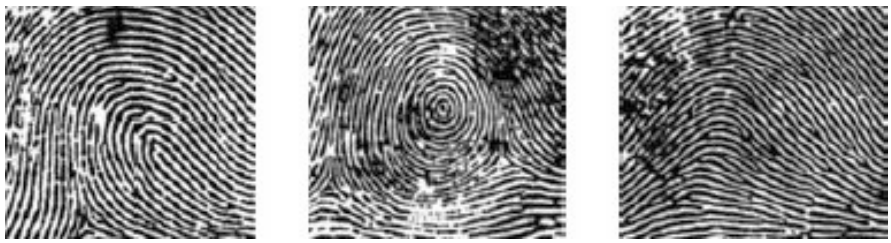
Vyhodnocování otisků prstů patří k nejstarší, nejznámější a nejrozšířenější biometrické metodě. Otisky prstů jsou nejvyužívanější způsob identifikace nejen v kriminalistice, ale i v běžném životě, a to zejména v různých bezpečnostních systémech, bankách, bezpečnostních službách apod. Tyto biometrické systémy poměrně rychle „identifikují“ oprávněnou osobu na základě předem vytvořeného referenčního vzorku v databázi a umožňují jí vstup do objektu, přístup do určitých systémů, přístup k určitým službám apod. Tato biometrická identifikace se řadí do skupiny daktyloskopických identifikací. Daktyloskopie představuje nauku o obrazech papilárních linií na vnitřních stranách článků prstů a dlaní člověka. Tvary papilárních linií, jejich průběh a směr jsou u jednotlivých osob odlišné.

Daktyloskopie využívá tzv. tři daktyloskopické zákony, které lze zjednodušeně definovat takto:

- na světě neexistují dva jedinci, kteří mají absolutně shodné obrazce papilárních linií
- obrazce papilárních linií jsou po celý život relativně neměnné
- obrazce papilárních linií jsou trvale neodstranitelné, pokud není odstraněna zárodečná vrstva pokožky

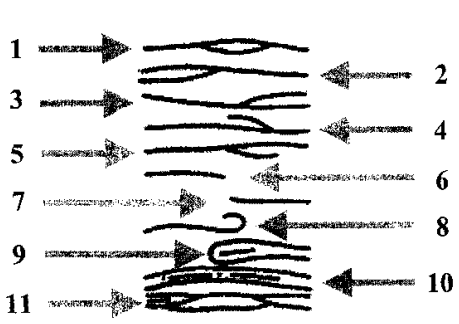
Vnitřní povrch prstů obsahuje vyvýšené drobné brázdovité útvary, které vytvářejí různé vzory. Tyto vzory se dělí do tří hlavních kategorií, a to **smyčky**, **přesleny** a **oblouky** (obr.7). Důležité je to, s jakou frekvencí se vyskytují. Například smyčky obsahuje 65% všech otisků, přesleny něco kolem 30% a oblouky jen asi 5% všech otisků. Obrazy papilárních linií se nemění celý život a není možné je odstranit.

Mezi nevýhody těchto systémů patří to, že např. drobné poranění prstu může být důvodem odmítnutí akceptace, a naopak, existuje možnost akceptace kopie prstu zhotovené ze silikonu anebo dokonce z potravinářské želatiny apod.



Obr. 7: *Základní klasifikační vzory - smyčka, přeslen a oblouk*

Kromě určení vzoru daktyloskopického otisku prstu je třeba ještě určit shodnost individuálních znaků, resp. zvláštnosti papilárních linií – markantů. Tyto body se nacházejí v rýhách vzoru. Za individuální znaky se považují zejména:



1. **Oko**
2. **Vidlice**
3. **Protividlice**
4. **Hák**
5. **Protihák**
6. **Končící linie**
7. **Začínající linie**
8. **Nedokončená smyčka**
9. **Vložená linie**
10. **Přerušovaná linie**
11. **Ostrov a spojená vidlice**

Obr. 8: *Individuální znaky*

3.1.1.1 Snímání otisků prstů

Každé zařízení, které obecně provádí jakékoliv vyhodnocení, je mimo jiné závislé na kvalitě vstupních dat. Nejinak je tomu i v případě automatizované identifikace osob založené na daktyloskopických otiscích. Snímání daktyloskopických otisků lze podle časové posloupnosti a technologie snímání rozdělit do dvou základních skupin, a to:

1. Klasické snímání daktyloskopických stop

2. Bezprostřední (interaktivní) snímání daktyloskopických otisků

Klasické snímání daktyloskopických stop

Jedná se o postupy používané bezpečnostními, zejména policejními (kriminálními) službami. Součástí tohoto procesu je vyhledávání daktyloskopických stop, jejich zviditelňování a přenášení do daktyloskopických evidencí. S rozvojem prvních počítačových aplikací sloužících k vyhodnocování otisků prstů, bylo nutné převést tyto data z papírových karet do elektronické podoby. Tento problém byl vyřešen až uplatněním klasických optických snímačů, které se staly běžnou součástí počítačů sloužících pro přenos daktyloskopických otisků do digitální podoby tak, jak je známe nyní.

Bezprostřední snímání daktyloskopických otisků

V současné době je tato skupina typická spíše pro aplikace, které mají komerčně-bezpečnostní charakter. U této metody není osoba bezprostředně v kontaktu se snímacím zařízením a zařízení je pouze mezičlánkem pro převod dat získaných jiným (klasickým kriminalistickým) způsobem do počítače k dalšímu automatizovanému zpracování. Pro bezprostřední snímání daktyloskopických otisků se v praxi užívá anglický termín live-scaning. Pod pojmem live-scaning se v praxi rozumějí všechny technologie snímání daktyloskopického otisku a jejich automatický převod do digitální podoby, s výjimkou metod používaných v klasické kriminalistice. V budoucnu lze očekávat, že bezprostřední snímání najde široké uplatnění i v aplikacích policejně-soudního charakteru, kde zatím převládá klasické snímání pomocí např. tiskařské černi.

Interaktivní snímání otisků prstů je realizováno pomocí snímačů. Snímače jsou zařízení pracující na různých fyzikálních principech a lze je podle způsobu kontaktu snímaného povrchu tkáně s daktyloskopickou kresbou rozdělit na:

- Snímače kontaktní
- Snímače bezkontaktní

3.1.1.1.1 Snímače kontaktní

Tato skupina snímačů zahrnuje mnoho fyzikálních způsobů snímání otisků prstů. Používají se zde technologie, které se používaly před více než třiceti lety, ale také technologie podstatně mladšího data. Patří sem snímače:

- Optoelektronické
- Kapacitní
- Teplotní
- Elektroluminiscenční
- Tlakové
- Elektronické

Optoelektronické snímače otisků prstů

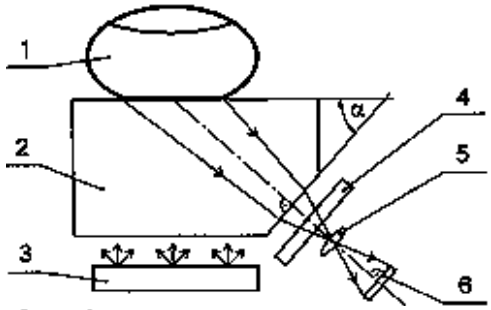
Technologie snímání pomocí optoelektronického snímače je asi nejkvalitnější a do budoucna nejlepší technologií pro toto odvětví. I když tento přístup není bez chyby, je odstranění chyb otázkou času.

Princip činnosti optoelektronického snímače (obr.9) je založen na získání otisku prstu pomocí principu rozdílného odrazu, resp. rozptylu světla na rozhraní snímací plochy hranolu a přiloženého prstu. Takovýto zdánlivý obraz otisku prstu, který je přiložen na plochu snímacího hranolu je zobrazen na maticový CCD detektor. Obraz otisku je následně digitalizován a předán ke zpracování algoritmem pro rozpoznávání obrazu.

Výhodou těchto snímačů je dostatečně velká snímací plocha, dobré rozlišení a dobrá kvalita obrazu. Proto jsou vhodné především pro algoritmy rozpoznání založené na markantech.

Nevýhodou tohoto typu snímače je, že otisk vytvořený na povrchu optického hranolu způsobuje problémy, protože zůstává na snímací ploše a u levných, nesprávně navržených snímačů dochází v dalším kole ku snímání části otisku předchozího žadatele společně s novým otiskem aktuálního žadatele. Pak dochází k automatickému zamítnutí žadatele, neboť jeho otisk nemůže souhlasit s žádným otiskem v databázi. Při testování těchto snímačů se navíc ukázalo, že mohou nastat problémy s kvalitou obrazu u velmi suchých prstů. Navíc i přítomnost organických látek má u optoelektronických snímačů otisků prstů

svůj význam pro získání kvalitního obrazu. Z toho důvodu bývá řada optických snímačů řešena tak, že na snímací ploše bývá navíc speciální silikonová fólie, která zlepšuje kvalitu otisku u suchých prstů. Mimoto tato fólie chrání povrch hranolu i před mechanickým poškozením.

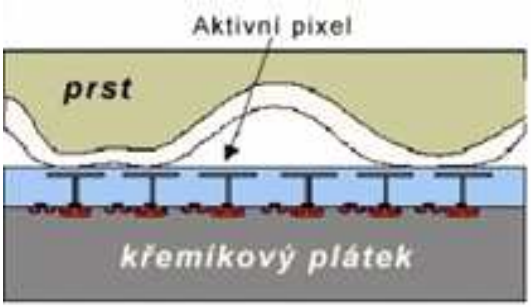


Obr. 9: *Optoelektronický snímač*

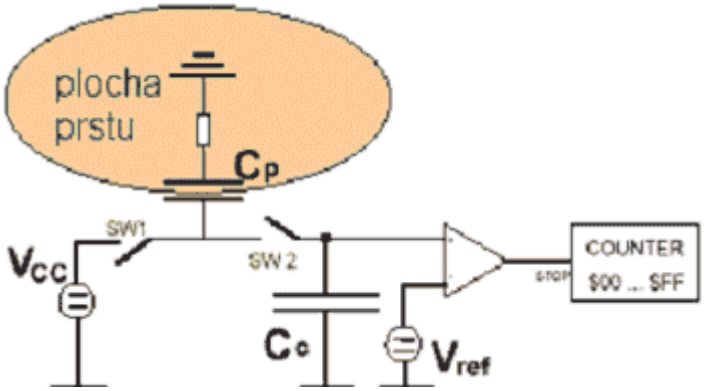
Kapacitní snímače otisků prstů

Kapacitní snímače otisků prstů - také nazývané silikonové - (obr.10), měří kapacitní odpor v ploše dotyku prstu se snímací podložkou, kdy přiložený prst funguje jako jedna deska kondenzátoru a podložka zastává druhou. Dotykem kůže papilární linie „přemosťují“ jednotlivé vodivé plošky v závislosti na kresbě papilárních linií, zatímco brázdy se chovají jako izolant. Měří se napětí a kapacitní úbytky mezi jednotlivými vodivými ploškami. Tak vzniká digitalizovaný obraz papilární kresby, který je získán z aktivních pixelů (obr.11). Rozdíly těchto hodnot se zachytí a podle nich se vytvoří obraz otisku prstu. Principiální schéma kapacitního snímače je znázorněno na obr. 12.

