Biometrické metody identifikace osob v bezpečnostní praxi

Studijní text

VŠB TU Ostrava,
Fakulta bezpečnostního inženýrství,
Katedra bezpečnostního managementu,
Oddělení bezpečnosti osob a majetku

Mgr. Ing. Radomír Ščurek, Ph.D.

Červen 2008

Obsah:

1 Biometrie a základní pojmy

Biometrie (biometric) je vědní obor zabývající se studií a zkoumáním živých organismů (bio-), především člověka, a měřením (-metric) jeho biologických (anatomických a fyziologických) vlastností a také jeho chováním, tzn. behaviorálních charakteristik. Pojem biometrika je odvozený z řeckých slov "bios" a "metron". První znamená "život", druhé pak "měřit, měření". Kdybychom se chtěli držet doslovného překladu, zněla by biometrie jako "měření živého". V přeneseném významu jde ovšem o měření a rozpoznávání určitých charakteristik člověka. Biometrika se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností. V zahraniční je pojem biometric přímo vykládán jako proces automatizované metody rozpoznávání jedince založený na měřitelnosti biologických a behaviorálních vlastností (dle NSTC – Nation Science and Technology Council – Národní rada pro vědu a technologii USA, Výboru pro vnitrostátní a národní bezpečnost).

Rozpoznávání lidí pomocí biologických charakteristik je metoda využívaná historicky, lidé se rozpoznávají pomocí vzhledu tváře nebo jsou známy otisky dlaní v jeskyních jako jakýsi podpis autora (některé z nich jsou až 30 000 let staré). S rozvojem počítačových technologií na konci 60. let se začalo i biometrické rozpoznávání člověka stávat automatizovaným.

V problematice biometrie je nutné správně rozumět základním pojmům, jelikož mají původ v anglickém jazyce a do češtiny bývají občas nesprávně překládány.

Recognition (rozpoznávání) je druhový termín, který nutně nemusí znamenat identifikaci ani verifikaci. Jedná se o rozpoznávání člověka použitím vhodné tělesné vlastnosti.

Verification (ověření nebo verifikace) označuje proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku s již dříve zapsaným (tzv. šablonou neboli template). Jedná se o tzv. princip one-to-one. Identification identifikace je proces, kdy se biometrické systém pokouší určit totožnost neznámého jedince. Biometrická informace je sejmuta a porovnávána se všemi uloženými vzorky (šablonami). Princip je znám jako one-to-many.

Authentication (autentifikace, autentizace nebo legalizace) je pojem, který lze sloučit s termínem rozpoznávání. Ovšem na konci procesu v tomto případě získá uživatel určitý status, např. oprávněný/neoprávněný atd.

Aplikace lze uplatnit například:

- Docházka, komerční organizace všeho druhu (výrobní, obchodní, instituce, atd.) s hodinovou i úkolovou mzdou
- Přístupové systémy, fyzická kontrola vstupů: režimová pracoviště, výpočetní centra, atomové elektrárny (75% atomových elektráren v USA používá HandKey), vývojové laboratoře, komunikační centra, vojenské objekty, kritická místa v nemocnicích, kanceláře vedoucích pracovníků, atp.
- Osobní identifikace, stravovací systémy, identifikace majitele karty, elektronický podpis

1.1 Metody autentizace

Všechny systémy pracující s automatizovaným přístupem jsou závislé především na principu, kterým je přístup zabezpečen. V základě existují tři mechanismy pojetí, použití hesla, předmětu nebo biometrického prvku.

1.1.1 Autentizace heslem

Použití hesla jako prostředku pro přístup do systému je stále nejpoužívanějším principem zabezpečení. Velký podíl na tom má i jeho globální použití v osobních počítačích, počítačových sítí, emailových účtech, u SIM karet mobilních telefonů a u platebních karet. Bezpečnost je v tomto případě zajištěna tím, že si omezený počet uživatelů (nejlépe jeden) pamatuje určitou posloupnost znaků, kterou mu umožní přístup do chráněné oblasti. Výhody hesel jsou snadný způsob realizace a nízká cena pořízení. Velká řada nevýhod ovšem použití hesel omezuje na systémy s nízkým stupněm zabezpečení. Mezi největší nevýhody patří možnost dekódování speciálními programy, zapomenutí nebo vysledování neoprávněnou. Bezpečnost lze v omezené míře zvýšit používáním vhodných zásad, jako je složení z malých i velkých písmen nebo speciálních znaků, dostatečná délka, neobvyklost slova nebo fráze

a nesouvislost s osobou vlastníka. Zároveň musí být měněno v pravidelných intervalech, nesmí být nikde poznamenáváno a musí být distribuováno zabezpečeným způsobem.

1.1.2 Autentizace předmětem

Bezpečnost tohoto principu je zaručena vlastnictvím speciálního předmětu – tokenu, který je pro přístup do systému vyžadován. Token je jedinečný předmět, co možná nejhůře kopírovatelný, vybavený informací nutnou pro autentizační protokol, čímž se ověří identita uživatele. Výhodou a zároveň nevýhodou tokenu je jeho přenositelnost, proto by měl být token vždy používán jen v kombinaci s heslem anebo jako nositel biometrického vzorku uživatele. V praxi používanými tokeny jsou:

- tokeny pouze s pamětí (magnetické, elektronické nebo optické karty) jako obdoba mechanického klíče
- tokeny s heslem – vyžadují zadání hesla zároveň s použitím, např. platební karty
- logické tokeny – dokáží zpracovávat jednoduché podněty, např. vydej klíč/cyklickou sekvenci klíčů
- inteligentní token – mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, mohou umět šifrovat a generovat náhodná čísla

1.1.3 Biometrická autentizace

Biometrika využívá jedinečných tělesných znaků pro identifikaci osoby. Výhodou tohoto typu autentizace je, že není nutné pamatovat si několika místné kombinace hesel či neustále s sebou nosit snadno zcizitelný token, např. přihlašovací kartu. Biometrická autentizace je rychlou a pohodlnou a velice přesnou metodou, která je navíc levným řešením, vzhledem ke svým neexistujícím pozdějším nákladům. Její hlavní výhodou je skutečnost, že biometrické charakteristické znaky zůstávají během života neměnné a nelze je ukrást či zapomenout.

Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik a jejich následné porovnávání s údaji předem sejmutými. Cílem v oblasti bezpečnosti je vytvoření komplexních systémů založených na kombinaci měření více charakteristik. Tím se bezpečnost těchto systémů mnohonásobně zvýší. Současné biometrické

systémy pracují s různými charakteristickými znaky člověka, jako jsou otisk prstu, geometrie tváře, duhovka oka, sítnice oka, geometrie ruky, geometrie prstů, struktura žil na zápěstí, tvar ucha, složky lidského hlasu, lidský pach, DNA, dynamika podpisu a dynamika psaní na klávesnici a další. Výčet a popis některých je popsán dále v tomto textu.

Výhody biometrické autentizace jsou především:

- vysoký stupeň spolehlivosti: osvědčené technologie lze jen obtížně oklamat
- nulové provozní náklady: žádná režie spojená s procesem autentizace
- rychlost
- praktičnost: není co ztrácet ani přenášet
- zřejmost: výsledek je jednoznačný a okamžitý
- efektivnost: přímé datové propojení s databází a počítači
- cena: příznivá ve vztahu k bezpečnosti a v poměru cena/výkon, neexistující dodatečné náklady

Porovnání autentizačních metod

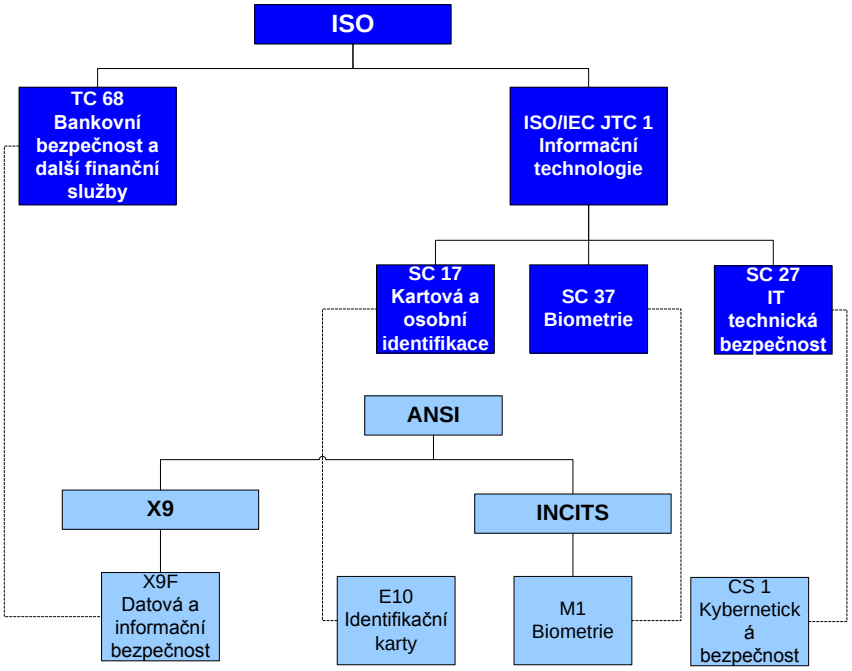
Hesla lze použít pouze pro nejnižší stupně zabezpečení. Lze se jich relativně snadno zmocnit a jsou přenositelné. Tokeny lze použít pro vyšší stupně zabezpečení. Lze se jich snadno zmocnit a jsou přenositelné. Kombinace tokenu a hesla lze použít pro poměrně vysoký stupeň zabezpečení. Kombinace je značně odolná při odcizení nebo ztrátě tokenu, avšak opět může selhat lidský činitel a může dojít k vyzrazení hesla a zapůjčení tokenu. Jsou přenositelné. Biometrické znaky člověka lze použít pro nejvyšší stupeň zabezpečení. Nelze je ztratit ani předat, jsou nepřenositelné.

Souhrnně lze konstatovat, že každý typ zabezpečení je možno podrobit útokům. Tyto hrozby lze snížit použitím jednotlivých autentizačních metod ve vzájemných kombinacích. Použití biometrické specifické vlastnosti člověka v automatických systémech řízení a kontroly vstupů však představuje v současnosti nezastupitelný prostředek pro dosažená nejvyššího stupně zabezpečení objektu.

2 Elektronické biometrické rozpoznávací systémy

Využití elektronických biometrických rozpoznávacích systému v praxi má široké uplatnění, ať už se jedná o soukromou nebo forenzní sféru. Ve forenzní (soudní, kriminalistické a vyšetřovací) sféře je světově nejznámější a nejvíce používaný systém AFIS (Automated Fingerprint Identification Systém - Automatický systém pro identifikaci dle otisku prstu), vyvinutý vládou USA ve spolupráci s FBI (Federal Bureau of Investigation - Národní úřad pro vyšetřování) a NSTC. Tento systém je instalován i v České republice v Praze pod názvem AFIS200, který byl dodán společností De Lat Rue Printrac, v ceně přes 100 miliónů Kč. Podobné systémy pracující na jiných principech než je otisk prstu lze najít v mnoha státech světa. Velký rozmach nastává s automatickou identifikací dle DNA a systémů pracujících na průběžném vyhodnocování geometrie tváře osob v davu (použitelný na nádražích, letištích, rušných náměstí atd.) Velký vliv na jejich implementaci v každém státě má i postoj odpovědných osob. Dále je nutno poznamenat rozvoj biometrické identifikace u cestovních pasů a při bankovních peněžních transakcí.

Jak je ovšem zřejmé z ceny pořízení takovýchto systémů, je zcela nepřijatelné uvažovat o jejich implementaci v komerční sféře. K dosažení redukce ceny je nutné přehodnotit princip systému. Hlavní rozdíl u soukromého systému je především v mnohem menší databázi jak biometrických vzorků tak i samotných osob. Taktéž není např. u otisků prstů nutné ukládat otisky všech deseti prstů, jak to mu bývá v kriminalistické sféře, ale pouze jen jednoho. Proto si systém vystačí z mnohem menší kapacitou paměti a hlavně operačním výkonem, který jde ruku v ruce s cenou celého systému.



Obrázek č. 1: Subordinace a spolupráce orgánů při tvorbě technických norem

2.1 Biometrické systémy řízení a kontroly vstupů

Systémy kontroly a řízení vstupů v bezpečnostních aplikacích (ACS – Access Control Systems) hlídají vstup do chráněných prostor a vstup do těchto prostor umožňují pouze uživateli, který se prokazuje nějakou metodou autentizace. ACS systémy spadají pod normu ČSN EN 50133. Verifikace značí ověřovací proces v systému ACS, který vždy vyžaduje přihlášení uživatele do systému, kde je poté provedeno porovnání neskenovaného záznamu se záznamem v databázi. Je důležité omezit počet možných přihlašovacích pokusů, než bude uživatel systémem definitivně odmítnut jako nepovolaná osoba. Pro daný počet přihlašovacích pokusů je nutné vzít v úvahu úroveň zabezpečení systému. Čím menší počet pokusů je zvolen, tím s větší pravděpodobností vyvoláme několik falešných poplachů kvůli neprovedené identifikaci oprávněného uživatele. Na druhou stranu je ale nutné zvolit takový počet pokusů, aby neoprávněný uživatel neměl čas získat dostatek informací o systému, které by mu později pomohly systém prolomit.

U vysoce zabezpečených systémů by měly být výsledky verifikace pro pozdější zpracování ukládány. Nabízí se tři možnosti: přímo do zařízení (do hlavní jednotky snímače) nebo do vzdáleného počítače nebo přímo do tokenu pokud je použit. Ukládání přímo

do snímače je nevýhodné vzhledem k omezené paměti jednotky a ke snadnějšímu přístupu k uloženým datům pro narušitele. Při plné paměti by starší záznamy byly přepsány novějšími. Při ukládání do vzdáleného počítače není proces omezen velikostí paměti, ale existuje určité nebezpečí průniku do systému zvnějšku, čili je nutné tuto komunikaci i samotnou databázi dále zabezpečit. Třetí způsob, ukládání dat do tokenu, je nevýhodný z hlediska nutnosti složitější elektroniky a rozhraní pro token, tedy z hlediska ceny řešení a stupně zabezpečení.