Obr. 10: *Pohled na čip kapacitního snímače*

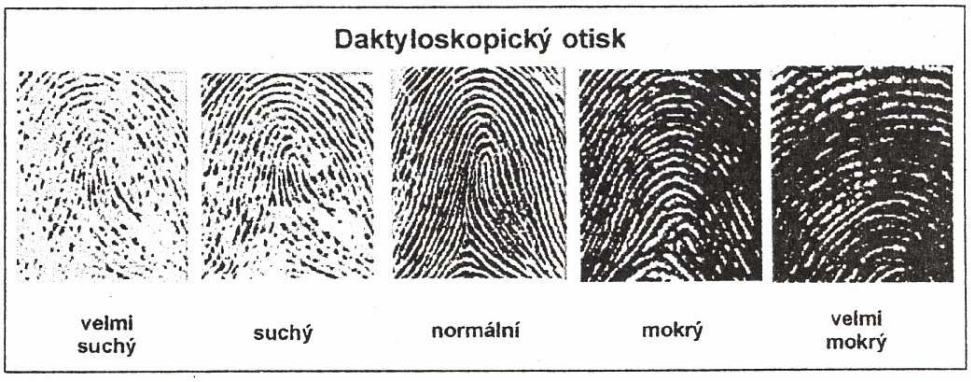


Obr. 11: *Princip funkce kapacitního snímače*



Obr. 12: *Principiální schéma kapacitního snímače*

Slabým místem kapacitních senzorů je citlivost na znečištění pokožky prstu zbytky od jídla obsahující např. sůl nebo cukr (slané pečivo, dorty atd.), které podstatně mění vodivost lidské kůže. Stejně tak i používání ochranných nebo léčivých krémů na pokožku rukou, může ovlivňovat kvalitu snímání. Tyto snímače mají taktéž problémy se snímáním tzv. „suchých“ otisků (obr.13), které jsou pro některé osoby typické.

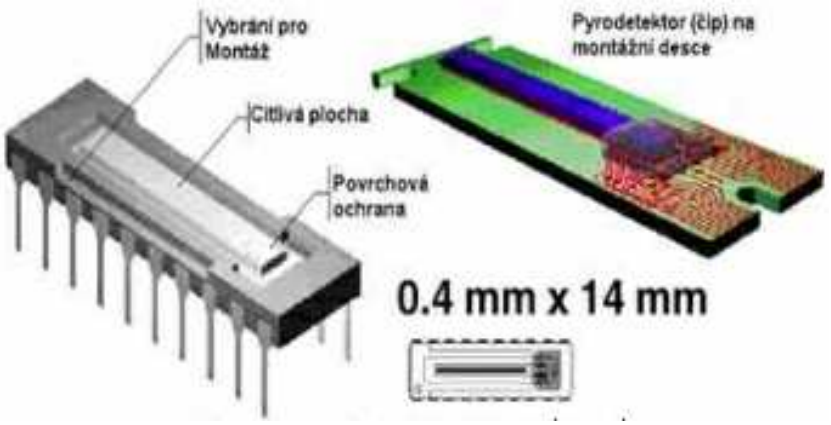


Obr. 13: *Ukázka rozdílů různé „suchosti“ otisků prstů*

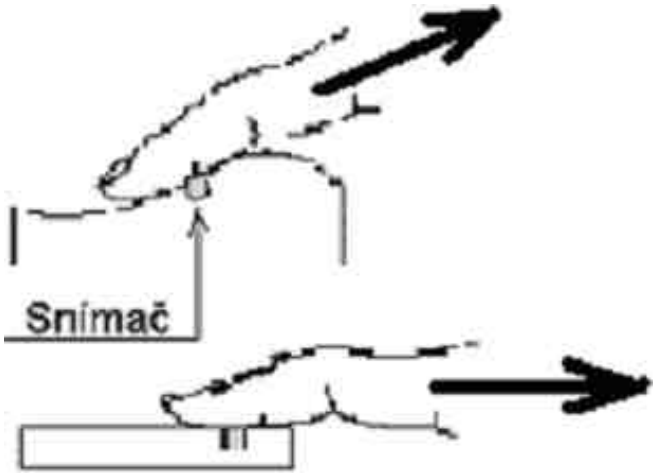
Teplotní snímače otisků prstů

Teplotní snímače otisků prstu (obr.14) jsou vybaveny miniaturním, velmi citlivým pyrodetektorem, který snímá rozdíl teplot mezi papilárními liniemi, jenž se dotýkají pyrodetektoru a prostoru mezi liniemi (výstupky), které se pyrodetektoru nedotýkají. Pro získání obrazu otisku prstu je nutné přejíždět prstem přes citlivou plochu (0,4 x 14 mm). Na výstupu snímače se získává obraz otisků ve formě digitálních pásů, které se softwarově skládají do výsledného obrazu otisku prstu. U těchto snímačů je teplota důležitým faktorem, který dokáže rozpoznat, zda snímaný otisk patří živé osobě.

Velkou nevýhodou snímače je, že otisk získáme pouze pohybem prstu přes citlivou vrstvu čipu, díky čemuž většinou při několika pokusech získáme obrazy otisků různých částí prstu (obr.15). Vzhledem k tomu, že při opakování získáme třeba i jiný otisk stejného prstu, je problematické vytvořit databázi otisků. Protože v databázi otisků je uložena pouze určitá část otisku a při pokusu o autentizaci byla získána jiná část prstu, často dochází k tomu, že i oprávněný uživatel není autentizován.



Obr. 14: *Teplotní snímač otisků prstů*

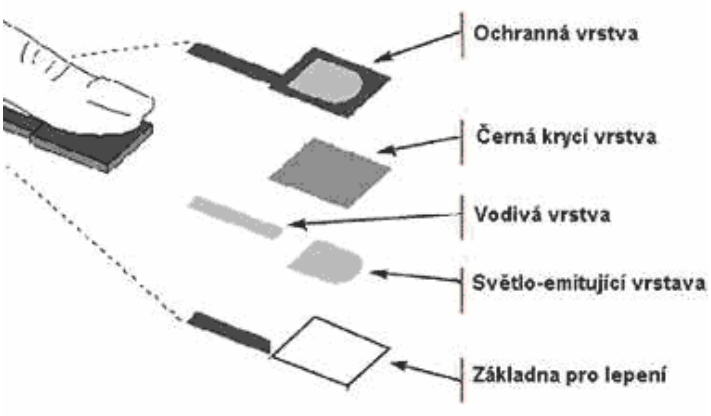


Obr. 15: *Pohyb prstu přes čip pro získání obrazu otisku*

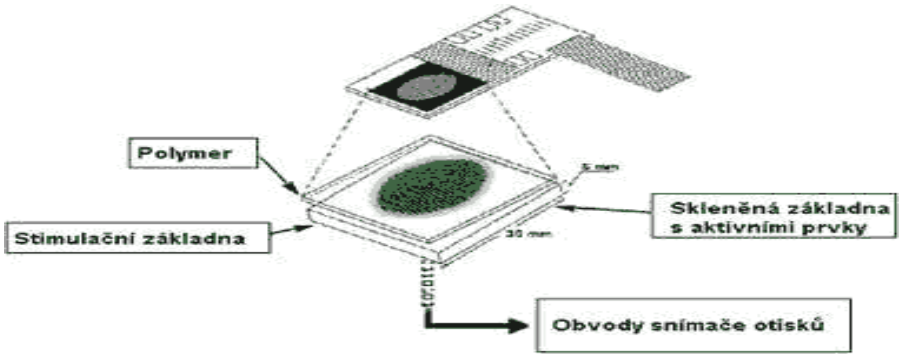
Elektroluminiscenční snímače otisků prstů

Elektroluminiscenční snímač otisků prstů je jedním z nejnovějších snímačů. Snímací plocha je polymer, který se skládá z několika vrstev (obr.16).

Princip funkce elektroluminiscenčního snímače (obr.17) spočívá v tom, že po přiložení prstu na světlo-emitující polymer se ve vrstvě polymeru vytvoří obraz otisku prstu důsledkem emise světla a vlivem tlaku papilárních linií. Emitovaný obraz je následně detekován polem fotodiod a pak transformován do digitálního formátu. Poté je obraz v digitálním formátu odeslán do databáze.



Obr. 16: *Polymer tvořící snímací plochu snímače*



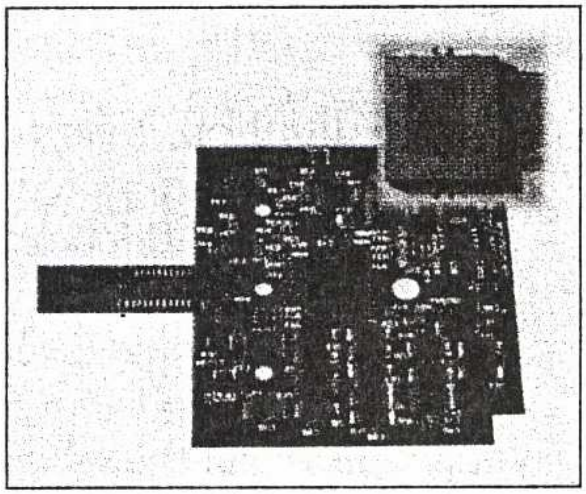
Obr. 17: *Konstrukce elektroluminiscenčního snímače*

Výhodou elektroluminiscenčních snímačů jsou miniaturní rozměry, dobré rozlišení (až 500 dpi) a přijatelná cena. Nezanedbatelnou výhodou je také skutečnost, že kvalita otisku se nesnižuje, i když je prst extrémně suchý (bez přirozených organických látek).

Nevýhodou je menší odolnost vůči mechanickému poškození a náchylnost ke znečištění prostředím (prach, voda).

Tlakové snímače otisků prstů

Tlakové snímače otisků prstů (obr.18) reagují na tlak papilárních linií na povrch snímače. Povrch snímače je tvořen elastickým, piezoelektrickým materiálem, který transformuje tlak papilárních linií do elektrického signálu, a tak vytváří obraz daktyloskopického obrazu. Papilární linie vyvolávají na snímané ploše lokální tlakové působení, zatímco v brázdách je tlak nižší. Pro tlakové snímače platí, že pracují stejně dobře v suchém i mokrém prostředí. Jejich použití není omezeno vlhkostí vzduchu jako u některých jiných typů založených na odlišných fyzikálních principech. Tento typ senzorů není tedy citlivý na „vlhké“ nebo „suché“ otisky prstů určitých skupin lidí.

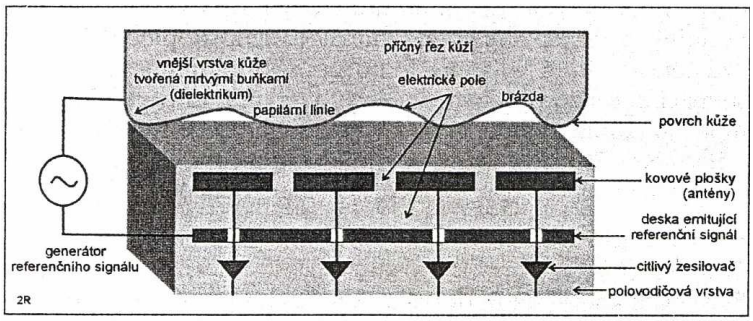


Obr. 18: *Tlakový snímač JDFS s integrovaným HW pro vyhodnocování otisků prstů*

Elektronické snímače otisků prstů

Elektronické snímače otisků prstů (obr.19) pracují na principu vzniku elektrického pole mezi dvěma paralelními vodivými a elektricky nabitými deskami. Horní desku elektronického snímače tvoří povrch kůže, do které je pouštěn řídící elektrický signál. Jakmile se prst dotkne vodivého prstence, který je kolem snímače, dojde k uzavření elektrického obvodu. Husté pole snímacích antén (deskových ploch) zachytí elektrické pole deformované tvarem povrchu kůže (papilárními liniemi abrázdami). Poté je signál zesílen a transformován do elektronického obrazu daktyloskopického otisku.

Výhoda těchto snímačů spočívá v tom, že nereagují na vrchní vrstvu kůže, která může být znečištěna nebo poškozena, ale pronikají hlouběji pod povrch. Tím pádem pak tento snímač není citlivý ani na „suché“ nebo „mokré“ otisky.



Obr. 19*: Principiální schéma elektronického senzoru*

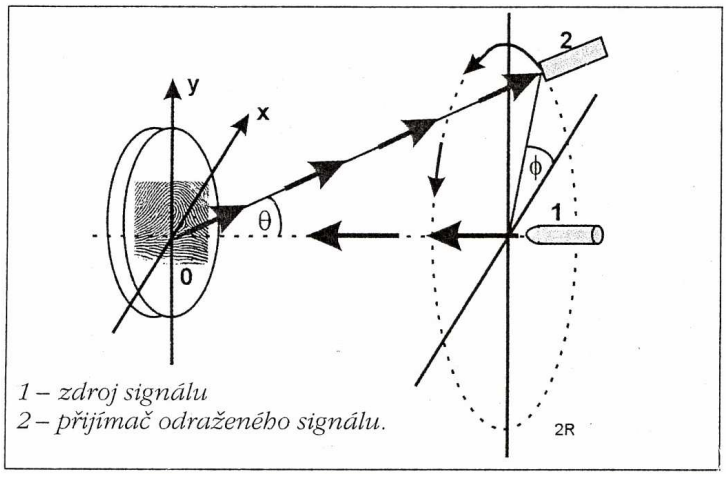
3.1.1.1.2 Snímače bezkontaktní

Do této skupiny snímačů patří:

- Ultrazvukové
- Optické

Ultrazvukové snímače otisků prstů

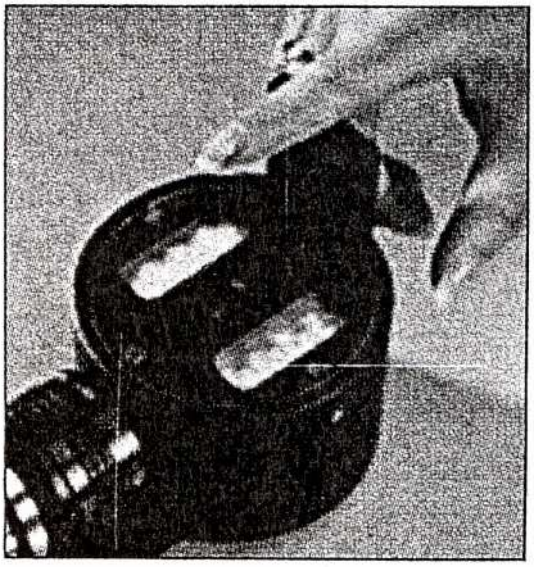
Ultrazvukové snímače otisků prstů fungují podobně jako optické, neměří však dopadající světlo, nýbrž zvukovou vlnu, díky níž jsou schopné rozeznat přilehlé linie od vzdálenějších rýh. Princip ultrazvukového snímání (obr.20) spočívá ve vysílání zvukových vln s vysokou frekvencí (řádově MHz) generovaných zdrojem směrem ke snímané ploše (otisku) a vyhodnocování odražených zvukových vln přijímačem. Vysílaný signál má charakter velice krátkých impulsů. Snímání odražených a deformovaných vln je realizováno rotující hlavou (snímačem) nebo hustou sítí pevných snímacích čidel umístěných v rovině. Obraz otisku prstu je trojrozměrný (3D) s vysokým kontrastem. Snímání má vysokou přesnost až 0,1 mm. Technika ultrazvukového snímání se vyznačuje vysokou odolností vůči vlhkosti, dále přesností při znečištění prstu nebo odbroušení slabé vrstvy kůže (např. u fyzicky pracujících osob). Rovněž lze poměrně snadno rozpoznat případný daktyloskopický podvrh. Výsledný obraz papilárních linií je bez jakéhokoliv zkreslení. Tato metoda je vhodná i pro otisky dlaní.



Obr. 20: *Principiální schéma práce ultrazvukového snímače*

Optické snímače otisků prstů

Princip činnosti těchto snímačů je podobný dotykovým optickým snímačům. Světelný paprsek umožňuje snímat daktyloskopický otisk na vzdálenost 30 až 50 mm. Tento způsob snímání eliminuje znečištění snímače dotyky špinavých prstů a zároveň eliminuje ulpívání papilárních linií na povrchu snímače.



Obr. 21: *Bezkontaktní optický snímač TFS 050 firmy BPI*

3.1.1.2 Požadavky na snímače otisků prstů

Ze základních fyzikálních principů snímání otisků prstů vyplývá, že je velmi důležitá volba vhodného snímače pro autentizaci, příp. identifikaci, protože jednotlivé technologie snímání otisků prstů se svými technickými nároky a následnými výsledky mohou značně lišit, a tím pádem do značné míry ovlivňovat kvalitu celého přístupového systému. Požadavky na snímače jsou dané především prostředím, do něhož bude snímač implementován a použitým algoritmem pro rozpoznání.

Mezi základní požadavky kladené na snímače otisků prstů patří především:

- **Vyhovující celkové rozměry** - tento požadavek je snadno splnitelný u systémů určených pro přístup do místnosti, budov atd. Pro přístup do počítačů, notebooků, apod. je již potřeba zásadní miniaturizace.

- **Dostatečně velká snímací plocha** - dostatečná snímací plocha je nutná pro záznam dostatečného počtu identifikačních znaků, nebo plochy obrazu.

- **Dostatečné rozlišení** - požadavek na rozlišení je dán především použitým algoritmem na rozpoznání, požadavky na spolehlivost a nastavením chyb prvního a druhého druhu pro systém. Kvalitní obraz by neměl mít zkreslení, měl by mít dostatečný kontrast a obsahovat pokud možno co nejširší škálu rozsahu šedé barvy. Kvalita obrazu je ovlivněná nejen konstrukcí snímače a použitým fyzikálním principem, ale také např. vlhkým prstem, suchým prstem, prachem, atd. Pro algoritmy rozpoznávající obraz otisků jako celek je limitující především nerovnoměrné zkreslení.

- **Opakovatelnost dosažené kvality obrazu otisku prstu** - pro dosažení dobrých výsledků při autentizaci z hlediska hodnot chyby prvního a druhého druhu je důležitá opakovatelnost kvality obrazu otisku. Posun obrazu otisků při pokusu o autentizaci vzhledem k otisku a jeho natočení musí být minimální a současně při této činnosti nesmí být nadměrně zatěžován autorizovaný uživatel.

- **Dostatečná ochrana vůči napodobeninám** - snímač sám o sobě nezabezpečuje dostatečnou ochranu vůči napodobeninám. Jde o to, že při znalosti obrazu otisku prstu autorizovaného uživatele nemůže být provedena autentizace ani tím nejdokonalejším padělkem. Dostatečná ochrana vůči napodobeninám je slabým místem současných snímačů.

- **Odolnost vůči elektrostatickému výboji** - k umělým zdrojům přepětí patří lokální elektrostatické výboje. Přestože energie lokálních výbojů je velmi nízká, jejich napěťová úroveň je velmi nebezpečná. Pro většinu moderních elektronických součástek je pravděpodobně největším provozním nebezpečím elektrostatický náboj vznikající na osobách. Osoba tak může běžně dosáhnout napětí proti zemi 5 - 15 kV. Požadavek je významný především pro snímače tepelné a kapacitní.

- **Uživatelská přívětivost** - uživatelská přívětivost je základním požadavkem ve směru k uživateli systému a ergonomii snímače. Vzhledem k určitým omezením, která mají jak snímače, tak algoritmy pro rozpoznání, je reálné nebezpečí, že uživatel bude nepřátelsky naladěn vůči systémům se snímačem otisků prstů.

- **Nároky na implementaci do zvoleného systému** (interface, knihovny) - tento požadavek vystupuje do popředí v případě, že systém pro rozpoznání je určen k připojení do počítače (I/O), ale také do distribuovaných systémů.
- **Spolehlivost snímačů otisků prstu** - spolehlivost je zjišťována především testy na chybu prvního a druhého druhu. Řada výrobců udává ovšem hodnoty, které nejsou dosažitelné ani teoreticky.
- **Zvýšená spolehlivost** - pomocí zdvojených systémů, například pomocí kamerového systému na identifikaci osoby pomocí tváře.
- **Životnost snímačů** - jedná se o konstrukční prvky snímačů, u nichž je z podstaty omezena životnost. Jsou to především materiály, které chrání snímací plochu vůči poškození, a které mohou mít omezenou životnost.
- **Cena snímače** - cena snímače je velmi variabilní v závislosti na řadě faktorů. Z výše uvedených charakteristik snímačů je zřejmé, že nejdražší budou kvalitní optoelektronické snímače.

Obr. 22: *Příklad snímače otisků prstů V-Pass*

3.1.2 Identifikace podle geometrie ruky

Tato biometrická metoda není natolik přesná jako otisky prstů, a proto se využívá pouze k verifikaci, nikoliv identifikaci. Identifikace podle geometrie ruky je založena na skutečnosti, že každý člověk má specifický tvar ruky, který se od určitého věku nemění. Podstatou této metody je dvou nebo třírozměrné měření délek nebo šířek jednotlivých prstů, kloubů nebo kostí, kdy uživatel přikládá svou ruku na čtecí zařízení s dlaní směřující dolů (obr.23). Naopak se u této metody neměří délka nehtů či povrchové poškození kůže, protože se totiž jedná o vlastnosti, které se časem mohou měnit, a tedy i negativně ovlivnit úspěch verifikace.

Mezi výhody této identifikace patří poměrně dobrá vyváženost z hlediska výkonnostních charakteristik i relativní snadnost používání. Tato metoda je také vhodná pro větší databázi uživatelů nebo pro uživatele s ne příliš častým přístupem (takoví uživatelé bývají méně disciplinovaní z hlediska správného používání biometrického systému, což může vést k častějšímu zamítnutí žadatele). A právě díky jednoznačnosti charakteristik ruky lze docílit poměrně vysoké přesnosti systému. Pro mnoho biometrických projektů je verifikace geometrie ruky obvykle prvním systémem, o kterém se při návrhu uvažuje.

K nevýhodám patří zejména to, že lidé s artrózou nebo jí podobnou vadou mohou mít potíže se správným přiložením ruky ke čtecímu zařízení. A také to, že velikost ruky se u někoho se může změnit v důsledku přibrání nebo naopak zhubnutí.

Obr. 23: *Čtecí zařízení sloužící k identifikaci geometrie ruky*

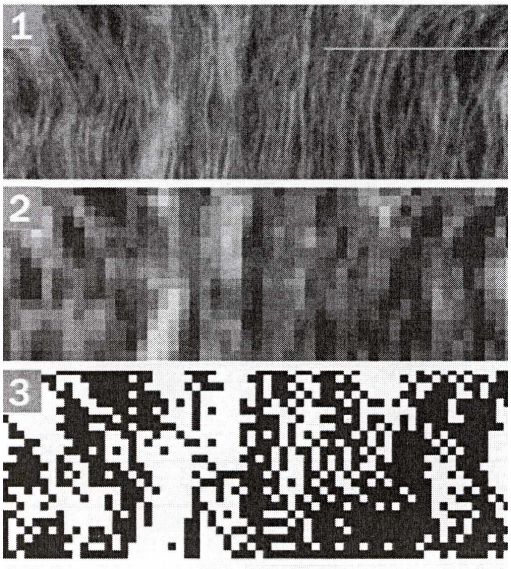
3.1.3 Identifikace podle oční duhovky

Tato metoda je založena na snímání lidské duhovky. Přitom v jejím prvním kroku nejde o nic jiného než o digitální vyfotografování očí. Teprve potom systém vyhodnotí komplexní vzor duhovky. Neexistuje jiná biometrická charakteristika člověka, která by poskytovala více rozlišovacích možností než právě duhovka. Nalezení dvou identických duhovek náhodným výběrem je mnohonásobně méně pravděpodobné než nalezení dvou identických otisků prstů. Dokonce i obě duhovky jednoho člověka jsou rozdílné a jedinečné. Ani dvě identická dvojčata nemají duhovky stejné. Detailním zkoumáním lidského oka lze v duhovce zaregistrovat několik jasně viditelných vnějších znaků (kruhy, skvrny, rýhy, koróny atd.), které jsou stabilizovány během prvního roku po narození a zůstávají neměnné celý život. Při snímání dochází k digitalizaci těchto rysů, přičemž je pořizován černobílý snímek uživatelova oka ve vysokém rozlišení (obr.26). K rozpoznávání se obvykle používá spodní půlkruh duhovky – kruhový segment se přitom transformuje na pravoúhlý proužek. Jelikož je struktura duhovky na rozdíl od ostatních biometrických znaků velmi symetrická, dají se její případné deformace snadno matematicky upravit. Proto se tohoto faktu využívá pro identifikaci osob, zvláště v případě oprávnění k přístupu do informačního systému. Protože struktura duhovky je u osob s tmavou barvou očí v normálním světle těžko rozeznatelná, osvětlují se oči při fotografování neviditelným infračerveným světlem, které lépe proniká očním barvivem, tzv. melaninem. „Intenzita světla je přitom menší než u dálkového ovládání televizorů," zdůrazňuje bezpečnost tohoto postupu Harald Zander z výrobní firmy Panasonic.