2.2 Princip biometrických systémů řízení a kontroly vstupů

Předpokladem pro provedení biometrické autentifikace je sejmutí a zápis biometrické vlastnosti osoby, která je dále uložena jako osobní referenční šablona buď decentralizovaně na čip ID karty nebo počítače, nebo centrálně do datové paměti systému nebo aplikace. Je nutné provádět snímání a zápis opatrně, jelikož kvalita pořízeného obrazu má zásadní vliv na proces autentifikace. Je zřejmé, že proces snímání musí být prováděn v důvěryhodném prostředí. Většina biometrických systémů pracuje s následujícím postupem:

- Pořízení datového souboru (obraz, zvuk, atd.), který obsahuje biometrickou vlastnost, která z něj jde vyextrahovat použitím vhodného snímače (senzoru).
- Prověření kvality dat: pokud jejich kvalita nevyhovuje, jsou okamžitě odmítnuta nebo je uživateli poskytnuta vhodná rada pro zvýšení kvality sejmuté biometrické vlastnosti (např. upozornění na směr snímání, polohu části těla atd.)
- Vyextrahování požadované biometrické veličiny z datového souboru a vytvoření šablony vzorku
- Zápis: uložení šablony jako referenční šablony do archívu referenčních šablon systému či aplikace (dle definování místa ukládání)
- Ověřování: porovnání aktuální (vyžadované) šablony s referenční šablonou užitím algoritmu pro určení shody a vygenerování hodnoty (skóre), která je rozhodná pro determinování stupně shody
- Výsledek ověřování: pokud skóre shody překročí předdefinovanou hranici, tak je přístup umožněn, v opačném případě je žádost odmítnuta.

Biometrické informace používané pro identifikaci

Kritéria pro výběr biologické nebo behaviorální vlastnosti člověka určené pro jeho další identifikaci jsou determinována co nejširším a nejefektivnějším způsobem užití. Takto vhodná vlastnost člověka musí splňovat:

- jedinečnost: vlastnost musí být co možná nejvíc výjimečná, tzn. že se shodná vlastnost nesmí objevit u dvou lidí zároveň
- univerzálnost: vlastnost musí být měřitelná u co možná největší množiny lidí
- trvalost: vlastnost se nesmí měnit v čase
- měřitelnost: vlastnosti musí být měřitelné shodnými technickými zařízeními
- uživatelská přijatelnost: vlastnost musí být snadno a pohodlně měřitelná

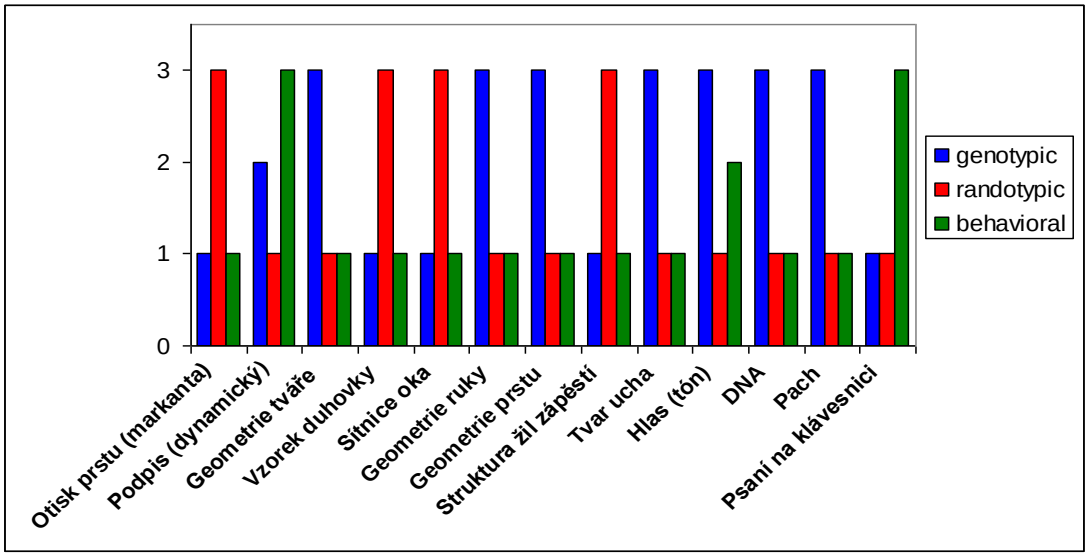
Nejlépe prozkoumané a nejvíce rozšířené biometrické vlastnosti používané pro identifikační účely jsou uvedeny níže spolu se stručným popisem toho, co se měří:

- otisk prstu (struktura papilárních linií a jejich detailů)
- dynamika podpisu (rozdíly v tlaku a rychlosti psaní)
- geometrie tváře (vzdálenosti specifických částí – oči, nos, ústa…)
- duhovka oka (obrazový vzorec duhovky)
- sítnice oka (struktura žil na očním pozadí)
- geometrie ruky (rozměry dlaně a prstů)
- struktura žil na zápěstí (struktura žil)
- tvar ucha (rozměry viditelné části ucha)
- hlas (tón a zabarvení hlasu)
- DNA (řetězec deoxyribonukleové kyseliny)
- pach (chemické složení)
- psaní na klávesnici (rytmus úderů do klávesnice PC)

Způsoby, kterými biometrické vlastnosti člověka vznikají, jsou v základě tři:

- skrze genetický vývoj: uplatňuje se vliv dědičnosti (DNA) – genotypické
- skrze náhodné varianty vzniku v časném stádiu vývoje embrya – randotypické
- skrze učení a výchovu: chování jedince – behaviorální

Je dokázáno, že všechny tři faktory přispívají k vývoji biometrické vlastnosti, ačkoliv každý v jiné míře. Obrázek č. 2 je popisuje relativní vliv vývojových vlastností na jednotlivé biometrické znaky a přehledně hodnotí relativní důležitost jednotlivých faktorů (1 znamená zanedbatelný vliv, 3 významný vliv).



Obrázek č. 2: Vliv vývojových vlastností na jednotlivé biometrické znaky a jejich porovnání

Na obrázku č. 3 jsou v tabulce přehledně popsány výhody a nevýhody jednotlivých biometrických znaků.

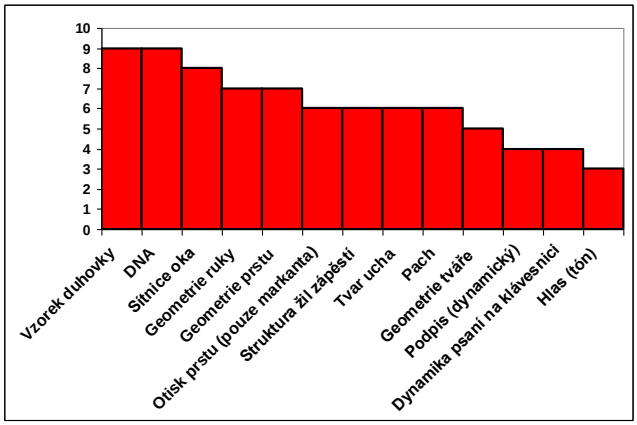
Biometrická vlastnost	komfort	přesnost	dostupnost	cena
Otisk prstu	ooooooo (7)	ooooooo (7)	oooo (4)	ooo (3)
Podpis (dynamický)	ooo (3)	oooo (4)	ooooo (5)	oooo (4)
Geometrie tváře	ooooooooo (9)	oooo (4)	ooooooo (7)	ooooo (5)
Vzorek duhovky	oooooooo (8)	ooooooooo(9)	oooooooo (8)	oooooooo (8)
Sítnice oka	oooooo (6)	oooooooo (8)	ooooo (5)	ooooooo (7)
Geometrie ruky	oooooo (6)	ooooo (5)	oooooo (6)	ooooo (5)

Geometrie prstu	ooooooo (7)	ooo (3)	ooooooo (7)	oooo (4)
Struktura žil zápěstí	oooooo (6)	oooooo (6)	oooooo (6)	ooooo (5)
Tvar ucha	ooooo (5)	oooo (4)	ooooooo (7)	ooooo (5)
Hlas (tón)	oooo (4)	oo (3)	ooo (3)	oo (2)
DNA	o (1)	ooooooo (7)	oooooooooo(9)	oooooooooo(9)
Pach	?	oo (2)	ooooooo (7)	?
Psaní na klávesnici	oooo (4)	o (1)	oo (2)	o (1)
Srovnání: heslo	ooooo (5)	oo (2)	oooooooo (8)	o (1)

zelená = nejlepší; červená = nejhorší

Obrázek č. 3: Porovnání jednotlivých biometrických vlastností

Jak již bylo zmíněno jedním z nejdůležitější požadavků na biometrickou vlastnost je její stálost v čase, aby nemohlo dojít k její kompromitaci se stárnutím člověka. Důvodů proč se vlastnost může změnit je několik. Vliv růstu živé tkáně, opotřebení, biologické stárnutí, špína a nečistoty, zranění a následné hojící procesy a nespecifikované vlivy. Biometrické vlastnosti, které jsou nejméně ovlivněné těmito možnostmi a jsou nejvíce upřednostňovány. Stupeň stálosti v čase je znázorněna v následujícím grafu č. 1 (10 znamená nejvyšší stálost v čase, 0 nejnižší).



Graf 1: Stálost biometrické vlastnosti v čase

Z poměrně široké škály možností využití jedinečné vlastnosti člověka je nutné se praxi umět správně rozhodnout, který princip zvolit. Ke srovnání jednotlivých principů srovnávání jsou stanovena určitá kritéria. Je zřejmé, že bude preferována taková biometrická vlastnost, která bude pro uživatele i správce komfortní, navíc bude dostatečně přesná, dostupná pro co identifikování co možná největšího okruhu lidí a zároveň bude i cenově přijatelná.

Je těžké definovat optimální biometrickou metodu. V poměru cena a přesnost vychází nejlépe otisk prstu. Duhovka oka má vysoké hodnocení ve všech kategoriích v případě, že cena nehraje roli, vychází duhovka oka nejlépe. DNA ztrácí body v komfortu snímání a také v přesnosti, protože jednovaječná dvojčata mají shodnou DNA.

2.3 Měření výkonnosti biometrických systémů

Efektivnost biometrických rozpoznávacích systémů lze měřit mnoha statistickými koeficienty. Charakteristickými výkonnostními mírami jsou koeficient nesprávného přijetí, koeficient nesprávného odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu a doba ověření. Takových koeficientů existuje ovšem celá řada v závislosti na hloubce zkoumání problému.

False Acceptance Rate (FAR)

Koeficient FAR udává pravděpodobnost toho, že neoprávněná osoba je přijata jako oprávněná. Jelikož nesprávné přijetí může často vést ke vzniku škody, FAR je především koeficient udávající míru bezpečnosti. Označuje se jako chyba II. druhu. Jde o přijetí, připuštění neregistrované osoby do systému, a tato osoba nemá za normálních podmínek oprávněný přístup do systému. Jde o chybu velmi závažnou; kritickou z bezpečnostního i marketingové hlediska.

$$FAR = \frac{N_{FA}}{N_{IIA}} \cdot 100 \ [\%]$$

N_{FA} - počet chybných přijeti
N_{IIA} - počet všech pokusů neoprávněných osob o identifikaci

False Rejection Rate (FRR)

Koeficient FRR udává pravděpodobnost toho, že oprávněný uživatel je systémem odmítnutý. FRR je především koeficient udávající komfort, protože nesprávné odmítnutí je pro uživatele nepříjemné. Označuje se jako chyba I. druhu. Jde o odmítnutí, nerozpoznání osoby, která je v systému registrována a má do něj za normálních podmínek oprávněný přístup. Jde o chybu, která nemá z bezpečnostního hlediska velký význam. Ale jde o marketingově nevýhodnou chybu, protože nutí oprávněného uživatele k opakování pokusu o přístup a to má za následek jeho nespokojenost.

$$FRR = \frac{N_{FR}}{N_{EIA}} \cdot 100 \ [\%]$$

N_{FR} – počet chybných odmítnutí
N_{EIA} - počet všech pokusů oprávněných osob o identifikaci

Chyby FFR a FAR jsou kromě častého vyjádření v procentech vyjadřovány i poměrem. Např. FAR 0,001% odpovídá poměru 1: 100 000. V tomto případě to znamená, že jeden ze sto tisíc neoprávněných pokusů může být připuštěn do systému.

Failure to Enroll Rate (FTE nebo FER)

Udává poměr osob, u kterých selhal proces sejmutí vlastnosti. Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti, která se snímá. Lze poté určit i tzn. osobní FER (Personál FER) udávající vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání. V případě, že byla uživateli správně sejmuta biometrická vlastnost, avšak systém ho chybně odmítl i po mnoha identifikačních/verifikačních pokusech, mluvíme o tzv. Koeficientu selhání přístupu FTA (Failure To Acquire).

Abychom získali spolehlivé statistické údaje, je nutno provést velké množství pokusů o sejmutí biometrické vlastnosti. Pravděpodobnost neúspěchu sejmutí vlastnosti konkrétní osoby se vypočte podle vzorce .

$$FER(n) = \frac{počočneúspesných\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n}{celkovy\ pocet\ pokusů\ o\ zápis\ u\ 1\ osoby\ (nebo\ 1\ vlastnosti)\ n} \quad (1.1)$$

Čím více pokusů provedeme, tím lepší hodnoty nám vycházejí. Celkové FER pro N účastníků (uživatelů) je definován jako průměr z FER(n) podle vzorce.

$$FER = \frac{1}{N} \cdot \sum_{n=1}^{N} FER(n) \quad (1.2)$$

Čím více uživatelů se bude započítávat, tím přesnější hodnoty nám budou vycházet.

False Identification Rate (FIR)

Koeficient FIR udává pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně přiřazena k některému referenčnímu vzorku. Přesná definice závisí na principu, kterým se přiřazuje pořízený vzorek k referenčnímu, jelikož se často stává, že po srovnávacím procesu vyhovuje více než jeden referenční vzorek, tzn. překračuje rozhodovací práh.