Výhodou této metody je, že není vyžadován žádný fyzický kontakt mezi duhovkou a snímající kamerou, tím je používání rychlé, pohodlné a vysoce přesné. Dokonce ani fotografie oka nebo skleněné oko nemohou přelstít takovýto systém.

Obr. 24: *Čtecí zařízení sloužící k identifikaci oční duhovky*

Obr. 25*: Iris Access 3000 – snímač oční duhovky*



Obr. 26: *Proces rozpoznávání oční duhovky*

Popis procesu rozpoznávání oční duhovky:

1. ČÁSTEČNÝ OBRAZ DUHOVKY

Nejprve se sejme (spodní) polovina duhovky a pro další zpracování se v počítači přetransformuje na pravoúhlý proužek. V něm jsou stále ještě patrné struktury původního obrazu.

2. MATEMATICKÉ VYJÁDŘENÍ

Snímek se rozloží na malá políčka, jejichž obsah se matematickými operacemi převede na číselné hodnoty reprezentované stupni šedi.

3. DIGITÁLNÍ DATA

Políčka světlejší než průměr se změní na bílá, zbývající políčka obdrží černou barvu. Bílá a černá představují jedničky a nuly v tzv. šabloně, 512 bajtů velkém datovém bloku reprezentujícím skenovanou duhovku.

3.1.4 Identifikace podle oční sítnice

Při použití této metody dochází k porovnávání struktury sítnice v okolí slepé skvrny. Sítnice, stejně jako duhovka, obsahuje rovněž dostatek specifických anatomických znaků,

které zajišťují její vysokou identifikační přesnost. Protože sítnice není viditelný lidský orgán, používají se pro její transformaci do viditelné podoby koherentní infračervené světelné zdroje. Důvodem je, že cévy sítnice rychleji absorbují infračervenou energii než ostatní tkáně, což způsobuje, že tyto cévy jsou na snímaném obraze tmavší.

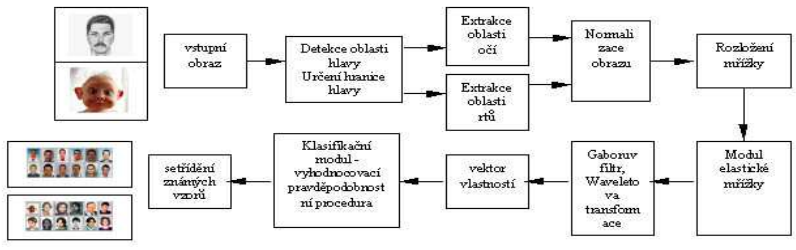
K výhodám snímaní oční sítnice patří velice dobrá přesnost, nicméně kvůli vysoké ceně a uživatelské nepřívětivosti, zejména kvůli neochotě lidí nechat si skenovat oči, se tento typ identifikace nedočkal velkého rozšíření. Brýle ani kontaktní čočky nemají na funkci tohoto systému vliv.

3.1.5 Identifikace podle geometrie obličeje

Identifikace podle geometrie obličeje je jednou z nejpřirozenějších biometrických metod. Podobně jako při skenování duhovky i při rozeznávání obličeje se na základě digitální fotografie stanoví charakteristické ukazatele, které se porovnají s uloženou šablonou (obr.27). Využívají se především ty znaky, které nejsou příliš ovlivněny mimikou, jako jsou - horní okraje očnic, oblasti kolem lícních kostí a postranní partie úst. Software nejprve vyhledá oči jako temné body v horní polovině obrazu a odtud se pak pokouší najít další markantní body obličeje. Pokud se nepodaří spolehlivě určit pozici očí, další rozpoznávání je zbytečné, protože by bylo neúspěšné. Obličej a jeho individuální znaky jsou v podstatě jako otisky prstů.

Mezi výhody této identifikace patří zejména to, že rozpoznávání nevyžaduje žádný kontakt s identifikovanou osobou.

Nevýhodami jsou problémy, které mohou nastat v případě dvojčat a zejména nedokonalé kamerové systémy, které zobrazený obličej nedokáží rozpoznat, protože na porovnávaných snímcích je pokaždé jiná orientace hlavy nebo nesouhlasí světelné poměry.



Obr. 27: Proces rozpoznávání obličeje

Obr. 28: *Příklad snímače obličeje*

3.1.6 Identifikace podle hlasu

Podstatou této biometrické metody je elektronická analýza řeči identifikované osoby. Lidská řeč je charakteristická svým subjektivním vlivem osobnosti mluvčího (barva hlasu, rytmus atd.), akustickou a lingvistickou strukturou (gramatika a skladba řeči). Zdrojem řečových kmitů jsou řečové orgány, tzv. vokálový trakt, který je složen z hlasivek, ústní dutiny, jazyka a zubů, přičemž tvar těchto orgánů způsobuje, že rezonance vokálního traktu je u různých osob dostatečně odlišná.

K výhodám této identifikace patří rychlost, spolehlivost, jednoduchost na použití, nízká cena a také zde není zapotřebí žádné speciální hardwarové zařízení.

Nevýhodou je to, že verifikace může být za určitých okolností (nastydnutí, šum okolí, atd.) mnohem komplikovanější než u jiných biometrik.

3.1.7 Identifikace podle dynamiky podpisu

K identifikaci podpisu je zapotřebí, aby se osoba podepsala na speciální podložku pomocí speciálního pera (obr.29). Biometrický systém pak ověřuje podpis osoby na základě porovnání s uloženým podpisovým vzorem. Vlastní technologie rozpoznávání je založena na porovnávání změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na papíře a nad ním. V případě verifikace podpisu není ani tak důležitá podoba podpisu či tvar písmen, ale

důraz je kladen zejména na dynamiku podpisu, provedení tahů, sílu, kterou identifikovaná osoba při psaní tlačí na podložku, rychlost psaní apod.

Oproti jiným biometrickým metodám má verifikace podpisu výhodu v tom, že lidé jsou zvyklí se podepisovat při různých transakcích spojených s ověřením identity a zpravidla nevidí na zavedení této verifikace nic neobvyklého. Zařízení pro verifikaci podpisu jsou poměrně přesná a obvykle se používají na místech, kde se podpis vyžadoval ještě před zavedením biometrického systému.

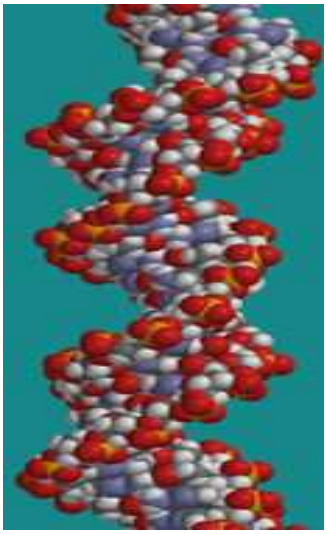
I přesto je v současnosti těchto zařízení v porovnání s jinými biometrickými systémy používáno poměrně málo.

Obr. 29: *Příklad speciálního pera pro identifikaci podpisem od firmy Logitech*

3.1.8 Identifikace podle DNA

U této identifikace se vychází z principu, že stejně jako má každý člověk jedinečné otisky prstů, má i jedinečný tzv. DNA-otisk. Průměrný počet rozdílů mezi dvěma nepříbuznými jedinci je přibližně 10^6. Vyjímku tvoří jednovaječná dvojčata, která mají tento „otisk“ stejný. Možnosti jeho získání jsou však mnohem širší než u otisků prstů. Výhodou je, že na rozdíl od obvyklého otisku prstu, který muže být chirurgicky změněn, je DNA-otisk stejný pro každou buňku, tkáň a orgán člověka, tj. nemůže být změněn žádnou známou úpravou.

Značnou nevýhodou této metody je fakt, že k identifikaci je zapotřebí krev nebo jiné tělesné vzorky a také proti jinému, než je použití k danému účelu, hovoří zásady ochrany osobních údajů a pochybnosti o etické vhodnosti tohoto postupu.



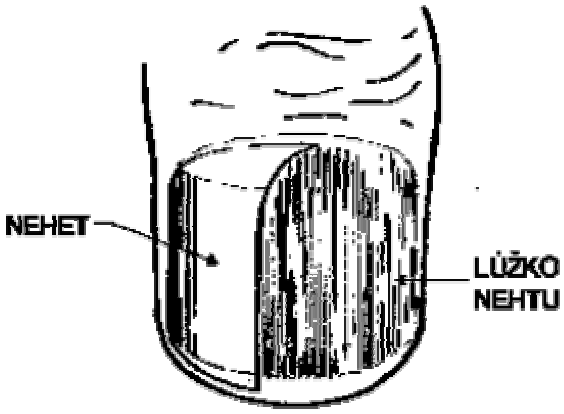
Obr. 30: *Struktura DNA*

3.2 Ezoterická identifikace

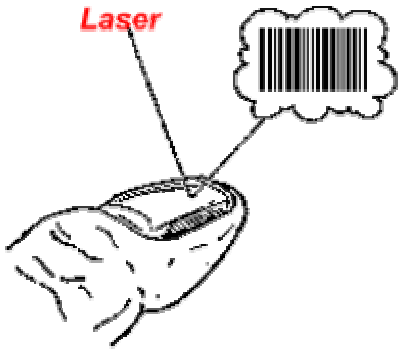
3.2.1 Identifikace podle nehtu

Nehet člověka má na povrchu čárové nerovnosti kopírující strukturu lůžka nehtu (obr.31), která je na každém prstu a pro každého člověka unikátní. Lůžko nehtu je v podstatě paralelní podkožní struktura nacházející se přímo pod nehtem. Rostoucí nehet se pohybuje po této struktuře a kopíruje její povrch. Mezi nehtem a lůžkem je keratin, což je přírodní polymer měnící orientaci dopadajícího polarizovaného světla. Pokud paprsek polarizovaného světla dopadá na nehet pod určitým úhlem, je možné analyzovat fázové změny paprsku po odrazu. Po zpracování snímaného odrazu se pak dostane jednorozměrná struktura lůžka nehtu, tj. číselná sekvence, která připomíná sekvenci čárového kódu (obr.32).

Tato metoda je zatím ve stadiu vývoje a představuje možnost levné a velmi rychlé biometrické identifikace. Nevýhodou zřejmě bude nízká odolnost proti podvrhům.



Obr. 31: *Struktura nehtu*



Obr. 32: *Princip identifikace*

3.2.2 Identifikace podle žil na rukách

Jedná se o biometrickou identifikaci využívající záznamy podkožních žil jako vzorku pro jednoznačnou identifikaci určité osoby. Princip této identifikace je podobný identifikaci podle oční sítnice. Snímání se realizuje kamerou v infračervené oblasti elektromagnetického spektra. Tato technologie umožňuje vytvořit z takovýchto vzorků pro každou osobu čárový kód.

Výhodou této metody je, že vzory žil se dají jen velmi obtížně zničit, skrýt nebo změnit. Žíly představují velké, stabilní a opakovatelné vzorky a mohou být snadno zobrazeny v rámci zápěstí, dlaně a dorsální části ruky.

3.2.3 Identifikace podle dlaní

Tato identifikace patří do skupiny daktyloskopických identifikací a využívá podobných přístupů a technologií jako identifikace podle otisku prstů. Tato metoda závisí na typu snímacího zařízení a mimo jiné měří úhel nebo velikost jednotlivých prstů. Ačkoliv jde oproti jiným biometrickým identifikacím o jednoduchou záležitost, není pro uživatele stále příliš komfortní.