False Match rate (FMR)

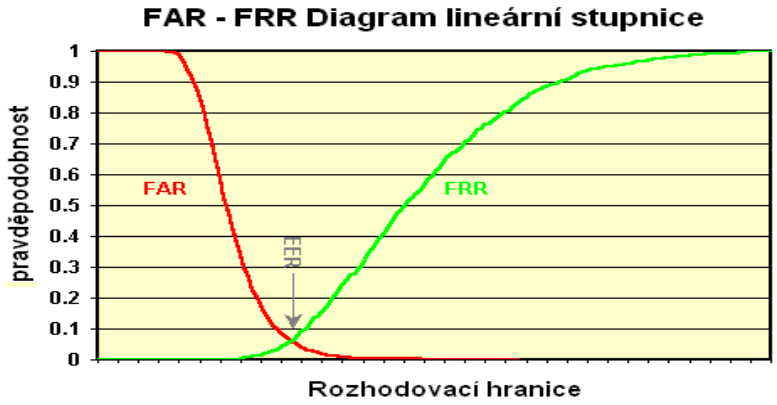
Koeficient FIR udává poměr neoprávněných osob, které jsou nesprávně rozpoznány jako akreditované během srovnávacího procesu. Porovnáme-li ho z koeficientem FAR liší se v tom, že na rozdíl od FAR se do FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Znamená to tedy, že koeficienty FAR a FRR jsou více závislé na způsobu používání biometrického zařízení, tzn. nesprávně rozpoznané biometrické vlastnosti tyto koeficienty zhoršují.

False Non-Match Rate (FNMR)

Koeficient FNMR udává poměr toho, že oprávněné osoby jsou nesprávně nerozpoznány během srovnávacího procesu. V porovnání s FRR se liší v tom, že se nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu.

Důležitým pojmem při měření efektivnosti (výkonnosti) biometrických systémů je tzv. křížový koeficient, udávající, s jakou pravděpodobností při jakém nastavení hranice

rozhodování nastane jev FAR a FFR současně (tzn. FAR=FFR). Křížový koeficient EER (Equal error rate) je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR. Je-li FAR koeficientem bezpečnosti a FRR koeficientem komfortu, je zřejmé, že ve chvíli kdy jsou v rovnováze je v rovnováze i celkové nastavení systému. Z diagramu je také patrné, že posouvání hranice jedním či druhým směrem lze systém buď činit více bezpečným, nebo více uživatelsky příjemnějším. Následující diagram (viz Graf 2) průniku pravděpodobnostních distribučních funkcí FAR – FRR názorně ukazuje jak se v závislosti na nastavené hranici rozhodování projeví celková pravděpodobnost, že mohou nastat obě chyby stejně pravděpodobně.



Graf 2: Distribuční pravděpodobnostní funkce FAR – FRR

Zvyšování bezpečnosti biometrických systémů

Důvodem zvyšování bezpečnosti biometrických systémů, je přes jedinečnost biometrických znaků to, že reálné biometrické aplikace pracují s určitou chybovostí a to ve všech aplikacích nevyhovuje. Dále je zaznamenáno, že pachatelé trestných činů kromě klasické přístupových systémů (karta, PIN…), začínají napadat i biometrické aplikace.

Objevují se pokusy o změny otisků prstů, odlívání otisků prstů do silikonu, plastické operace (změny v obličeji), což je nebezpečné pro bezpečnostní aplikace typu forenzní identifikace, tak i pro přístupové systémy.

Jedním z možných způsobů jak bezpečnost zvýšit je aplikace ezoterické identifikace, protože skryté znaky je mnohem obtížnější změnit, dokonce v některých případech i nemožné změnit.

Druhým z možných způsobů jak zvýšit bezpečnost biometrických aplikací je tzv. Multiple Biometric, tedy vícenásobná biometrie. Jde o kombinaci vice biometrických znaků v jednom systému (nejméně dvou). Nejčastěji používanou kombinací je identifikace podle otisků prstů, geometrie obličeje (2D, 3D), geometrie oční duhovky nebo sítnice a identifikace podle hlasu. Lze očekávat, že v brzké době přibudou i kombinace jiných znaků. Pro občany se stane nejznámější Multiple biometrii při použití e-cestovních pasů s biometrickými údaji. Protože se Evropská unie zavázala, že od roku 2009 bude, kromě dnes používané identifikace obličeje, používán k identifikaci i otisk prstu.

U vícenásobné biometrie je pak výsledná pravděpodobnost přijeti neoprávněné osoby rovna součinu jednotlivých (dílčích) pravděpodobností.

$$FAR_c = FAR_1 \cdot FAR_2 \cdot \cdots \cdot FAR_N$$

FARc - výsledná pravděpodobnost přijeti neoprávněné osoby

FAR (čidlo) - dílčí pravděpodobnosti přijetí neoprávněné osoby (záleží na počtu použitých metod)

U vícenásobné biometrie je pak výsledná pravděpodobnost odmítnutí oprávněného uživatele rovna součtu jednotlivých (dílčích) pravděpodobností.

$$FRR_c = FRR_1 + FRR_2 + \cdots + FRR_N$$

FRRc - výsledná pravděpodobnost odmítnutí oprávněného uživatele

FAR (čidlo) - dílčí pravděpodobností odmítnuti oprávněného uživatele (záleží na počtu použitých metod)

Použití v soukromé praxi

V soukromé sféře naleznou automatické biometrické systémy pro rozpoznávání uplatnění mnoha oblastech:

Ochrana počítačů a dat

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

Zajištění komfortu

- náhrada průkazů
- stravovací systémy, kasina
- uživatelské nastavení (PC, automobily atd.) bezhotovostní platební transakce

Přístupové systémy

- zajištění zabezpečení vstupu do objektu nebo chráněných prostor (obytné objekty, sklady, elektrárny, letiště, výpočetní střediska, trezory)

Docházkové systémy

- státní i soukromé instituce

3 Jednotlivé biometrické technologie

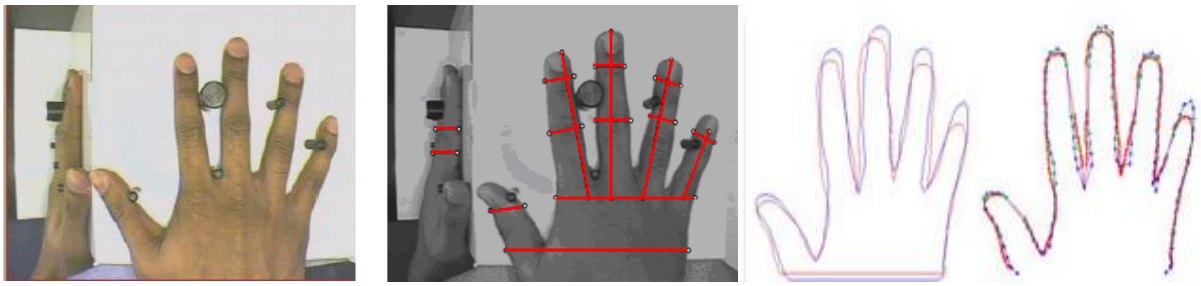
V bezpečnostní praxi je využíváno mnoho metod k individuální identifikaci osob. Výčet a popis nejznámějších a nejčastěji využívaných metod je uveden níže.

3.1.1 Geometrie ruky

Systémy rozpoznávající geometrii ruky jsou nestarším implementovaným biometrický principem. Vyvinul a nechal si jej patentovat David Sidlauskas v roce 1985 a hned v příštím roce byli již systémy rozpoznávající geometrii ruky komerčně dostupné. V roce 1996 byly tyto systémy použity pro identifikaci na Olympijských hrách v Atlantě, kde zajišťovaly bezpečnost vstupu do olympijské vesnice. Jelikož ale není geometrie ruky příliš unikátní

biometrickou vlastností, je její aplikace v bezpečnostní sféře omezena právě stupněm bezpečnosti, kterého chceme dosáhnout.

Zařízení pro rozeznávání geometrie ruky využívají jednoduchého principu měření a 3 dimensionálního snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce s pěti polohovými kolíky (viz Obrázek 4) pomocí CCD kamery.



Obrázek 4: Ruka se zrcadly snímaná CCD kamerou a příklad měření vzdáleností

Na obrazu ruky lze najít přes 31 000 polohových bodů a provést 90 různých měření vzdáleností. Vybrané měřené informace se ukládají do 9 bitového souboru, což činí tyto systémy velice výhodné z hlediska nízkého požadavku na paměť systému. Biometrické systémy založené na verifikaci geometrie ruky jsou používány v různorodých aplikacích docházkových systémů a přístupových systémech, kde jsou poměrně velmi rozšířené.

V USA je systém normalizován ANSI INCITS 396–2005. Celosvětově použitelní norma ISO/IEC CD 19794-10 - Part 10 Geometrie ruky, je stále ve stádiu návrhu a nebyla ještě schválena. FRR: <0.1%; FAR: 0.1%, Čas verifikace: 1 až 2 sekundy; Míra spolehlivosti: střední

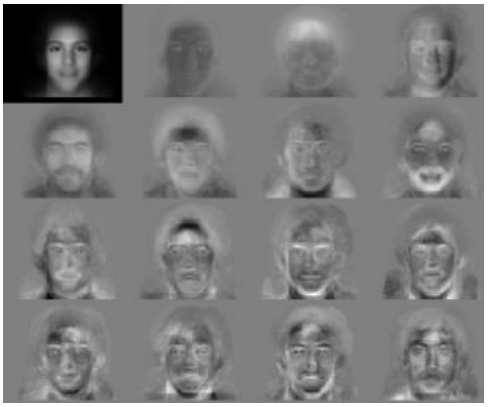
3.1.2 Geometrie tváře

Verifikace obličeje je dnes nejvíce zkoumanou metodou, neboť problematika identifikace osob dle tváří je velmi obsáhlá. Rozpoznávání je založeno na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. K jednoznačné identifikaci slouží většinou tvar obličeje a poloha opticky významných míst na tváři, jako jsou oči, nos, ústa či obočí. Obraz v počítači může být někdy uložen jako matice jasových úrovní, častěji je však diskriminován nějakou funkcí, která snižuje redundanci dat. Neuchovává se tedy přesná poloha očí, nosu a rtů, ale ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem, atd.

V současné době je známo několik technik rozpoznávání tváří. K těm významnějším a nejvíce používaným patří metoda měření geometrických vlastností a metoda porovnávání šablon. Všeobecně se věří, že po zdokonalení systému rozpoznávání obličeje, by mohli odpadnout mnohé, méně efektivní systémy (např. docházkový systém do zaměstnání). Je však pravdou, že během výzkumů se velmi často špatně specifikovaly požadavky, což vedlo k nízké funkčnosti a efektivitě systému. Jsou však známy i případy, kdy byly požadavky na systém tak přemrštěné, že bylo obtížné, respektive naprosto nemožné takový systém realizovat. Proto je nutné si uvědomit jak vysoké nároky je nutné klást na daný identifikační systém. Je obrovský rozdíl v realizaci systémů, který porovnává dva statické obrazy a systému, který ověřuje totožnosti jednotlivce nacházejícího se ve skupině lidí.

Atraktivnost rozpoznávání obličejů je z hlediska praktického užívání pochopitelná, ovšem je nezbytné být realistický ohledně vyhlídek této technologie. Doposud neměli obličejové rozpoznávací systémy v praktických aplikacích velký úspěch. Existují dva odlišné přístupy k rozpoznávání geometrie tváře: geometrický (založený na rysech tváře) a fotometrický (založený na vzhledu obrazu tváře). Tři nejlépe prozkoumané a studované algoritmy rozpoznávání tváře jsou: Analýza hlavních částí (PCA - Principal Components Analysis), Lineární diskriminační analýza (LDA - Linear Discriminant Analysis), Elastický srovnávací diagram (EBGM - Elastic bunch graph matching).

PCA využívá vektorů tváře odvozených s kovarianční matice pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání. Každá tvář lze rozdělit na tzv. eigenfaces (vzory tváří - matice jasových úrovní) a poté jde opět složit (viz. Obrázek5). Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo.

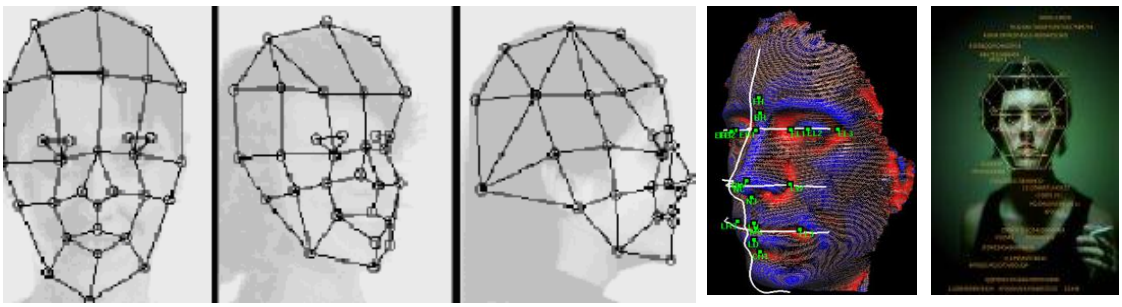


Obrázek 5: Standardní eigenfaces používané pro rozložení obrazu

LDA je metoda, kdy se třídí pořízené obrazy tváří do skupin. Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině, každý blok snímků reprezentuje jednu třídu (viz Obrázek6).

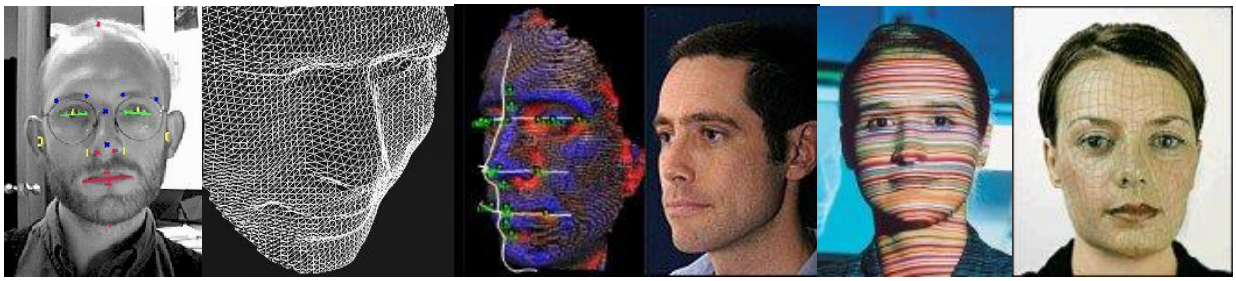
Obrázek 6: Příklad šesti tříd užitím LDA

EBGM byla vyvinuta, jelikož předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení). Na obličeji se definuji uzlové body, které se poté propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje (viz. Obrázek7). Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou. FRR: <1%; FAR: 0,1%, Čas verifikace: 3 sekundy, Míra spolehlivost: střední



Obrázek 7: Síť vytvořená elastickým mapováním a obraz zpracovaný počítačem

Identifikace osob dle geometrie tváře je dnes velice moderním a expandujícím principem. Dochází k jejímu nasazování na letištích, nádražích, rušných ulicích a náměstích a všeobecně na místech, kde by se mohli pohybovat pohřešované a hledané osoby apod.



Obrázek 8: Počítačové zpracování bioemetrických dat obličeje

Nepřesnosti detekce tváře

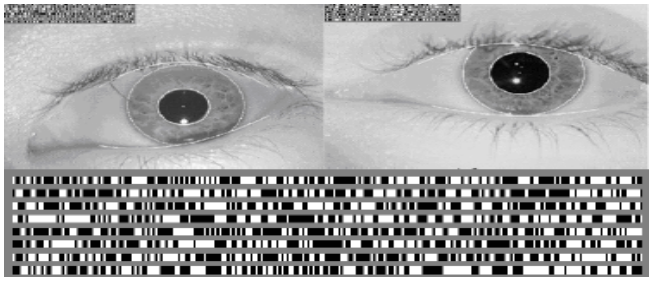
Systémy, které jsou schopny poznávat tváře, omezují rozsah možného správného výběru na třetinu všech možných kandidátů pozitivní identifikace. Jestliže je tvář osoby vyfotografována venku, a to z úhlu 45 stupňů, typický automatizovaný systém selhává v osmdesáti procentech případů,“. Vliv má také proměnlivost osvětlení, způsobovaná odlišností oblečení, vede k tomu, že ve 40 procent případů nedokáže systém danou osobu identifikovat na základě uložené fotografie. Tato technologie může být nápomocná při prohledávání databází fotografií osob, ale fotografie musejí obsahovat záběr celé tváře a musí být k dispozici dostatečné množství manuálních pracovníků, kteří budou schopni spojit fotografii hledaného jedince s fotografií v databázi.

3.1.3 Duhovka oka

Automatické biometrické systémy pro rozpoznávání duhovky lidského oka jsou relativně nové vyvinuté. První patent je datován k roku 1994 a vyvinul ho americký Úřad pro jadernou bezpečnost včele s Dr. Johnem Daugman. Duhovka je sval uvnitř oka, který reguluje velikost čočky (tedy zaostření oka) na základě intenzity světla dopadajícího na oko. Duhovka je barevná část oka, jejíž zabarvení odpovídá množství meletoninového pigmentu uvnitř svaloviny. Ačkoliv je zabarvení i struktura duhovky geneticky závislá, její vzorkování není. Duhovka se vyvíjí během prenatálního růstu plodu a její vzorkování je náhodné, tudíž jedinečné pro každého člověka i dvojčata, dokonce i jeden člověk má každou duhovku jinou, což činí tyto systémy nejpřesnějšími ze všech.

Obrázek 9: Duhovka, její popis a snímač biometrických dat oční duhovky

Snímání duhovky vyžaduje velice kvalitní digitální kameru a infračervené osvětlení oka. Během snímání se duhovka mapuje do fázorových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Tyto informace pak slouží k vytvoření duhovkové mapy (viz Obrázek 10) a šablony pro identifikaci.



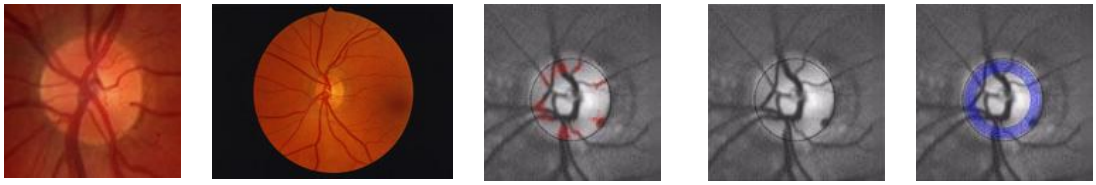
Obrázek 10: Lokalizování duhovky a její piktografické znázornění

Při verifikačním procesu se porovnává žadatelova mapa duhovky s tou referenční pomocí testu statistické nezávislosti. Pokud je pouze méně než jedna třetina dat odlišná, test statistické nezávislosti selhal, což znamená, že vzorky jsou ze stejné duhovky. FRR: 0,00066%; FAR: 0,00078%, Čas verifikace: 2 sekundy, Míra spolehlivosti: vysoká

3.1.4 Sítnice oka

Pro rozpoznávání osoby dle její sítnice oka se používá obraz struktury cév na pozadí lidského oka v okolí slepé skvrny. Sítnice je světlo-citlivý povrch na zadní straně oka a je složena z velkého množství nervových buněk. Pro získání obrazu se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém (dnes se již používá pouze jedna infračervená LED dioda, což snižuje riziko nebezpečného ozáření oka oproti používání systému několika LED diod). Neskenovaný obraz je poté převeden do podoby 40 bitového čísla. Verifikace sítnice je velice přesnou metodou identifikace. Její používání vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné, pokud používají brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast

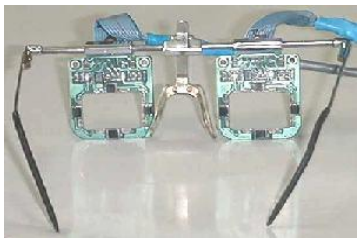
používání a její použití se shrnuje na oblasti vůbec nejvyššího stupně zabezpečení. FRR: 0,4%; FAR: 0,001%, čas verifikace: 1,5 až 4 sekundy, Míra spolehlivosti: vysoká.



Obrázek 11: Lokalizování sítnice a znázornění charakteristických parametrů

3.1.5 Verifikace podle způsobu pohybu očí

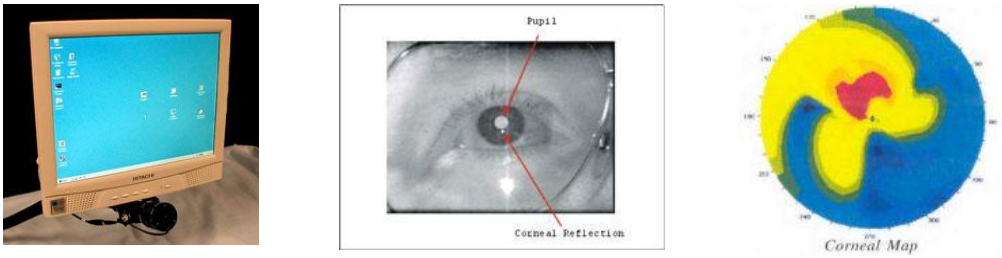
Na Slezské universitě v Gliwicích v Polsku byl vyvinut biometrický snímač pohybu očí při pozorování cílů na obrazovce počítače. Při této metodě jsou nutné brýle, které na principu infračerveného světla snímají pohyby očí a ty srovnávají se záznamy uloženými v databázi. Upravené brýle pro tuto potřebu jsou na obrázku 12. Tento způsob zatím není však využíván komerčně.



Obrázek 12: Brýle ke sledování pohybu očí

3.1.6 Verifikace pomocí povrchové topografie rohovky

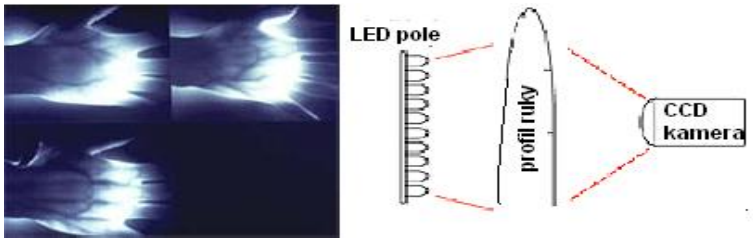
Princip metody je založen na tom, že infračervené světlo malého výkonu (vydávané diodou LED) zaměřené na střed čočky osvětluje oko. Světlo se odráží od rohovky a podle jeho intenzity oko reaguje. Tato reakce je u každého jedince v závislosti na čase a rozšíření čočky oka jiná. Tato reakce je kamerou snímána a srovnána s údaji v databázi. Na obrázku je znázorněno zařízení k uvedené povrchové topografii rohovky.



Obrázek 13: Princip verifikace při povrchové topografii rohovky

3.1.7 Struktura žil na zápěstí

Jedná se o jednu z nejnovějších metod rozpoznávání jedince (první komerčně dostupné systémy jsou datovány až k roku 2000). Tato technologie se vyznačuje obtížností falšování (síť cév je obtížné napodobit, jelikož je uvnitř ruky a není tedy viditelná pro napodobení, navíc některé principy přímo vyžadují, aby byla ruka živá, tedy aby v ní tekla teplá krev). Technologie spočívá ve snímání hřbetu ruky speciální kamerou v infračerveném světle. Tak lze získat černobílý obraz stromové struktury žil, které tvoří zřetelný vzorec. Struktura krevního řečiště se navíc v dospělém věku příliš nemění, je velice výrazná a její jedinečnost i mezi jednovaječnými dvojčaty prokázaly některé vědecké studie. Výhodou je také bezkontaktní princip (uživatel se nemusí dotýkat povrchu snímače, což zvyšuje hygienu a pravděpodobnost správného přijmutí uživatele). Pro uplatnění této technologie existuje mnoho různých použití (např. v Japonsku jsou systémy rozmístěny na univerzitách, nemocnicích a pokladních automatech). Aplikace musí mít zajištěnu ID verifikaci, vysokou fyzickou bezpečnost kontroly přístupů, vysokou bezpečnost datových sítí a kontrolu přístupu do pokladních systémů. Další nespornou výhodou je možnost verifikace i identifikace (lze použít pro systémy 1:1, kdy se používá ID karet nebo jiných tokenů, anebo systémů 1:N, kdy je pořízený vzorek porovnáván s celou databází šablon). Snímání probíhá tak, že zdroj (pole LED diody) prosvítí ruku a na základě různé absorpce (odrazu) záření krevních cév a ostatních tkání se vytvoří obraz (viz Obrázek 14) pomocí snímací CCD kamery (charge-coupled device - zařízení s nábojovou vazbou). Obraz je dále digitalizován a zpracováván za cílem vyextrahování sítě cév. Ukládají se důležité vlastnosti jako: body a úhly větvení cév a tloušťka cév.



Obrázek 14: Obraz světelné prostupnosti ruky a princip snímání

Použitím zobrazení ve spektru blízkému infračervenému světlu (IR záření) se zvýrazní kontrast mezi cévním řečištěm hřbetu ruky a okolní kůží. Toto je znázorněno na obrázku 9. Odkysličený hemoglobin v žilách pohlcuje světlo o vlnové délce přibližně $7{,}6 \times 10^{-4}$ mm, což je hodnota blízká infračervenému světlu. Hloubka absorpce IR záření živou tkání je přibližně 3 mm, tzn. že termální IR záření proniká do hřbetu ruky jen povrchově a v nasnímaném

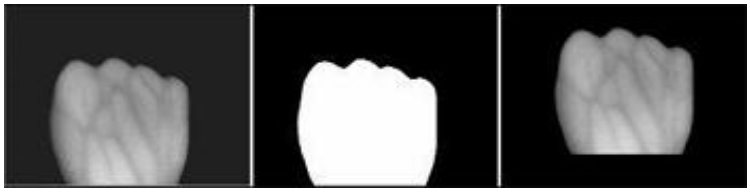
obrazu je pak nejvíce rozeznatelné právě celé cévní řečiště. Díky tomu jsou žíly na IR snímku vytaženy tmavou (černou) barvou, jak je patrné i z obrázku 15.

Obrázek 15: IR zobrazení hřbetu ruky

Jakmile je sejmut potřebný obraz hřbetu ruky, nastupuje další fáze rozpoznání žil ruky, která se může skládat ze 4 kroků. Jde o segmentaci obrazu, tj. rozdělení na části (hand region segmentation), vyhlazení a redukce šumu (difussion smoothing), prahování (local tresholding) a postprocessing.

Segmentace obrazu

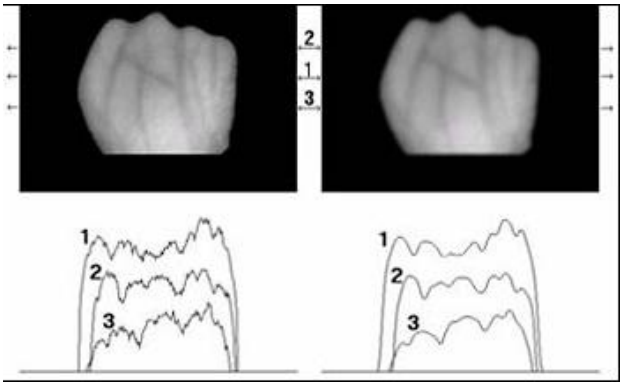
Účelem tohoto primárního kroku je rozdělit nasnímaný obraz na část ruky, tj. požadované části, a pozadí obrazu. Na obrázku 16 je část ruky zobrazena bíle a pozadí černě. Poslední část obrazu napravo je výstup tohoto kroku, tj. obraz s vycentrovanou částí ruky.