K nevýhodám patří to, že na rozdíl od snímání otisků prstů vyžaduje tato metoda snímání podstatně větších rozměrů, což představuje limitní faktor z hlediska rychlosti zpracování snímaných dat. Dalším negativem je, že vnitřní strana dlaně je zakřivena a proto se obtížně snímá.

3.2.4 Identifikace podle pachu lidského těla

Pachovou identifikaci používá policie jako nepřímého důkazu již desítky let, ale v civilní branži se tato technika stále jeví jako okrajová, a to i přes zřejmost faktu, že lidský pach může být při dostatečně přesném měření poměrně spolehlivým identifikačním vodítkem. V kriminalistice je s pojmem „lidský pach“ spojena řada jevů, jako je vznik pachových látek, jejich uvolnění, přenos do vzduchu (vznik pachu), proces detekce a identifikace pachu apod. Oborem, který se zabývá zkoumáním pachu, je věda o pachu – ***odorologie***.

Člověk do okolního prostředí vylučuje řadu látek, které jsou podstatou lidského pachu, jedná se především o pot a dech. Prakticky nejdůležitějším zdrojem lidského pachu je pot, který je potními žlázami vylučován nepřetržitě. Sekreci potu nelze nijak zabránit ani ji účinně omezit. Kromě vody, minerálních látek a některých organických látek obsahuje pot i významné množství těkavých látek (např. kyselina mléčná, aldehydy, ketony apod.). Individualizace lidského pachu je dána celou řadou okolností, které mají na lidského jedince vliv; jedná se zejména o věk, pohlaví, rasu, nemoci, požívání léků, konzum tabákových výrobků nebo alkoholických nápojů apod.

Problém při využití této identifikace spočívá zejména v tom, že v civilní oblasti je potřeba porovnávat a správně identifikovat více než jednu pachovou stopu zároveň, a proto zatím neexistují dostatečně přesné senzory. Dalším problémem jsou změny ve skladbě pachových stop při emocionálních či hormonálních výkyvech.

3.2.5 Identifikace termovizními obrazy

Protože črty tváře nebo jiných fyziologických znaků osob se vzájemně liší, tepelné poměry na snímaných částech osob budou vytvářet jiné termovizní obrazy, které se snímají termovizními snímači. Identifikace spočívá v analýze příznaků termovizních obrazů.

3.2.6 Identifikace podle tvaru vnějšího ucha

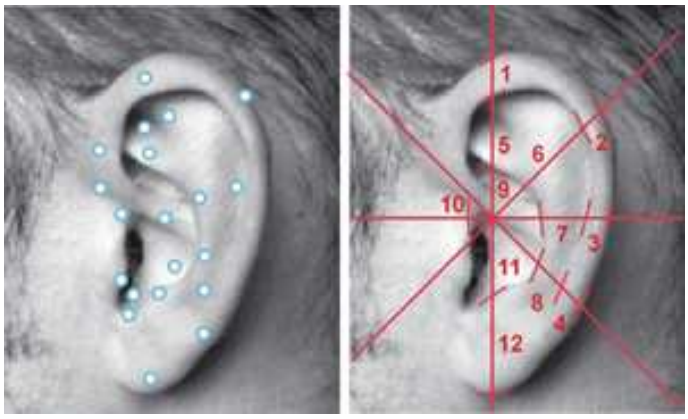
Tato identifikační metoda říká, že každý člověk má unikátní a specifický tvar ucha. Neexistují dvě absolutně identické uši, ale pouze uši podobné. Dokonce ani obě uši jedné osoby nejsou identické, ale mezi pravým a levým uchem existují rozdíly. To samé platí rovněž i pro uši jednovaječných dvojčat. Rozlišujeme čtyři základní tvary vnějšího ucha: tvar oválný, kulatý, obdélníkovitý a trojúhelníkovitý. Tyto základní tvary se objevují u každé rasy, ale v různé procentuální četnosti výskytu. Rozdíly ve tvaru vnějšího ucha tvoří základ klasifikace otisků ucha. Otisky je možné snímat podobným způsobem jako otisky daktyloskopické a uchovávat je pro další zpracování. Mezi nejrozšířenější metody snímání otisku ucha patří metoda daktyloskopická a fotografická, které se v praxi vzájemně kombinují a doplňují (obr.33 a obr.34).

Hlavní nevýhodou této identifikace je skutečnost, že v okamžiku, kdy je ucho překryto vlasy, což bývá poměrně často, nelze pozorovat, natož i rozpoznávat tvar vnějšího ucha osoby.

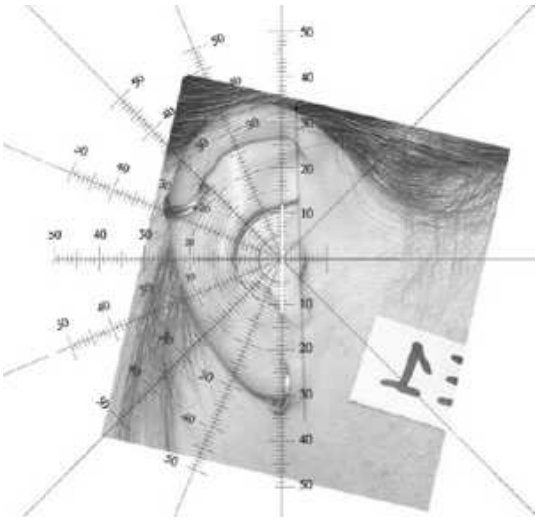
V případě, že používaná aplikace je aktivního charakteru, to nemusí být na závadu, protože prověřovaná osoba sama odkryje vlasy překrývající ucho. Aktivní aplikace předpokládá spolupráci.

U pasivních aplikací se naopak předpokládá, že prověřovaná osoba nebude vykonávat žádnou zvláštní činnost, aby umožnila nebo usnadnila identifikačně-verifikační proces. U plně nebo částečně zakrytých ušních boltců lze výhodně využít snímání obrazu ucha v infračerveném pásmu. Využívá se skutečnost, že teplota vlasů osoby se pohybuje v pásmu 27,2 až 29,7 °C, zatímco teplota ucha při normálních klimatických podmínkách je 30,0 až 37,2 °C. Teplota se na povrchu ucha mění a izotermy odrážejí anatomický tvar ucha. Této skutečnosti se využívá pro získání snímku ucha podobně jako při pořízení záznamu dnes CCD kamerou. Termogram pak odstraňuje nedostatky vyplývající ze zakrytí ucha vlasy, popř. jiným materiálem.

Obr. 33: *Daktyloskopický otisk ucha*



Obr. 34: *Fotografie ucha – Vlevo: Základní anatomické charakteristiky; Vpravo: Udávané geometrické charakteristiky*



Obr. 35: *Pomůcka pro měření geometrických charakteristik ucha*

Mezi další ezoterické identifikace patří:

- identifikace podle lokomoce (chůze)
- identifikace podle otisků rtů a pórů
- identifikace podle obsahu soli v lidském těle

3.2.7 Identifikace podle dynamiky klávesových úderů

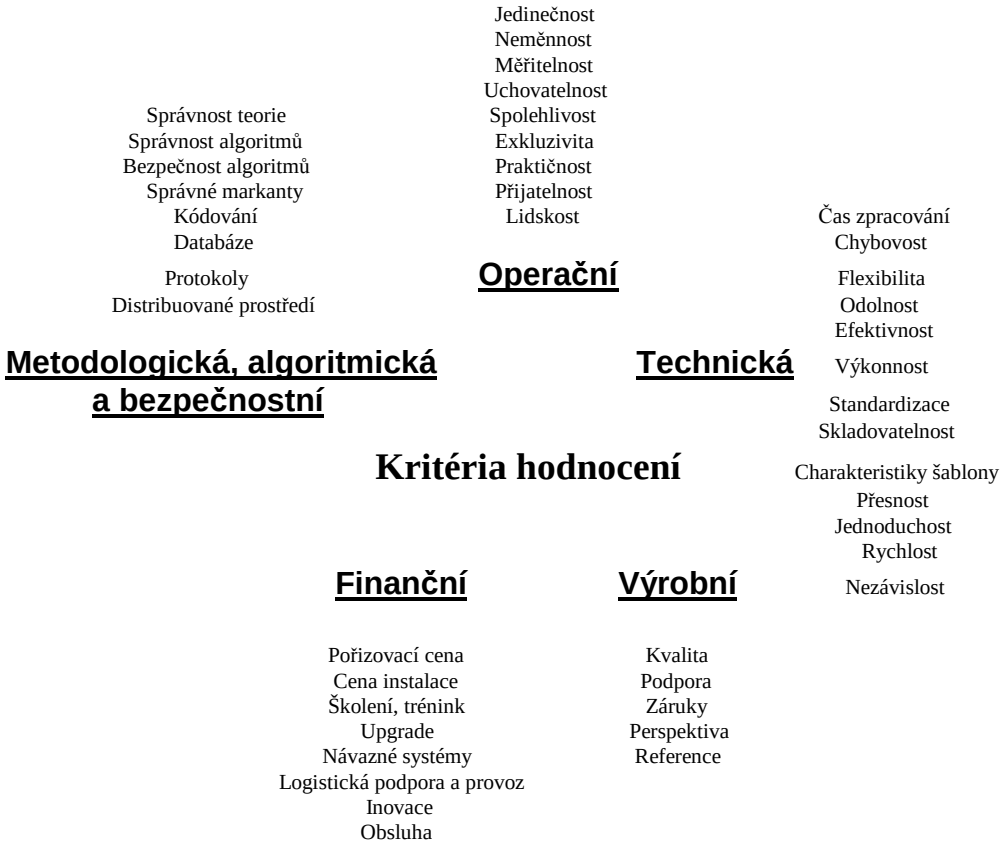
Tato metoda využívá k ověření identity uživatele rytmus sázení znaků do klávesnice. Styl psaní na klávesnici se u jednotlivých uživatelů jasně odlišuje. Proto se jako příznaky identifikace používají trvání stisku nějakého znaku a prodleva mezi stisky dvou různých znaků.

Problém může nastat v případě, kdy uživatel „nováček“ je ve fázi registrace a postupem času se naučí psát všemi deseti, pak je třeba zpravidla registraci opakovat. Měření dynamiky stisku kláves nevyžaduje žádné speciální hardwarové zařízení, protože vstup lze realizovat pomocí jakékoliv klávesnice.

Všechny tyto biometrické identifikační metody, s vyjímkou posledně jmenované - tedy identifikace podle dynamiky klávesových úderů, jsou metody, které nejsou v praxi zatím běžně rozšířené a dostatečně prověřené. Jsou známé jen úzké skupině specialistů a odtud vyplývá i název ezoterický – utajovaný, skrytý, přístupný jen zasvěceným.

3.3 Základní kritéria biometrických technologií

Následující charakteristiky jsou důležité jak pro samu funkčnost biometrických identifikačních a verifikačních technologií, tak i pro jejich celkovou úspěšnost. Některá kritéria jsou spojena se základní teorií a praxí identifikace či verifikace a ochrany osobních údajů, jiná odrážejí ekonomičnost, praktičnost i společenskou a finanční přijatelnost.



Obr. 36: *Základní kritéria biometrických technologií*

3.3.1 Operační kritéria

Jedinečnost – biometrické charakteristiky dané identifikační metody musí být dostatečně jedinečné, aby bylo možné odlišit jednu osobu od druhé s vysokou přesností a spolehlivostí.

Neměnnost – prvky (markanty), na kterých je založena biometrická identifikace, musí být v čase neměnné, tj. aby vlastnosti člověka, které se měří a dále technologicky zpracovávají, byly neměnné po celou dobu jeho života, nebo alespoň po dobu od produktivního do důchodového věku.

Měřitelnost – charakteristiky, na kterých je založena identifikace, musejí být měřitelné a symbolicky vyjádřitelné. Musí být dopředu známa teoretická i praktická chybovost měření, než je biometrická metoda zavedena do praxe.

Uchovatelnost – naměřené identifikační charakteristiky musí být možné uchovávat s přijatelnými náklady, aniž by došlo ke ztrátě jejich kvality.