Obrázek 16:Segmentace ruky od pozadí obrazu

Vyhlazení a redukce šumu

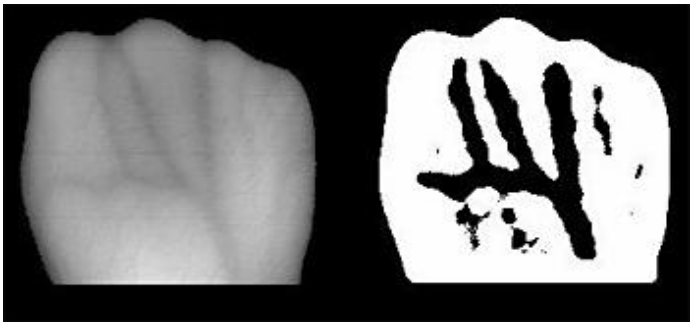
Pro redukci šumu a vyhlazení obrazu se používá např. filtr Gaussovské rozmazání (nezachovává hrany) nebo nelineární rozptýlení (zachovává hrany). Tento krok slouží k vyhlazení obrazu cévního řečiště a k potlačení případného vlivu tvaru hřbetu ruky.



Obrázek 17: Vyhlazení obrazu hřbetu ruky

Lokální prahování

Úkolem tohoto kroku je oddělit vzor žilní struktury od zbytku obrazu. Metody pro toto oddělení lze rozdělit do 4 skupin: segmentace prahováním, segmentace pomocí hran, segmentace pomocí oblastí a segmentace porovnáním. Výpočetně nenáročná a rychlá je první z uvedených metod. Používá se technika lokálního prahování, tj. výpočet průměrné hodnoty z okolních pixelů a použití této průměrné hodnoty jako hodnoty prahu.



Obrázek 18: lokální prahování obrazu hřbetu ruky

Postprocessing

Posledním krokem je postprocessing, kde se již po finálních úpravách na obrázku vyskytuje pouze struktura žil hřbetu ruky ve stavu, který lze již označit jako šablonu. Na obrázku 19 je zobrazena (v pravé části obrázku) výsledná šablona, která se při verifikaci porovnává s uloženou šablonou uživatele.

Obrázek 19: postprocessing hřbetu ruky

Technologie žil dlaně ruky

Princip rozpoznání vzorce krevního řečiště v dlani ruky je velmi podobný technologii žil hřbetu ruky. V tomto případě se ale samozřejmě detekují žíly dlaně ruky. Používá se k tomu **bezdotykový snímač**, ke kterému se ruka přiloží, viz obrázek 20. Snímač je schopen zachytit obraz dlaně bez ohledu na pozici a pohyb dlaně.

Obrázek 20: snímač dlaně

Nejdříve se zachytí **snímek dlaně infračerveným paprskem**, jak je vidět na obrázku 21. Síť tmavších čar (zvýrazněná krev obsahující odkysličený hemoglobin) zde představuje vzorec žil dlaně.

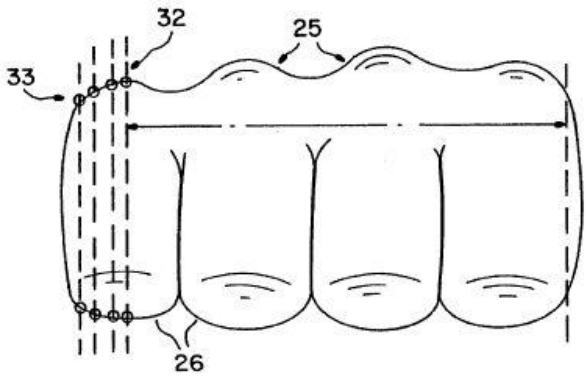
Obrázek 21: IR snímek dlaně

Z tohoto obrazu systém extrahuje vzorec žil dlaně do nového obrazu, viz obrázek 22. Takovýto obraz se následně dle potřeby transformuje a porovná s uloženou šablonou z registrace uživatele.

Obrázek 22: extrahované žíly dlaně

3.1.8 Verifikace podle tvaru článku prstu a pěsti

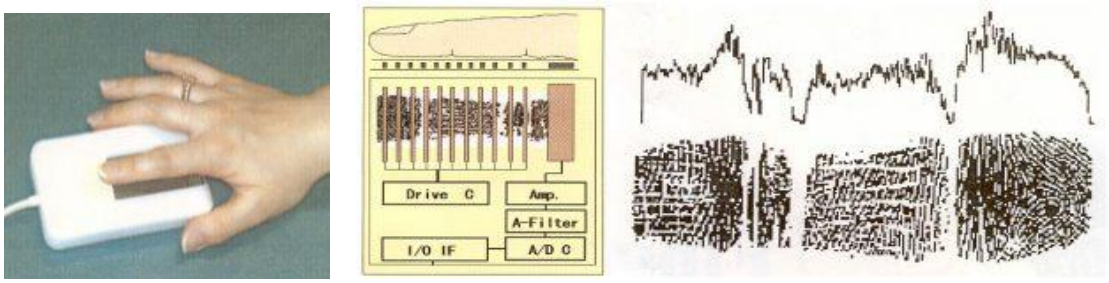
K individuální identifikaci se využívají biometrická měření článků prstů na sevřené dlani ve vnější části. Podle potřeb na přesnost se využívá až 35 parametrů, resp. měření sevřené dlaně na digitální fotografii uložené v paměti počítače s parametry sejmutými například při vstupu do chráněného objektu u snímače. Na obrázku 23 jsou uvedeny příklady možných měření.



Obrázek 23: Biometrické parametry sevřené dlaně k verifikaci totožnosti.

3.1.9 Verifikace podle vrásnění článků prstů

Firma Toshiba již v roce 1998 předvedla identifikační systém založený na měření vrásnění na prstech a rozmístění kloubů prstu. Využívá se elektrostatické kapacitní reaktance měření vrásek za dvěma klouby na prstu ruky u osob. Základní princip je na obrázku 24.



Obrázek 24: Snímač vrásnění článků prstu

3.1.10 Behaviometrika

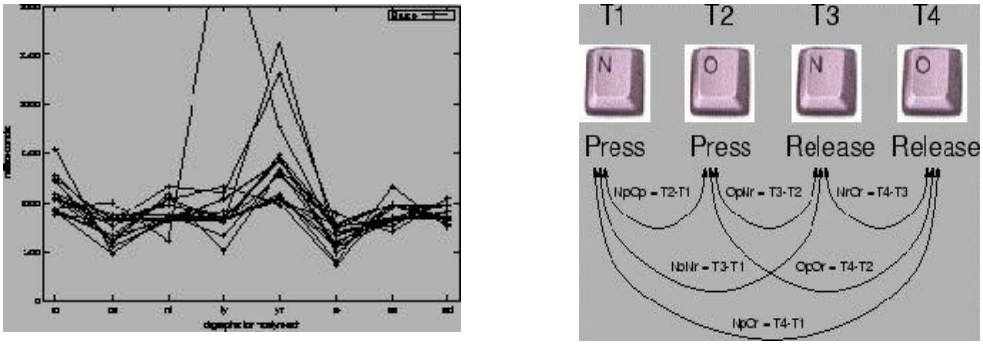
Speciální podkapitolou biometriky je "behaviometrika", při níž dochází ke sledování vlastností (nikoliv fyzických parametrů) člověka. Typickým příkladem může být třeba styl psaní na klávesnici – četnost úderů, jejich rytmika – toto je pro každého člověka jedinečné. Na stejném principu pracuje ověřování pomocí hlasu nebo pomocí monitorování pohybů myší. Rozhodně jsou to zajímavé systémy, protože umožňují průběžnou kontrolu – nestačí, že oprávněný uživatel provedl autorizaci, neboť systém následně pozná, kdy v průběhu práce usedá ke klávesnici jiná osoba. V podstatě zde neexistuje možnost napodobení, protože nuance jsou tak drobné, že se je člověk nemůže naučit.

Jinak behaviometrika obsahuje třeba studium stylu chůze, gest, typických znaků. Můžete tak identifikovat osobu i na velkou vzdálenost (do budoucna se uvažuje třeba i o pomoci družic z oběžné dráhy). Problémem u některých z těchto faktorů je skutečnost, že se v čase mění.

3.1.11 Psaní na klávesnici

Tato technologie je obdobou dynamického podpisu, přičemž sleduje dynamiku úhozů na klávesnici, která se u různých lidí liší. Sleduje se doba, po kterou jsou klávesy drženy, stejně jako prodleva mezi jednotlivými stisky kláves. Vytvoření „otisku“ psaní na klávesnici trvá trochu déle než sejmutí otisku prstu do databáze, ale přesto jde o neinvazivní a dobře přijímanou metodu identifikace. Možnosti nasazení této metody jsou zcela zjevné. Výborně se hodí pro ochranu nežádoucích přístupů k osobním počítačům i ke vzdáleným informačním

systémům pracujících v režimu on-line. Nasazení této technologie má ovšem i několik proti. Tím hlavím je poměrně velká pravděpodobnost „zaměnitelnosti“ charakteristik psaní na klávesnici u více uživatelů. Dynamika psaní se navíc s časem může měnit. Jde o zajímavou metodu sekundární autentizace přístupů, protože rozpoznávání může běžet na pozadí a při zjištění odchylky od uloženého vzorku může například vyvolat žádost o další identifikaci.



Obrázek 25: Dynamika psaní na klávesnici a diagram, který jí zachycuje

3.1.12 Dynamika podpisu

Tato metoda je datována k roku 1977 a využívá jedinečnosti kombinace anatomických a behaviorálních vlastností člověka, které se projeví, když se podepisuje. Zařízení na dynamický podpis se často mylně zaměňují s pojmy jako je elektronický podpis (šifrovaný klíč) nebo se zařízeními na snímání podpisu jako obrazu. Z ručního podpisu lze tak elektronicky zjistit tah, tvar a tlak při psaní, což lze použít pro verifikaci osoby. Jednotlivé druhy zařízení se liší dle výrobce způsobem užití a jeho významem, ale mají shodnou vlastnost použití technologií citlivých na dotek, tedy PDA záznamníků nebo digitalizačních tabulí. Většina těchto zařízení využívá dynamických vlastností podpisu, ačkoliv existují i kombinace se statickými a geometrickými vlastnostmi podpisu. Základními dynamickými vlastnostmi jsou rychlost, akcelerace, časování, tlak a směr tahu, které jsou zaznamenávány v trojrozměrném souřadnicovém systému (viz Obrázek 26). Osy ‚x‘ a ‚y‘ slouží k určení rychlosti a směru tahu, souřadnice, z’ určuje tlak na podložku. Na rozdíl od statického obrazu podpisu, který může být naučen a napodobován, je nemožné se dynamiku podpisu pouze z obrázku naučit. Výhodou je i snadné integrování zařízení do již existujících systémů (stačí PDA a vhodný SW). Naopak nevýhodou je, že tyto systémy jsou schopné zvládat pouze verifikační principy.

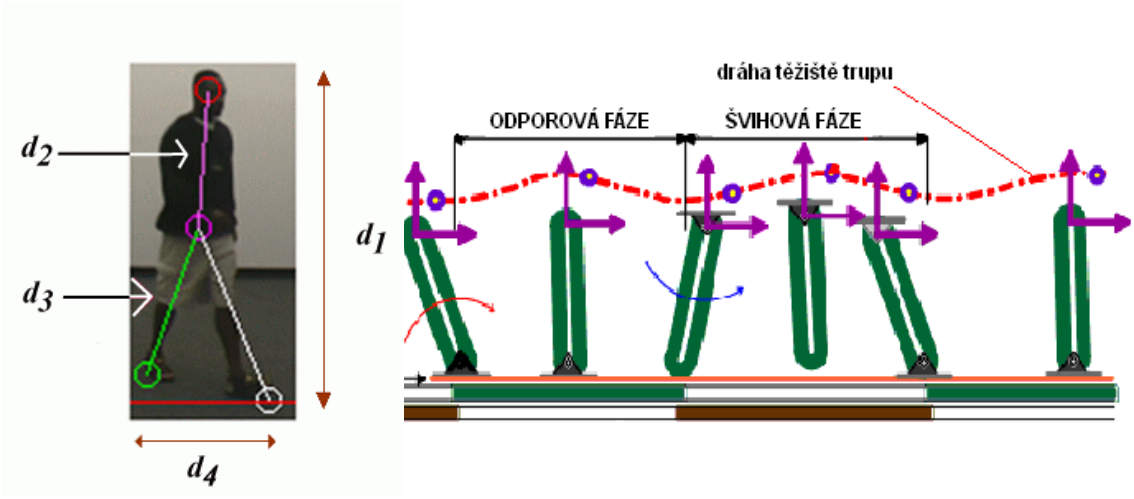
Obrázek 26: Princip dynamického podpisu; uživatel, měření a SW srovnání

3.1.13 Dynamika chůze

Stejně jako otisk prstu nebo duhovka oka je i pohyb člověka jedinečný a svým způsobem neměnný v relativně širokém časovém období neměnný. České kriminalistice a jejímu výzkumu patří přední místo ve světě ve vývoji identifikace člověka podle stylu chůze, tedy „pohybu po dvou nohách“ ,nebo bipedální lokomoce. Velký podíl na rozvoji této metody má i rozmach záznamové a snímací techniky.

Stejně jako při identifikaci podle ručního písma je rozlišovacím znakem jedinců různý dynamický stereotyp, u písma se jedná o stereotyp ruky a chůze celého pohybu těla. Tato metoda má obrovský význam při identifikování pachatelů loupežných přepadení, jimž je zcela zbytečné jakákoliv maskování nebo převleky. Další význam tato metoda nabývá při současném prudkém rozvoji nasazování průmyslových kamer na nejrůznější rušná místa (letiště, náměstí, nádraží, multifunkční komplexy atd.). Její uplatnění je tedy pouze ve forenzní sféře, kde však dosud stále neexistuje databáze srovnávacích materiálů.

Celá metoda pracuje na základě porovnávání křivek drah, které opisují určité body na lidském těle, tedy hlavně jeho těžiště. Jelikož je každý člověk jedinečný svým pohybovým svalově kosterním systémem a svým dynamickým stereotypem, jsou i křivky uvažovaných bodů unikátní a vhodné pro srovnávání a 1:1 identifikaci. Způsob vytváření těchto křivek je na obrázku 27.



Obrázek 27: Postup vytváření dráhy těžiště trupu ¨při bipedální lokomoci

3.1.14 Otisk prstu

Identifikace na základě otisku prstu je jednou z nejznámějších a nejvíce publikovaných biometrických metod. Otisk prstu se používá pro identifikaci už celé století, a to hlavně pro svou vlastnost jedinečnosti a stálosti v čase. Navíc se musela tato identifikace s rozvojem počítačové techniky stát plně automatizovanou, aby si zajistila místo v dnešní době. Identifikace otisku prstu je s oblibou používaná především pro relativní jednoduchost získání srovnávacího vzorku, pro vysoké procento použitelné populace (nelze identifikovat pouze jedince, kteří přišli o obě ruce i nohy, což je málo pravděpodobné), dále pro četnost zdrojů ze kterých lze získat vzorek (10 prstů) a také protože jde již o zavedenou metodu s velkou databází u policie a s uplatněním v právní sféře a imigrační problematice.

Používání otisku prstu (přesněji obrazců papilárních linií na vnější straně prstů rukou, nohou a dlaní) jako metody pro identifikaci se začala používat už na konci 19. století, kdy Sir Francis Galton nalezl a definoval některé charakteristické body na prstu, které mohou sloužit k identifikaci člověka. Tyto „Galtonovi body“ položily základ vědnímu zkoumání otisku prstu, který byl rozvíjen po celé století.

Metody zachycení otisku prstů

Otisk získaný pomocí inkoustu a papíru

Klasická metoda (rolled finger). Tato metoda se používá pouze ve forenzní sféře, policií při vyšetřování. Používá se inkoustu a papíru. Prst se po papíře roluje, aby se získal

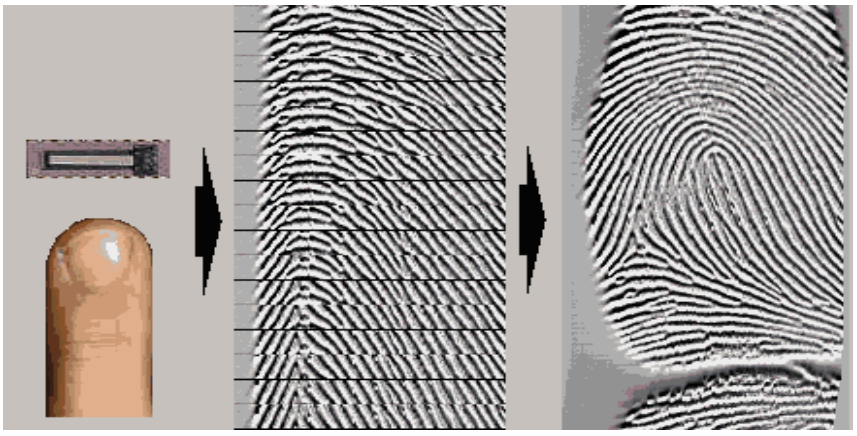
otisk celého prstu (prakticky od nehtu po nehet) s co možná nejvíce použitelnými markantami a aby se tím zvýšila i rychlost rozpoznání otisku.

Statické snímání

Jedná se o nejběžnější používanou metodu snímání otisku prstu. Uživatel přitiskne svůj prst na senzor bez jakéhokoliv pohybování s ním. (existují desítky různých fyzikálních principů snímání, které jsou vysvětleny dále). Výhodou této metody je nesporně jednoduché ovládání (stačí pouze přiložit prst). Na druhou stranu je zde řada nevýhod: přehnanou silou tlačení prstu může uživatel rozlomit snímací čočku (obzvlášť je-li doba snímání delší, uživatel znervózní a přitlačí více), přiložení prstu a jeho současné pootočení vede k deformaci pokožky a celého otisku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky.

Snímání šablonováním

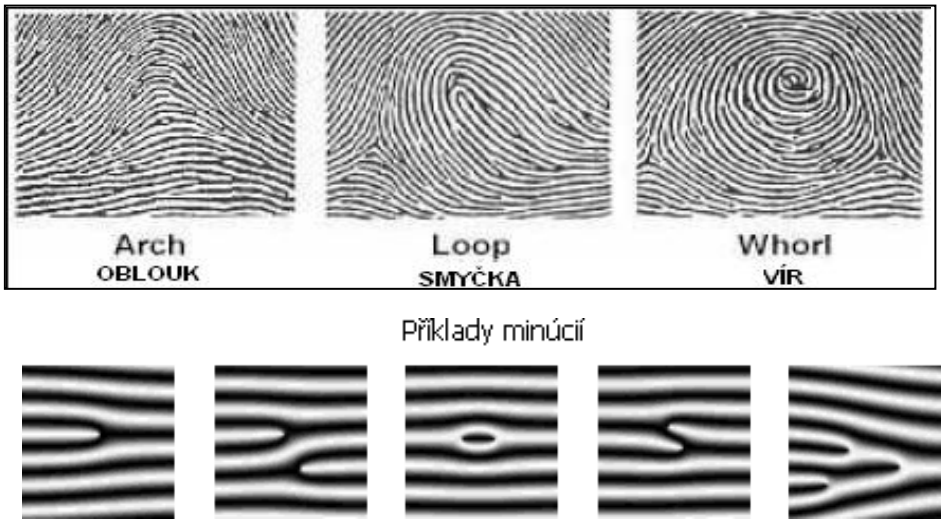
Uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů (viz Obrázek 28). Používá-li se křemíkový snímač, pohybuje se i cena v oblasti křemíkových součástek. Redukovat cenu lze právě využitím šablonovaného snímání, tím že snímač bude mít tvar úzkého pruhu. Celková cena pro pořízení otisku prstu je poté výrazně nižší. Výhody šablonovaného snímání jsou: snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor; na snímači nezůstávají skryté (latentní) staré otisky; uživatel nemá pocit ‚zanechaného' otisku prstu a snímání je rychlé. Nevýhodou je, že obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup.



Obrázek 28: Postup zachycení obrazu otisku prstu šablonováním

Používané algoritmy u snímačů otisku prstu – srovnávací metody.

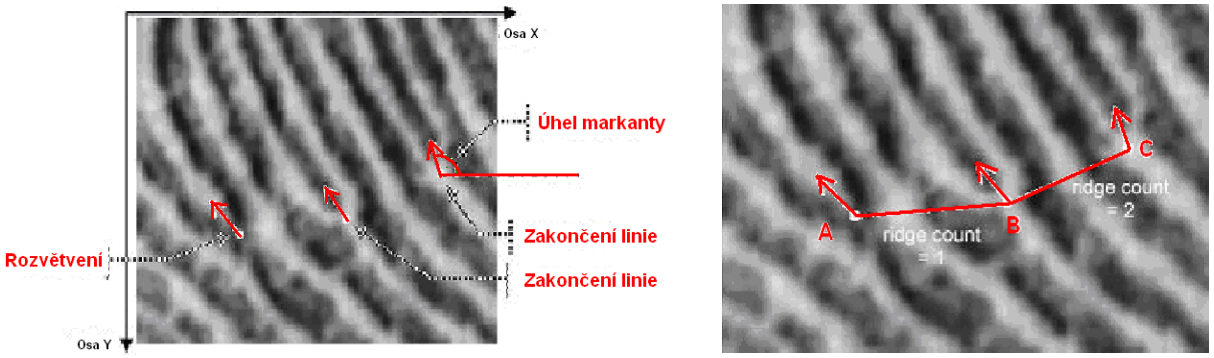
Většina algoritmů využívá existence markant, specifických bodů jako je zakončení linie, rozvětvení linie, bod (ostrov), jezero, výběžek (osten) nebo zkřížení, což jsou detaily třech hlavních vzorů (seskupení papilárních linií). Jedná se o smyčky, víry a oblouky (loop, whorl, arch) viz obrázek 29.



Obrázek 29: Ukázka hlavních seskupení papilárních linií

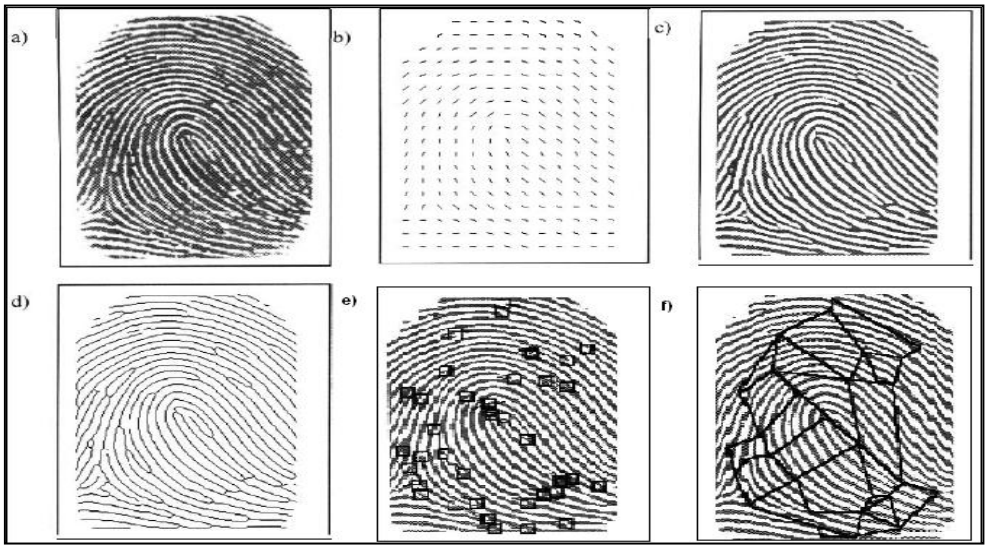
Některé algoritmy ukládají pro pozdější srovnávání pouze pozice (s=[x;y]) a směr (úhel Θ) markant, což vede k redukci dat nutných pro zápis (viz Obrázek 30a).

Jiné algoritmy namísto vzdálenosti znaku vypočítané z pozice, sčítají počet vyvýšených rýh mezi dvěmi konkrétními body, zpravidla markantami (viz Obrázek 30b).



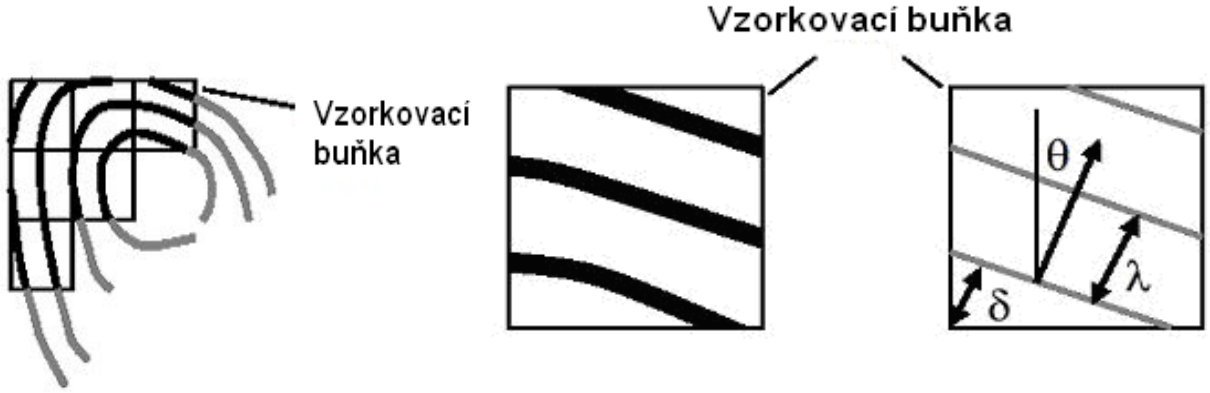
Obrázek 30: a) Příklady vzorkování markant b) Příklad sčítajícího algoritmu

Často používaný algoritmus vytváření tzv.markantografu pracuje na vytvoření obrazce spojnicemi mezi nalezenými markantami. Postup je následovný: obraz originálu otisku prstu je podroben filtru orientace markant, následné počítačové binarizaci dat, zeslabení linií, nalezení markant a vytvoření markantografu (viz Obrázek 31).



Obrázek 31: a) originální otisk b) filtr orientace markant c) binarizace d) zeslabení e) nalezení markant f) markantograf

Pro jiný srovnávací algoritmus je základní vzhled rýh. Samotný otisk prstu je rozdělen do malých sektorů, z nichž se vyextrahují a uloží: směr rýh, jejich vzájemný odstup a fáze (viz. **Chyba! Nenalezen zdroj odkazů.**32). Velmi často používají algoritmy, které jsou kombinací několika metod.



Obrázek 32: Vzorkovací buňky a zjišťování sklonu linie Θ, odstupů linií λ a odstupů od okraje buňky δ

U komerčního použití je práh citlivosti (hranice počtu shodných markant) volitelná dle bezpečnostního požadavku. Ve forenzní sféře je nutno splnit podmínku daného státu (v ČR se jedná o minimální počet 10 shodných markant, v USA 8, v Rusku 7, v EU 10–17). FRR: <1,0%; FAR: 0,0001% - 0,00001% dle použité technologie snímače, Čas verifikace: 0,2 - 1 sekunda, Míra spolehlivosti: vysoká.

Určení pravděpodobnosti, že dva různé otisky prstů budou shodné:

Podle vlastních výzkumů společnosti IBM/Pankanti je pravděpodobnost odhadována na $6 \cdot 10^{-8}$. Existuje ovšem velké množství způsobů výpočtů pro odhad pravděpodobnosti. V následující tabulce M, R definují snímanou oblast a N počet markant.