Spolehlivost – proces měření, zpracování, ukládání a vyhodnocování biometrických charakteristik musí být dostatečně spolehlivý a kdykoliv zopakovatelný se stejnými výsledky.

Exkluzivita – identifikační metoda by měla být dostatečná (úplná) takovým způsobem, aby nebyla nutná další podpůrná identifikační činnost (založena např. na jiné metodě identifikace).

Praktičnost – metoda musí být ve všech směrech praktická. Uživatel by měl být v minimálním kontaktu s technologickým zařízením a během procesu identifikace ztratit co nejméně času, měl by vykonat minimální množství požadovaných úkonů. Měření by mělo být co nejjednodušší, obsahovat co nejméně měřených a ukládaných charakteristik a vyžadovat minimum tréninku uživatele.

Přijatelnost – snímání stejně jako další zpracování, uchovávání a vyhodnocování biometrických údajů by mělo být přijatelné pro mnoho lidí. Musí být v vyloučeny takové technologické metody a postupy, které vyžadují část lidského těla, tj. provádějí zásah do jeho integrity a jakýmkoliv způsobem lidský organizmus poškozují nebo oslabují. Používání zařízení by mělo být důvěrné, bez přítomnosti přihlížející veřejnosti. Proces identifikace nesmí jakýmkoliv způsobem narušovat soukromí jakékoliv osoby a musí být zajištěna ochrana všech získaných údajů před neoprávněným přístupem, nebo dokonce zneužitím.

Uživatelská přívětivost (lidskost) – proces snímání a vyhodnocování nesmí být nijak vtíravý, ale naopak nerušivý. Osoba by neměla mít žádné pocity diskriminace v souvislosti např. s barvou pleti, věkem nebo profesí. Výběr identifikační technologie a její technická realizace je velmi citlivá psychologická záležitost, a proto nevhodný přístup při výběru metody a způsobu její realizace může v člověku vyvolat nepříjemné pocity.

3.3.2 Technická kritéria

Při analýze časové náročnosti biometrické identifikace se vyhodnocují: čas přípravy uživatele a zařízení na proces identifikace, čas samotného snímání, čas na zpracování a uložení získaných charakteristik, doba na prověření (identifikační/verifikační čas).

Testuje a vyhodnocuje se chybovost technologie, pozornost se věnuje pravděpodobnosti přijetí neoprávněného uživatele (FAR – False accept rate) i

pravděpodobnost odmítnutí uživatele oprávněného (FRR – False reject rate). Zařízení by mělo být schopno se vypořádat s oběma typy chyb. Technologie musí být nezávislá na vnějším prostředí nebo být schopná odfiltrovat rušivé vlivy (v závislosti na použité metodě) – hluk, světlo, elektromagnetické záření, teplotu, vlhkost, kouř, prach apod. Další charakteristiky jsou již běžné jako při vyhodnocování jakýchkoliv jiných standardních technologií.

3.3.3 Metodologická (matematická), algoritmická a bezpečnostní kritéria

Spolehlivost a přijatelnost systému záleží i na efektivitě systému, jak je systém chráněn proti neautorizovaným zásahům, modifikacím, poznání nebo použití, jak reaguje na různé hrozby a jak je schopen sám rozpoznat zneužívání. Biometrické metody používají různé matematické algoritmy, komprese, kódy a protokoly. Biometrické algoritmy jsou podobné a liší se v technologiích jednotlivých metod, kde jsou použity.

Kódování výskytu identifikačních markantů a sledování jejich výskytu, charakteristik a závislostí je nejčastějším prvkem biometrických procedur. Jestliže jsou algoritmy založené na chybné matematické teorii, technologie, které používají uvedené algoritmy, jsou nepoužitelné. Jestliže je teorie v pořádku, ale algoritmy jsou chybné nebo lze v průběhu identifikačního zpracování jinak ovlivnit výsledek, identifikační technologie není bezpečná.

Různé algoritmy nabízejí různý stupeň bezpečnosti a záleží na úsilí, které je potřeba vyvinout na jejich překonání. Jestliže vynaložené úsilí na překonání bezpečného algoritmu nás stojí více než je cena chráněných dat, pak se obecně technologie považují za bezpečné.

O technologické kvalitě používané metody rozhodují kromě teorie i algoritmy, kódování, protokoly a databáze, kde jsou biometrická data uložena. Zejména ve vládní, policejně-soudní, vojenské a finanční praxi nebudou akceptovány ty biometrické systémy a technologie, které nejsou dostatečně bezpečné a spolehlivé. Každé zařízení je proto důkladně a systematicky certifikováno.

3.3.4 Finanční kritéria

Otázka financí mnohdy hraje rozhodující roli při vývoji i nákupu biometrických technologií. Finance se posuzují z jednorázového i dlouhodobého pohledu.

3.3.5 Výrobní kritéria

Při výběrových řízeních se zohledňují i kvality dodavatele, výrobce technologií. Roli hraje schopnost efektivní a cenově přijatelné podpory při provozu zařízení ze strany výrobce nebo dodavatele. Stranou nezůstává ani kompatibilita s jinými technologiemi, reference od dalších uživatelů atd.

Biometrická metoda	Snímání	Neměnnost	Jednoznačnost	Přijatelnost
Geometrie ruky	optické - infračervené	dobrá	1:10 000	velmi dobrá
Oční sítnice	optické - laser	velmi dobrá	1:1 000 000	nedobrá
Oční duhovka	optické	velmi dobrá	1:6 000 000	nedobrá
Podpis	statický obraz nebo dynamické (tlak)	proměnlivá	1:10 000	velmi dobrá
Hlas	elektroakustické	proměnlivá	1:10 000	dobrá
Tvář	optické, infračervené	dobrá	neznámá	dobrá
Otisk prstu	optické, elektronické	velmi dobrá	1:1 000 000	dobrá

Tab. 2: *Základní biometrické metody a některé jejich charakteristiky*

Biometrická charakteristika	Výhody	Nevýhody	Kulturní a náboženská omezení
Otisk prstu	• Přesné • Snadno dostupné • Malé rozměry čtecích zařízení • Nízká cena	• Někteří lidé mají strojově nezpracovatelné otisky prstů	• Některé země nedovolují ukládat otisky prstů pro jiné než policejní
Geometrie ruky	• Nepovažuje se za dotěrné • Malá velikost šablony • Rychlost zpracování	• Nepřesnost v režimu One-to-Many • Větší nároky na prostor • Může vyžadovat znovusejmutí šablony z důvodu změny hmotnosti, a tedy rozměrů ruky	• Žádná
Hlas	• Nepovažuje se za dotěrné • Jedině možné pro telefonní bezpečnostní systémy	• Méně přesné než ostatní charakteristiky	• Žádná
Sítnice	• Nejpřesnější z uvedených charakteristik	• Považuje se za velmi dotěrné • Oko musí být v průběhu dlouhé doby snímání nehybné	• Nepřijatelné v zemích, kde je oko považováno za okno

			do duše
Duhovka	• Velmi přesné • Od narození neměnné	• Často se zaměňuje za snímání sítnice • Kamera je zatím velmi drahá pro běžné použití	• Nepřijatelné v zemích, kde je oko považováno za okno do duše nebo je zakázáno fotografování
Obličej	• Nepovažuje se za dotěrné • Levná kamera	• Méně přesné než ostatní charakteristiky	• Nepřijatelné v zemích, kde je zakázáno fotografování
Podpis	• Není dotěrné • Vhodné pro finanční transakce	• Nepřesnost v režimu One-to-Many • Vyžaduje více podpisových šablon	• Žádná

Tab. 3: *Porovnání jednotlivých biometrických metod*

3.4 Klasifikace biometrických aplikací ve vztahu k uživatelům a prostředí

Každá technologie má své silné i slabé stránky a biometrické systémy nejsou vyjímkou. Všechno to závisí na samotné aplikaci a způsobu jejího používání. Ačkoliv je každá biometrická metoda a technologie vždy specifická, lze najít základní společné znaky mezi biometrickými technologiemi, jejich uživateli a prostředím, ve kterém pracují. Aplikace biometrických systémů je možné rozdělit do následujících skupin:

- Spolupracující versus nespolupracující
- Zjevné versus skryté
- Obvyklé versus neobvyklé
- Samoobslužné versus s obsluhou
- Standardní versus nestandardní prostředí
- Veřejné versus privátní
- Otevřené versus uzavřené

Spolupracující versus nespolupracující

- Tato kategorie je dána tím, zda osoba s identifikační technologií spolupracuje ochotně či neochotně. Pozornost je věnována především osobám, které se snaží skrýt svou identitu. Pod pojmem ***spolupracující uživatel*** se rozumí takový uživatel, který je zainteresován tak, aby byla rozpoznána jeho pravá identita. Za ***nespolupracujícího uživatele*** je považován každý, kdo se snaží skrýt svou skutečnou identitu nebo využít identitu někoho jiného, aby pronikl do objektu a tam provedl činnost, na kterou nemá oprávnění. U spolupracujícího uživatele se předpokládá, že může být požádán, aby se sám identifikoval prostřednictvím hesla nebo PIN kódu a usnadnil tak identifikaci/verifikaci. U nespolupracujícího uživatele je tato možnost vyloučena a prověřují se pouze jeho biometrické charakteristiky.

Zjevné versus skryté

- O ***zjevnou*** aplikaci se jedná tehdy, jestliže si uživatel uvědomuje, že je „měřen“ pomocí biometrické technologie. V aplikacích ***skrytého*** charakteru tato skutečnost není osobě známa. Aplikace, které mají přístupový charakter jsou zpravidla vždy zjevného typu naopak forenzní a policejně-soudní aplikace jsou skryté.

Obvyklé versus neobvyklé

- Jestliže se uživatel denně podrobuje biometrické identifikaci, je pro něj již po určitém čase ***obvyklá*** a známá. Ví, jak se má chovat a jak má spolupracovat, a proto jej tato identifikace zvlášť nepřekvapí. Naopak uživatelé, kteří s biometrickou identifikací nemají žádné zkušenosti, ji považují za ***neobvyklou***. Obvyklost versus neobvyklost se ke každé biometrické technologii vztahuje zvlášť a může být posuzována nejen z pohledu jednotlivce, ale i z pohledu větší skupiny lidí.

Samoobslužné versus s obsluhou

- O aplikaci ***s obsluhou*** se jedná tehdy, jestliže je identifikace kontrolována nebo řízena obsluhou. V opačném případě se jedná o ***samoobslužnou*** aplikaci. Nespolupracující aplikace jsou vždy s obsluhou, zatímco spolupracující můžou být s obsluhou i bez obsluhy.

Standardní versus nestandardní prostředí

- Pod pojmem ***standardní prostředí***, ve kterém biometrické aplikace pracují, se obvykle rozumí průměrná teplota vzduchu 20 – 25°C, atmosférický tlak, průměrná světelnost, prašnost, hlučnost apod. V ***nestandardním prostředí*** pracují takové aplikace, které jsou celoročně vystaveny vnějším klimatickým podmínkám – mrazu, větru, vlhkosti, intenzivnímu slunci atd.

Veřejné versus privátní

- U tohoto typu aplikace lze jen těžko stanovit přesnou hranici mezi veřejným a privátním sektorem. ***Privátní*** charakter bude mít zcela jistě např. vchodové biometrické zařízení do rodinného domu, protože umožňuje vstup pouze rodinným příslušníkům. ***Veřejné*** zařízení lze charakterizovat např. jako jakési „předplatné“, kdy si libovolný zákazník zaplatí vstup do objektu (např. plavecký bazén) a po dobu trvání předplatného je na základě svých biometrických charakteristik automaticky vpouštěn do objektu.

Otevřené versus uzavřené

- Toto členění závisí na tom, zda biometrické zařízení komunikuje s dalšími vzdálenými prvky např. informačními systémy, databázemi apod. Jestliže dochází k výměně dat se vzdálenými technologickými prvky, jedná se ***otevřené*** aplikace. V ***uzavřených*** aplikacích k žádné výměně dat nedochází. Toto členění je důležité z pohledu bezpečnosti. U otevřených aplikací musí být věnována pozornost jak přenosovým kanálům, tak i vzdáleným zařízením.

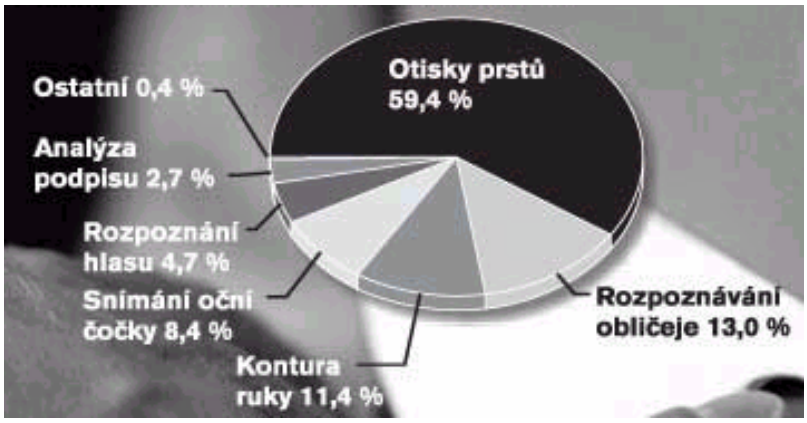
4 BUDOUCNOST A VÝVOJ BIOMETRICKÝCH IDENTIFIKAČNÍCH PROSTŘEDKŮ

Jak je již popsáno v předchozích kapitolách, jednou z největších předností biometrie je náhrada za nejrůznější hesla, klíče nebo vstupní karty. V této oblasti se ve většině

případů objevují systémy, které pracují s otisky prstů nebo dlaní. Výrobci těchto systémů proto neustále experimentují se stále novými a novými možnostmi, jak tyto technologie co nejefektivněji využít. Je pouze otázkou času, kdy budeme platit v obchodech pouhým přiložením palce a platební karty zmizí v „ propadlišti dějin.“

Trh s biometrickými produkty existuje již přibližně 15 let a na trhu jsou dnes kromě snímání otisku prstu/dlaně k dispozici ještě čtyři hlavní typy biometrických technologií, a to: optické snímání sítnice nebo duhovky, snímání obličeje, rozpoznávání hlasového profilu a ověření podpisu. Zatímco všechny typy biometrie pravděpodobně porostou s klesajícími náklady, zlepšováním technologie a nárůstem poptávky, snímání otisku prstu si i nadále udrží největší podíl na trhu a bude nabízet nejlepší kompromis mezi náklady, spolehlivostí a optimálností pro uživatele (obr.37).

Mezi nejperspektivnější oblasti, ve kterých se biometrie v současnosti stále více a častěji využívá a v budoucnu využívat bude, patří bankovnictví, zdravotnictví (identifikace pacientů) a cestování (cestovní doklady). Finanční instituce navíc mohou biometrické systémy využívat samostatně nebo v kombinaci s dalšími typy jako jsou například hesla. U bankomatů je zase možno využívat snímače duhovky nebo sítnice a u telebankingu rozpoznávání hlasu. Díky snížení ceny biometrických systémů si dnes tento způsob zabezpečení mohou dovolit i malé podniky.



Obr. 37: *Podíl jednotlivých technologií biometrických systémů na trhu*

Očekává se rovněž, že do této sféry vstoupí i velké společnosti z oboru informačních technologií, kdy výrobci PC a mobilních telefonů začnou integrovat snímače do svých zařízení.

Jako příklad takového snímače bych uvedl nový notebook od společnosti IBM s označením T42, který obsahuje čtečku otisků prstů integrovanou v opěrce pro zápěstí pod směrovými tlačítky (obr.38). Tato čtečka funguje tak, že uživatel přejede prstem po malém horizontálně orientovaném senzoru, a tím se může přihlásit k systému, softwarovým aplikacím, webovým serverům nebo databázím. Tento typ čtečky otisků prstů zachytí více než klasické políčko, na které se prst pouze přiloží, protože sejme větší plochu konečků prstů, čímž je navíc minimalizována možnost chybné identifikace. Celý proces skenování je přitom otázkou několika sekund.

Obr. 38: *Notebook T42 od společnosti IBM s integrovanou čtečkou otisků prstů*

Dokonce i taková společnost jako je Sony, se v poslední době začala více zabývat biometrikou, a to zejména díky svým produktům Sony "Puppy" a Memory Stick. Skutečnost, že jedna z nejúspěšnějších světových společností pracující v oboru spotřební elektroniky vstupuje na biometrický trh, je důležitou událostí, která v konečném dopadu může ohrozit současné dodavatele biometrického hardware.

Nový produkt z dílen společnosti Sony je v podstatě malá čtečka otisku prstů, která dokáže porovnat sejmutý otisk s tím, který má uložen v paměti, a na základě tohoto porovnání ověřit totožnost uživatele. Díky tomu, že je tento modul na snímání otisků prstů umístěn na kartě, která odpovídá formátu paměťových flash karet Memory Stick, jej lze přenášet a používat v různých zařízeních, jako je PDA nebo PC. Samotný snímač otisku prstů má rozlišení 128 x 128 pixelů.

"Puppy" je navíc vybaveno technologií, která umožňuje uživateli používat svůj prst jako pečetidlo. Tato technologie umožní po autorizaci osoby, kterou právě modul podle otisku prstu rozeznal, pracovat s elektronickým podpisem, tak jako by uživatel zadal svůj klíč. Jinak jej lze samozřejmě využít jako autorizační systém, který vám má umožnit místo psaní hesel používat k přihlašování svůj palec.

Výhodou systému je to, že veškeré kódy jsou umístěny přímo v paměti karty. Nemohou tak být z počítače zcizeny, jako při obyčejném zabezpečení systémů pomocí hesel, kdy je zadané heslo porovnávané s tím, které je nějakým způsobem uloženo na disku.

Obr. 39: *Příklad paměťové karty a produktu Sonny "Puppy" od společnosti Sony*

Pochopitelně, že podobnými produkty se nezabývají pouze celosvětově známé firmy jako IBM nebo Sony, ale i společnosti, které ve světě nejsou tak známé. Příkladem může

být kalifornská společnost DigitalPersona, která uvedla na veletrhu Comdex 2003 zajímavé bezpečnosní řešení nazvané U.are.U Personal.

Bezpečnostní řešení této společnosti, které je určeno pro platformu operačního systému Windows XP, odstraňuje nutnost vkládání přístupových hesel a výrazně zvyšuje úroveň zabezpečení počítače. U.are.U Personal je zařízení složené ze snímače otisku prstu a příslušného programového vybavení. V současnosti společnost DigitalPersona nabízí také snímač otisku prstu v podobě klávesnice s integrovaným snímačem a externí snímač připojitelný k počítači prostřednictvím USB rozhraní. Existuje i modul snímače, který se dá zabudovat prakticky do jakéhokoliv zařízení – toto řešení však nelze pro domácí či kancelářské použití považovat za standardní. Dodávané softwarové vybavení je kompatibilní nejen s Windows XP, ale i zpětně s Windows 98, Windows NT/2000 a Windows ME. Díky němu je možné zcela spolehlivě zabezpečit přístup k aplikacím, jednotlivým souborům, elektronické poště a webovým službám.

Obr. 40: *Zařízení U.are.U Personál od společnosti DigitalPersona*

Mimo společnosti, které vyrábí produkty založené na snímání otisku prstu, se na trhu postupně objevují i firmy zabývající se mimo jiné například i identifikací osob podle obličeje.

Jako příklad bych uvedl Japonskou společnost Omron, která vyvinula novou technologii „OAKO Vision Face Recognition“ určenou pro přenosná zařízení, jako mobilní telefony či PDA. Firma chce tímto krokem přispět k větší ochraně a bezpečnosti uživatelů

mobilních telefonů v případě využívání různých elektronických služeb či při krádeži. Tento systém složený z několika senzorů a software, porovnává pomocí integrované kamery sejmuté obrazy podle několika kritérií, jako jsou tvar očí, obočí nebo nosu a vzdálenosti mezi nimi. Konkrétně to znamená, že chce-li uživatel takové zařízení použít, musí se nejprve sám vyfotografovat, načež mu bude, po porovnání získaných dat s databází, umožněno s tímto zařízením pracovat. Navíc má tento program na základě databáze vytvořené z mnoha tisíc údajů rozpoznat, jakého je osoba pohlaví, jak je přibližně stará či jaké je národnosti.

Výrobce uvádí, že úspěšnost této technologie připadá na devadesát devět případů ze sta a co je pozitivní, že při fotografování nemusí být striktně dodržen úhel, ve kterém se uživatel fotografoval poprvé.

Společnosti Visionics, Wirehoud LCC a Motorola představily novou aplikaci technologie skenování obličejů určenou pro policejní účely. Jedná se mobilní telefon, jenž permanentně sleduje kolemjdoucí a fotografie jejich obličejů odesílá k porovnání do centrální databáze zločinců. Najde-li počítač shodný portrét s dodanou fotografií, okamžitě jej včetně osobních údajů odešle zpět na mobil. Tento telefon má navíc schopnost uchovávat velké množství portrétů přímo ve své paměti, což je nutné kvůli prodlevě při porovnávání s databází. Společnosti sice zaručují, že podobizny „nevinných“ budou z paměti telefonu okamžitě smazány, nicméně veřejné instituce zabývající se ochranou osobních údajů varují před velkým potenciálním zneužitím. Celý systém totiž umožňuje velmi podrobný sběr informací o každém jedinci. A tak nakonec může dojít k tomu, že pokud nastane chybné porovnání portrétů v databázi, stane se nevinný člověk rázem v očích policisty „těžkým zločincem“.

Samozřejmě, že je pouze otázkou času, kdy se k ověření totožnosti uživatele budou používat nejenom uvedené způsoby identifikace, jako je otisk prstu nebo skenování obličeje, ale i technologie využívající charakteristiky člověka, které zatím nejsou běžně známé.

Ač to zní neuvěřitelně, skupina vědců z VTT (Technického výzkumného centra) ve Finsku vyvinula speciální technologii, která má znemožnit krádeže kapesních zařízení a

mobilních telefonů, a to na základě detekce změn fyzického pohybu majitele mobilního zařízení.

Unikátní technologie využívá speciální senzory instalované v mobilním zařízení, které dokáží změřit určitý charakteristický způsob chůze uživatele. Získané údaje se pak automaticky ukládají v paměti přístroje. Na základě průběžného měření senzory porovnávají data s již uloženými hodnotami. V případě, že se odlišují, přístroj automaticky „zamrzne“ a jeho další využití si vyžádá přístupové heslo.

„ Jednou z hlavních výhod této biometrické metody je její nenáročnost, kdy na straně uživatele nevyžaduje žádnou speciální akci,“ podotýká ředitel výzkumu Heikki Ailisto. A dodává: „ V porovnání s hesly a dalšími biometrickými metodami identifikace, senzor založený na technologii rozpoznávání způsobu chůze potvrzuje identitu jednoduše, aniž by samotný uživatel musel nějakým způsobem zakročit.“ Přestože nová technologie není zcela bezchybná – technologie si musí přivyknout na změnu chůze uživatele zapříčiněnou například výměnou obuvi a navíc požadované senzory nejsou stále příliš rozšířené kvůli vysoké ceně – Ailisto doufá, že tato nová patentovaná technologie by se mohla v nových mobilních telefonech a PDA zařízeních objevit v průběhu příštího roku.

Nejenom světové společnosti se zabývají výrobou takovýchto zařízení, ale například také Pentagon pracuje na technologii, která umožní rozpoznat člověka podle jeho chůze. V rámci kontroverzního programu „Total Information Awarenes (TIA)“ jsou právě Pentagonem podporovány různé projekty, které mají na jednu stranu ochránit americkou veřejnost před různými „nekalými živly“, ale na druhou stranu zasahují až příliš do soukromí.