Author	P(Fingerprint Configuration)	N=36,R=24,M=72	N=12,R=8,M=72
Galton (1892)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{2}\right)^R$	1.45×10^{-11}	9.54×10^{-7}
Pearson (1930)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{36}\right)^R$	1.09×10^{-41}	8.65×10^{-17}
Henry (1900)	$\left(\frac{1}{4}\right)^{N+2}$	1.32×10^{-23}	3.72×10^{-9}
Balthazard (1911)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22}	5.96×10^{-8}
Bose (1917)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22}	5.96×10^{-8}
Wentworth & Wilder (1918)	$\left(\frac{1}{50}\right)^N$	6.87×10^{-62}	4.10×10^{-21}
Cummins & Midlo (1943)	$\frac{1}{31} \times \left(\frac{1}{50}\right)^N$	2.22×10^{-63}	1.32×10^{-22}
Gupta (1968)	$\frac{1}{10} \times \frac{1}{10} \times \left(\frac{1}{10}\right)^N$	1.00×10^{-38}	1.00×10^{-14}
Roxburgh (1933)	$\frac{1}{1000} \times \left(\frac{1.5}{10 \times 2.412}\right)^N$	3.75×10^{-47}	3.35×10^{-18}
Trauring (1963)	$(0.1944)^N$	2.47×10^{-26}	2.91×10^{-9}
Osterburg et al. (1980)	$(0.766)^{M-N}(0.234)^N$	1.33×10^{-27}	3.05×10^{-15}
Stoney (1985)	$\frac{N}{5} \times 0.6 \times (0.5 \times 10^{-3})^{N-1}$	1.2×10^{-80}	3.5×10^{-26}

Snímače otisků prstů

Existují desítky metod snímání otisku prstu využívajíc nejrůznější fyzikální principy. Vědci se neustále snaží o nalézání nových a nových metod, a avšak ty nejjednodušší a nejsnadnější jsou již objeveny a používány. Jedná se především o:

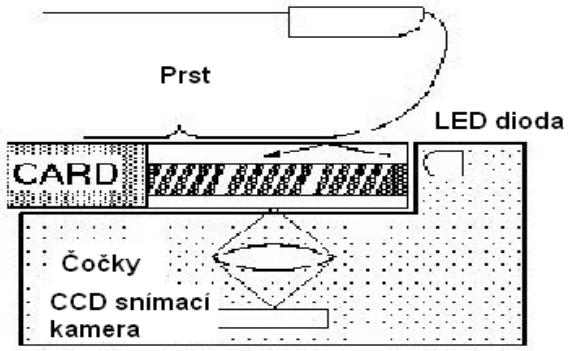
1. Optické senzory
   - Na základě odrazu (reflexní)
   - Reflexní se skládáním obrazu
   - Bezdotykový odraz
   - Transmisní
2. Elektro-optické snímače
3. Kapacitní snímače
   - Křemíkové čipy a kapacitní snímač
   - Kapacitní snímač a TFT

- TFT optické

4. Tlakové snímače
   - Vodivá membrána na silikonu
   - Vodivá membrána na TFT
   - Dotekové mikro-elektro-mechanické spínače
5. Rádiové snímače
6. Teplotní senzory
7. Ultrazvukové snímače
8. Fotonové krystaly
9. Snímače povrchové impedance

Optické senzory na základě odrazu (reflexní)

Optické senzory patří mezi nejstarší technologii snímání otisku prstu. Hlavní princip spočívá v přidržení prstu nad skleněnou podsvětlenou vrstvou, světlo se odráží od prstu a prochází do CCD snímače, který zachycuje vizuální obraz otisku (viz. Obrázek 33). Nevýhoda tohoto typu je, že je poměrně náchylný k chybám a tím k opakovanému snímání (špinavý prst nebo skenovací ploška vede ke špatnému obrazu, z čehož vyplývají vyšší nároky na údržbu).



Obrázek 33: Princip snímání reflexními optickými senzory

Optické senzory na základě odrazu (reflexní) se skládáním obrazu

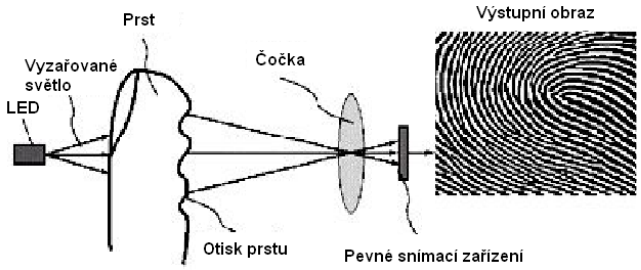
Princip je stejný jako u předchozího snímače, ale výsledný obraz není snímán staticky ale šablonováním. Používají se reflexní rolovací senzory, kdy je jedno-dimenzionální snímací zařízení spolu se zdrojem světla a optickými čočkami umístěno v průhledné rolovací tubě, po které prst klouže.

Optické bezkontaktní snímače

TST (Touchless Technology – bezkontaktní technologie) nepotřebuje optický hranol pro přímé snímání obrazu prstu. Světelné paprsky vysílané z LED diod se odrážejí pod různými úhly od papilárních linií prstu do optické čočky. Signál zpracovává CMOS čip.

Transmisní optické snímače

Princip (viz Obrázek 34) je založen na snímání světelných paprsků procházejících prstem ruky, který je z vrchní části prosvěcován všesměrovým zdrojem světla (většinou klasická infračervená LED dioda). Obraz otisku prstu je poté zpracován stejně jako u předchozích principů systémem čoček a snímacím zařízením. Dle druhu výrobce se jedná buď o standardní CCD - Charged Coupled Device kameru (společnost Mitsubishi), CMOS - Complementary Metal Oxid Semiconductor kameru (společnosti NEC, Delsy) anebo i s využitím polymerického organického fotodetektoru vyvinutým společností NanoIdent.



Obrázek 34: Princip transmisních snímačů otisku prstu

TFT optické snímače

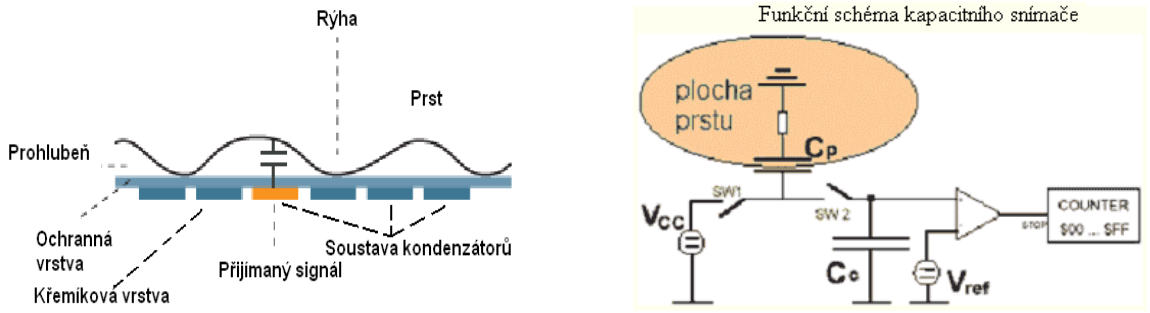
U tohoto typu snímačů dochází k nahrazení klasického snímacího zařízení, tedy určitého typu kamery (CMOS nebo CCD), TFT displejem (TFT - Thin Film Transistor).

Elektro-optické snímače

Princip snímání je založen na faktu, že některé polymerní materiály jsou schopné emitovat světelné záření, pokud se nabudí vhodným napětím. Pokud takovýto materiál přímo propojíme se snímacím zařízením (CMOS kamerou) lze získat obraz otisku prstu tím, že polymerní materiál emituje světlo jen v místech, kde se ho přiložený prst dotýká, tzn. ve styčných bodech papilárních linií. Zařízení tohoto typu vyrábí například společnost Ethentica a korejská společnost TesTech.

Kapacitní snímače otisku prstu

Jedná se o nejrozšířenější princip (viz Obrázek 35) snímání otisků, který je založen na měření kapacity mezi kůží prstu a aktivními pixely. Velikost měřeného elektrického pole se mění mezi rýhami a prohlubněmi struktury papilárních linií jako příčina změny dielektrika mezi jednou deskou kondenzátoru (pixelem) a druhou deskou kondenzátoru (prstem). Dielektrikem je tedy buď vzduchová vrstva (prohlubeň-pixel) nebo pokožka (rýha-pixel). Citlivá snímací plocha je tvořena deseti tisíci kondenzátory strukturovaných do sítě. Senzory využívající kapacitní princip jdou zdaleka nejpřesnějšími typy, jejich výhodou může být i velmi malý rozměr senzoru (zpravidla kolem 4 cm^2). Snímacím zařízením může být u této metody opět buď CMOS kamera (Fujitsu, Hitachi, Symwave), TFT displej (Mitsubishi, Alps Electric) nebo progresivní metoda silikonových čipů (NTT Laboratories, Shigematsu).



Obrázek 35: Kapacitní princip snímání otisku prstu

Rádiové snímače otisku prstu - Aktivní kapacitní snímače

Princip je založen na měření síly rádiového signálu, který je vysílán do prstu vysílačem nízkého RF (Radio frequency) signálu a snímán maticí miniaturních antén, které tvoří styčnou plochu z prstem. Síla signálu se mění v závislosti odporu či vodivosti spojení, tedy na vzdálenosti mezi kůží a anténní soustavou tvořenou pixely, znamená to tedy, že rádiový signál bude jiný v místě, kde se prst přímo dotýká senzoru (rýhy papilárních linií) a v místě kde se ho nedotýká (prohlubně papilárních linií).

Tlakové snímače otisku prstu

Piezoelektrické materiály, které jsou schopny snímat změnu tlaku existují již dlouho, ale problémem byla jejich citlivosti pro detaily papilárních linií. Jedním z řešením je umístit vodivostní membránu (tvořenou maticí piezoelektrických tlakových senzorů) na CMOS

kameru se silikonovým čipem (společnost Opsis). Jiná metoda umístí membránu na TFT podložku (společnost Sanyo, Fidellica, Alps Electric). Jedna z nejmodernějších metod využívá maticového systému mikro mechanických spínačů o velikosti pouhých 50μm, které tvoří síť spínací v místech, kde se prst dotýká svými prohlubněmi papilárních linií.

Teplotní snímače otisku prstu

Tepelné snímání pracuje na principu měření nepatrných rozdílů teploty mezi pokožkou prstu a vzduchu, který vyplňuje prostor mezi jejími papilárními liniemi. Neměří se absolutní velikost teploty, ale právě rozdíl mezi tepelnou energií pokožky předané senzoru v momentě, kdy se dotkne jeho snímací části. Ta je vyrobena z křemíkového čipu pokrytého pyro-elektrickým materiálem, neboli materiálem, který je citlivý na změny teploty. Na křemíku je nanesen v podobě přiléhajících pixelů. Teplotní diference se díky pyro-elektrickému materiálu převede na elektrický náboj, který je poté, díky samotným vlastnostem této látky, zesílen a předán na spodní křemíkový čip (který je také uspořádán do pixelů). Ten pak převede hodnoty elektrických signálů na samotný obraz v několika stupních šedi.

Ultrazvukové senzory

Ultrazvukové senzory narozdíl od optických, které měří odražené světlo, měří odraženou zvukovou vlnu. Technologie funguje na podobných principech jako sonar. Jejich výhodou je, že ultrazvuk snadno pronikne i nečistotami, které by znehodnotili obraz zachycený pomocí optického snímače.

Požadavky na senzory

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 miniaturizace zásadní.

Dostatečně velká snímací plocha – Dostatečná snímací plocha je nutná pro záznam dostatečného počtu identifikačních znaků (markant), nebo plochy obrazu. Existuje malá skupina lidí, která má extrémně málo markant nebo má část markant vyhlazených prací.

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.

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 otisku vzhledem k etalonu a jeho natočení musí být při pokusu o autentizaci minimální.

Dostatečná ochrana vůči napodobeninám – Snímač sám o sobě nezabezpečuje dostatečnou ochranu vůči napodobeninám. Jedná se o slabé místo celého systému. Některé testy s napodobeninami vykazují dokonce lepší poměr FAR a FRR než původní lidské biometrie. Řešením je dodatečná ochrana pomocí kamer nebo fyzické přítomnosti ostrahy.

Uživatelská přívětivost – Uživatelská přívětivost je základním požadavkem ve směru k uživateli systému a ergonomii snímače.

Odolnost vůči mechanickému poškození – Většina snímačů je konstruována pro připojení k počítači, notebooku, atd., a neprošla zkouškami na odolnost vůči mechanickému poškození ani zkouškami ve ztížených klimatických podmínkách, což je chyba.

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.

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.

Cena snímače je velmi variabilní v závislosti na řadě faktorů. Přesto je z výše uváděného rozboru zřejmé, že zřejmě nejdražší budou kvalitní optoelektronické snímače. Při realizaci konkrétního návrhu zabezpečení pomocí ACS je nutno zvážit všechny aspekty a vytvořit vhodný kompromis s požadavky zadavatele projektu. Šíře v současnosti nabízeného sortimentu dává však projektantům bezpečnostních opatření dostatečně velký prostor pro naplnění těchto cílů.

3.1.15 Akustická charakteristika hlasu

Porovnávání vzorků hlasu používají kriminalisté již desítky let. V civilní praxi se ale tato technologie začíná prosazovat až nyní. Pro ověření identity subjektu slouží předem uložené vzorky hlasu – namluvené klíčové věty. Výhoda ověření identity pomocí hlasu spočívá nejen ve specifiku lidského hlasu, ale také ve flexibilitě klíčových vět. Sebelepší imitátor bez znalosti klíčové věty nemůže ošálit identifikační systém.

Identifikace pomocí hlasu, tedy rozpoznání hlasu mezi jinými v reálném prostředí je mnohem náročnější a v současnosti neexistuje dostatečně přesný systém. Hlavní výhodou verifikace identity pomocí digitálních otisků hlasu je nízká cena, poměrně vysoká spolehlivost a naprostá neinvazivnost technologie i široké možnosti nasazení od telefonního bankovnictví po vzdálený přístup k informačním systémům.

3.1.16 Verifikace a identifikace podle pachu

Pachových stop používá policie jako nepřímého důkazu již desítky let, v civilní branži se ale 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.

Lidský pach se skládá přibližně ze třiceti chemických sloučenin, jejichž intenzita či absence vytváří jedinečný profil u každého člověka. Kriminalistická praxe místo senzorů používá s vysokou spolehlivostí psy. V oblasti civilního nasazení je ale potřeba porovnávat a správně identifikovat více než jednu pachovou konzervu zároveň a pro to zatím neexistují dostatečně přesné senzory. Dalším problémem jsou změny ve skladbě pachových stop při emocionálních či hormonálních výkyvech. V současnosti provádí výzkum možností analýzy pachu několik společností a univerzitních výzkumných programů, reálné nasazení v praxi je však zatím otázkou budoucnosti.