Jedním z takových projektů je práce na technologii využívající teorii o jedinečnosti lidské chůze. Tato teorie tvrdí, že každý jedinec má při chůzi natolik specifické pohyby, že je možno jej podle nich jednoznačně identifikovat. V podstatě je prý možno originalitu chůze přirovnat například k originalitě podpisu. Na základě této teorie byl vyvinut systém, jenž prostřednictvím radaru, kterému nečiní potíže ani tma či mlha, snímá lidskou chůzi a získaná data následně vyhodnotí a porovná s databází. Vývoj této technologie Pentagon financoval na Technologickém Institutu v Georgii a výsledkem výzkumu byl systém, jehož úspěšnost se při identifikaci osob pohybovala v rozmezí 80 – 95 %. Ačkoliv se to může

zdát málo, ve spolupráci s dalšími identifikačními systémy může být například v oblastech, kde se vyskytuje větší počet osob vybráno několik podezřelých, které bude snadnější prověřit.

Výhodou takového zařízení je jeho využití i za ztížených podmínek, kde jiné bezkontaktní identifikační systémy nemusejí tak dobře fungovat. To zařízení je navíc možné nasadit v prostorách, kde je z nějakého důvodu potřeba, aby lidé, kteří se v něm pohybují nevěděli, že jsou prověřováni.

Pochopitelně, že kromě uvedených zařízení určených pro mobilní telefony, PDA zařízení nebo ochranu počítačových či osobních dat, nacházejí v poslední době široké uplatnění zejména na letištích v podobě biometrické čtečky obličejů, otisků prstů, popř. skenu oční duhovky.

Podle tiskové zprávy společnosti Siemens začalo v loňském roce přibližně 400 zaměstnanců letecké společnosti Lufthansa na letišti ve Frankfurtu testovat nový způsob odbavování a nastupování cestujících do letadel, který je založen na snímání otisků prstů. Celý systém by tak měl přispět k rychlejšímu, bezpečnějšímu a efektivnějšímu odbavování cestujících. Tato technologie byla vyvinuta a implementována společností Siemens Business Services za podpory dceřiné softwarové společnosti Siemens PSE.

Ve druhé fázi, která bude zahájena v letošním roce, bude projekt nazvaný „Trusted Traveller“, převeden do reálného provozu na hlavním letišti a bude také fungovat na druhém pilotním letišti, kde jej budou moci zpočátku dobrovolně využívat pouze cestující, kteří často létají. Systém funguje tak, že při odbavení na terminálu jsou pasažérům společnosti Lufthansa sejmuty otisky prstů, jež jsou následně uloženy do databáze. Otisky prstů jsou poté společně s informacemi získanými při odbavení vytištěny na palubní lístek do podoby čárového kódu. Následně je při nastupování do letadla tento kód porovnán s vlastním otiskem prstu cestujících a pokud se údaje shodují, je jim umožněn vstup do letadla.

Nejenom pasažéři společnosti Lufthansa budou při nastupování do letadla odbavováni pomocí otisků prstů, ale také například cestující na londýnském letišti Heathrow budou namísto předkládání pasů podrobováni kontrole oční duhovky. Tím se

londýnské Heathrow stane prvním letištěm v zemi, které vyzkouší zařízení, jenž nascanuje duhovku každého cestujícího a následně ji uloží do paměti počítače. Při nastupování do letadla pak cestující budou procházet kabinkou, ve které počítač porovná jejich duhovku s předem získanými informacemi uloženými v databázi. Celý proces by přitom neměl trvat déle než dvě minuty.

Mezi další letiště, které využívá digitální technologie snímání otisků prstů a rozpoznávání obličejů, patří mezinárodní letiště Palm Beach v Miami. Vedení letiště vidí hlavní smysl tohoto systému zejména v zajištění povolení vstupu pro pracovníky, kteří mají přístup do bezpečnostních letištních zón, jako jsou např. letištní plocha nebo rampy k letadlům. Navíc chce těmito kroky snížit potenciální rizika teroristických útoků.

Otisky prstů, které se získají pomocí nového snímacího zařízení na letišti v Palm Beach, jsou nejprve digitalizovány a poté zaslány přes Internet do FBI ve Washingtonu. Ta poté provede porovnání těchto souborů s databází otisků prstů známých zločinců. Výsledek této analýzy je pak umístěn na zabezpečenou webovou stránku, na kterou mají přístup pouze vybraní pracovníci letiště. Mluvčí letiště k tomu uvedla, že nový digitální systém výrazně urychlí proces přístupu pro zaměstnance, kteří pracují v kritických letištních zónách, brigádníky, nebo pro ty zaměstnance, jenž nemají své identifikační karty. Výsledek analýzy od FBI by měl být k dispozici do 48 až 72 hodin od doby odeslání otisků.

Daleko kontroverzněji vyznívá program, který se zabývá digitálním rozpoznáváním obličejů lidí na letišti, jenž vzápětí porovnává tyto obrazy s fotografiemi teroristů uložených v elektronické databázi. V případě, že se porovnávaný vzorek bude shodovat s některou z uložených fotografií, budou ihned upozorněny patřičné instituce. V opačném případě budou nasnímané fotky kolemjdoucích po negativním porovnání s databází ihned smazány.

Zkušební provoz bude vyžadovat instalaci malé databáze obsahující obličeje některých nejhledanějších zločinců v Americe a také naskenované fotografie zaměstnanců letiště. „Pracujeme s pravděpodobnostmi, “ řekl John Costanzo, viceprezident společnosti ATC, jenž je systémovým integrátorem tohoto zařízení. A dodal: „Zajímá nás počet úspěšných a neúspěšných přiřazení i další podobné hodnoty, abychom mohli systém vyladit

tak, aby se mohl stát nedílnou součástí bezpečnostní ochrany, jako jsou dnes např. detektory kovů.“

Pokud se po ukončení zkušebního provozu vedení letiště rozhodne ponechat a zakoupit tento systém, bude vše záležet na právnících a zástupcích letiště, aby rozhodli, které fotografie zločinců budou uloženy v permanentní databázi. Po uvedení do plného provozu bude pak systém schopný obsahovat až 30 000 fotografií podezřelých osob. Zatím ale není zcela jasné, jak bude tento systém nakonec využit.

ZÁVĚR

Použití biometrických identifikačních metod má v současné době vzestupnou tendenci, zejména v souvislosti s růstem mezinárodního terorizmu. Rychlé zdokonalování počítačových technologií zjednodušuje naléhavou potřebu spolehlivého prokazování identity osob. Kromě dosud známých metod biometrické identifikace lze podstatná zlepšení očekávat zejména při výzkumu DNA v lékařských vědách a v genovém inženýrství. Pokroky v této oblasti mohou v budoucnu přinést efektivnější metody a prostředky použitelné k identifikaci jedince ve větším rozsahu zejména pro běžnou praxi.

Rychlý rozvoj biometrických technologií a jejich uplatňování v praxi v posledních letech vyžadují pečlivé zkoumání zejména v souvislosti s ochranou dat a platnou legislativou. Široké používání těchto technologií vede k obavám souvisejících s ochranou práv a svobod jednotlivců.

Na uvedenou problematiku, která je velmi aktuální se názory značně různí a dají se rozdělit zpravidla do dvou skupin. Jednu skupinu tvoří lidé, kteří podporují zavedení všestranných opatření na zvýšení společenské bezpečnosti a druhá je tvořena lidmi, jenž se obávají možnosti zneužití těchto prostředků na omezení individuální svobody a manipulace ústící do osobního ohrožení.

I když mnoho lidí nesouhlasí se zaváděním biometrie do běžného života, přesto využití biometrických identifikačních prostředků ve větší míře poslouží k lepšímu zabezpečení ochrany dat, objektů a také zdraví a života lidí. V souvislosti s rychlým vývojem biometrie se tak v budoucnu můžeme setkat s mnohými nečekanými alternativami a zvýšeným synergetickým efektem ve více oblastech.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] Porada, Viktor a kol. *Kriminalistika*. Akademické nakladatelství CERM, s. r. o. Brno, 2001, str. 215-216. ISBN 80-7204-194-0.

[2] Čandík, Marek. *Objektová bezpečnost II*. Univerzita Tomáše Bati ve Zlíně 2004, str.39-57. ISBN 80-7318-217-3.

[3] Rak, Roman. *Biometrická identifikace a verifikace*. In: Security Magazín, Roč. X., vyd. 53, 3/2003. Family media, spol. s. r. o., Praha, 2003, str. 56-59. ISSN 1210-8723.

[4] Rak, Roman. *Biometrická identifikace a verifikace*. In: Security Magazín, Roč. X., vyd. 54, 4/2003. Family media, spol. s. r. o., Praha, 2003, str. 32-36. ISSN 1210-8723.

[5] Rak, Roman. *Technologie digitálního snímání otisků prstů*. In: Security Magazín, Roč. XII., vyd. 66, 4/2005. Family media, spol. s. r. o., Praha, 2003, str. 2-5. ISSN 1210-8723.

[6] Vokůrková, Lenka. *Zloději mobilů třeste se!*. In: Computerworld, Roč. XVI., 37/2003. IDG Czech, a.s., Praha, 2005, str. 15. ISSN 1212-6510.

[7] Flohr, Manfred. *512 bajtů v oku*. In: CHIP, 8/2005. Vogel Burda Communications, s. r. o., Praha, 2005, str. 28-30. ISSN 1210-0684.

Internetové zdroje:

[8] Pužmanová, Rita. *Biometrické systémy v praxi:* IT SYSTEM 3/2004 – BEZPEČNOST [online]. [cit. 2003-03-21]. Dostupný z WWW: <http://www.systemonline.cz/site/bezpecnost/04 02puzman.htm>

[9] Vach, Martin. *Historie biometrik a jejich využiti ve výpočetní technice:* [online]. [cit. 2004-11-20]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm>

[10] Bitto, Ondřej. *Biometriky nejen v pasech (1.):* [online]. [cit. 2005-09-21]. Dostupný z WWW:
<http://www.lupa.cz/clankek.php3?show=4341>

[11] Ďásek, Milan. *Biometrika (referát do BIS):* [online]. [cit. 2003-02-26]. Dostupný z WWW:

<http://www.volny.cz/pretorian/biometrika.html>

[12] *Identifikace osoby na základě tvaru ucha a jeho otisků - II.:* Kriminalistika [online]. [cit. 2004-02-18]. Dostupný z WWW:

<http://www.mvcr.cz/2003/casopisy/krim/0402/ident_info.html>

[13] Všetečka, Roman. *Chraňte si PC otiskem svého prstu. Stačí vám karta velikosti Memory Stisk!:* [online]. [cit. 2003-01-27]. Dostupný z WWW:

<http://technet.idnes.cz/hardware.asp?r=hardware&c=A030124_5186854 hardware>

[14] Zouzalík, Marek. *Otisk palce: Bezpečný přístup k počítači…?:* [online]. [cit. 2001-11-15]. Dostupný z WWW:

<http://technet.idnes.cz/hardware.asp?r=hardware&c=A011115 0044245 hardware>

[15] *Biometrie, biometrika - geneze, vývoj a současné pojetí:* Kriminalistika [online]. [cit. 2005-01-12]. Dostupný z WWW:

<http://www.mvcr.cz/2003/casopisy/krim/0501/vanco info.html>

[16] *Biometrická identifikační zařízení:* Specialista [online]. [cit. 2005-09-26]. Dostupný z WWW:

<http://www.specialista.info/view.php?cisloclanku=2005100401>

[17] Škopek, Pavel. *Poznáme tě podle očí, chůze a tvaru ucha (Co to je biometrie?):* [online]. [cit. 2004-04-11]. Dostupný z WWW:

<http://technet.idnes.cz/hardware.asp?r=hardware&c=A041103_5285953 hardware>

[18] Featherly, Kevin. *Bezpečnost na letištích zvýší digitální scanování obličejů a otisk prstů:* [online]. [cit. 2002-02-07]. Dostupný z WWW:

<http://www.isdn.cz/clanek.php?cid=3566>

SEZNAM OBRÁZKŮ

SEZNAM TABULEK