3.1.17 Verifikace podle DNA

DNA je jako identifikační prvek používáno opět v policejní praxi, a to od druhé poloviny osmdesátých 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, která zahrnuje přibližně pět kroků. Během nichž je ze vzorku tkáně vypreparována nejprve celá spirála DNA, která je následně štěpena enzymem EcoR1 a posléze jsou fragmenty DNA prosévány, až se získá řetězec využitelné velikosti.

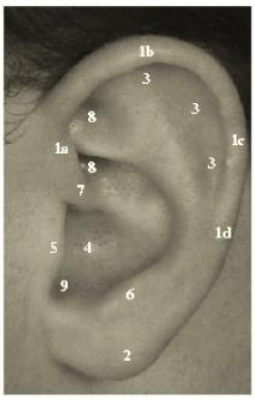
Získané fragmenty jsou přeneseny na nylonovou membránu a po přidání radioaktivních nebo obarvených genových sond je získán rentgenový snímek – otisk DNA. Tento otisk připomíná čárový kód, a proto je snadné jej převést do elektronické podoby. Takto získaná informace slouží k řešení celé řady otázek od přiznání otcovství až po identifikaci těl. Mnohé armády či záchranářské sbory proto budují databáze DNA svých zaměstnanců. Pro kontrolu přístupu v reálném čase však zatím tato technologie není použitelná.

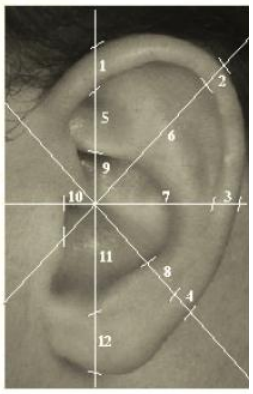
3.1.18 Biometrie ušního boltce

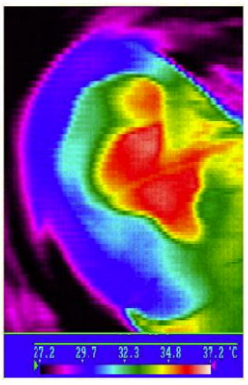
Identifikace člověka využívající biometrii ušního boltce je založená na individuálním tvaru a morfometrické stavbě ušního botce každého jedince. Obecně existují 3 metody biometrické identifikace podle ušního boltce:

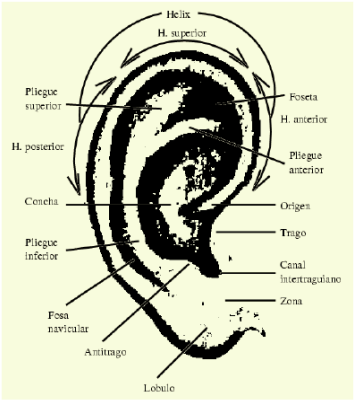
1. Podle morfometrických vztahů – geometrii ušního boltce, v 2D nebo 3D formě
2. Podle otisku struktur ušního boltce (podobně jako u otisků prstů) – tato metoda ale pro praxi není příliš "komfortní", její využití je ve forenzní oblasti
3. Podle termogramu ušního boltce – termografického snímku, mapujícího rozložení tělesné teploty na ušním boltci

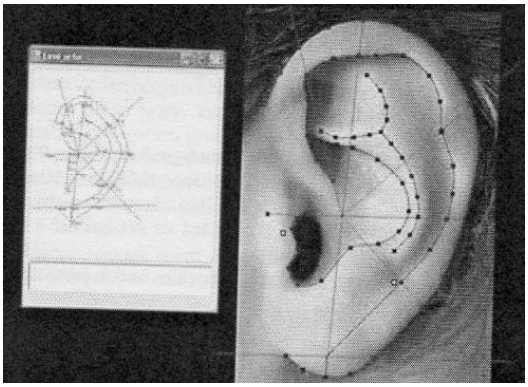
Použitelnou metodou pro komerční využití, tak aby byla komfortní pro uživatele, je identifikace podle morfometrických vztahů – geometrie ušního boltce. V tomto případě je uživateli ušní boltec nasnímán speciálním optickým snímacím zařízením, ze vzdálenosti cca 0,5 - 1 m. Data zanesená na snímku (morfometrické vztahy – rozměry, tvary, položení významných bodů, křivky apod.) jsou pak vyhodnocena a v závislosti na použitém typu algoritmu porovnána s příslušnou databází.

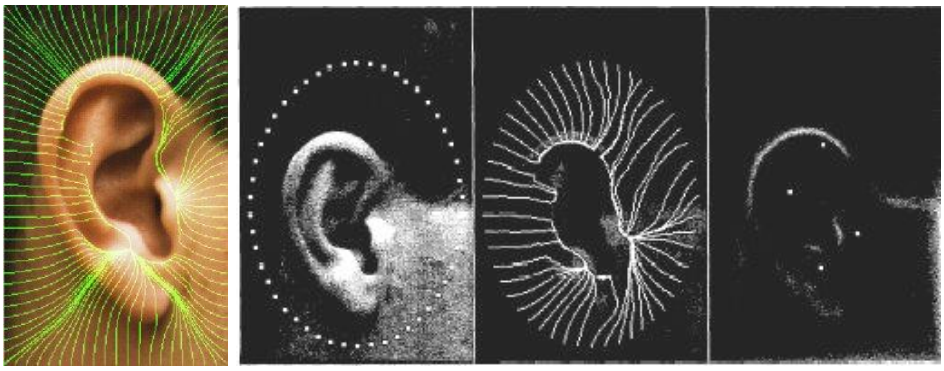








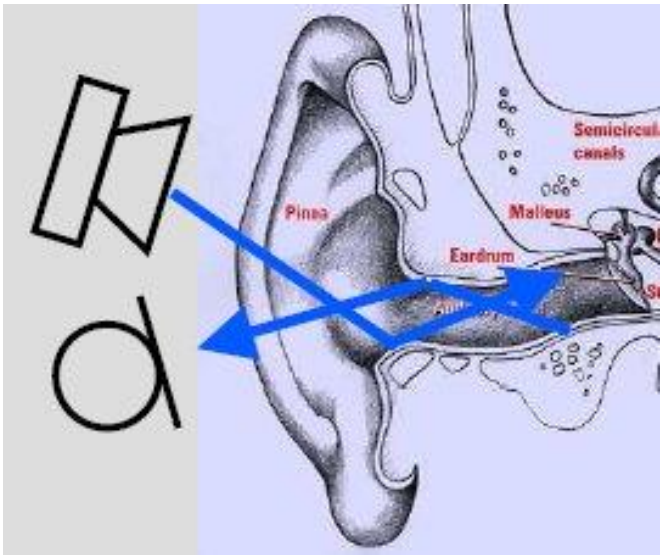




Obrázek 36: Biometrické měření parametrů ušního boltce

3.1.19 Verifikace odrazem zvuku v ušním kanálku

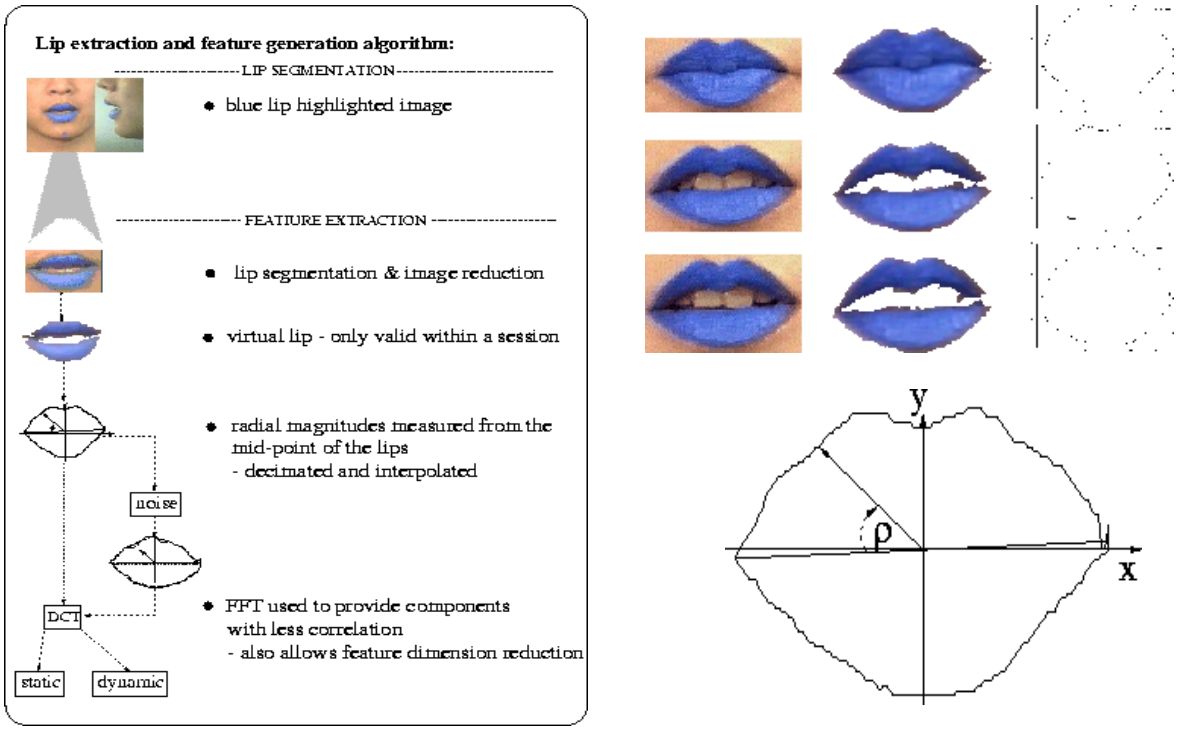
Jde o novou metodu, dosud málo využívanou v praxi. Při verifikaci se osoba přiloží ucho k reproduktoru. Zvuk se odráží od stěny zvukovodu a jeho část se vrací odrazem ušní stěny zpět. Intenzita pohlcení zvuku v ušním kanálku je u jednotlivců individuální a podle této intenzity lze individuálně identifikovat osobu a ověřit její totožnost. Schéma je na obrázku 37.



Obrázek 37: Odraz zvuku ve zvukovodu, jako prostředek individuální identifikace

3.1.20 Verifikace osob podle tvaru a pohybu rtů

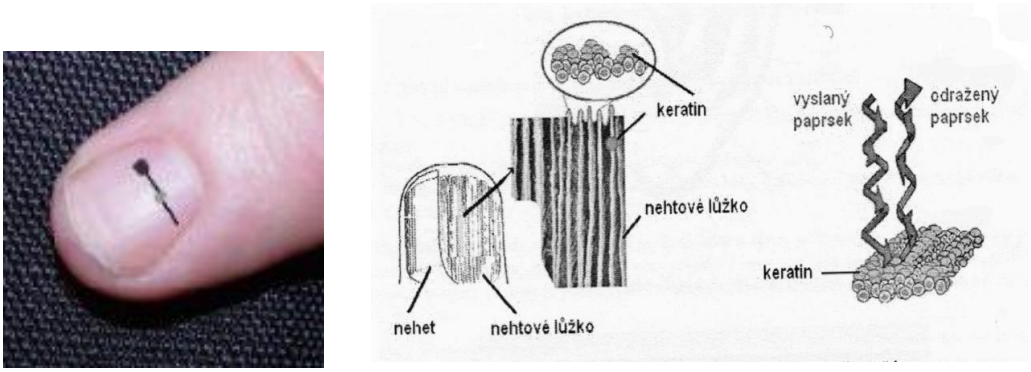
Pohyb a výraz obličeje lze využít v biometrické identifikaci rovněž na detekci pohybu rtů. Rty jsou pomocí PC na obličeji zvýrazněny a je sledována jejich dynamika při hovoru. Tato se pravidelně opakuje a tento pohyb lze využít k individuální identifikaci osoby. Základní princip verifikace osob podle pohybu rtů je na obrázku 38.



Obrázek 38: Algoritmus snímání charakteristického pohybu rtů

3.1.21 Identifikace podle podélného rýhování nehtů

Na prvni pohled se zdá, že rýhování nehtů je poměrně viditelným znakem. Metoda neidentifikuje přímo toto rýhování, ale strukturu, která se nachází pod ním, tedy nehtové lůžko. K identifikaci bylo využito keratinu v prostoru mezi nehtem a nehtovým lůžkem. Keratin je přírodní polymer, který mění orientaci dopadajícího světla. Pokud použijeme zdroj polarizovaného světla pod určitým úhlem a ozáříme jim nehet, můžeme zachytit a analyzovat fázové změny paprsku po odrazu z nehtu na přijímači. Po zpracování signálu získáme číselnou sekvenci čárového kódu, který lze rychle porovnat s databází. (viz Obrázek 39)



Obrázek 39: Identifikace podle podélného rýhování nehtů

3.1.22 Identifikace pomocí spektroskopie kůže

Někdy je také tato metoda zvána Lumidigm Reads Skin Physiology. Lidská kůže se skládá z několika vrstev, každá z vrstev má odlišnou tloušťku a tato tloušťka se u každého člověka jedinečně mění, je jedinečně zvlněná a vyznačuje se dalšími charakteristickými rysy. Kolagenové a pružná vlákna se u každého člověka liší, i kapilární lůžka jsou odlišná ve své hustotě a rozmístění, dále se liší velikost a hustota buněk uvnitř pleťových vrstev. Výzkumu této identifikační metody je v poslední době věnována velká pozornost.

Princip metody spočívá v tom, že vybraná část pokožky je ozářena světlem o více vlnových délkách (od viditelného až k blízkému infračervenému světlu). Každá vlnová délka světla se láme a odráží v jiné vrstvě pokožky a od jiných struktur kůže. Odraz je zachycen přijímačem složeným z fotodiod a předán k další zpracování a analyzováni. (viz Obrázek 40)

Obrázek 40: Princip skin spektroskopu se senzorem zn. Lumidigm

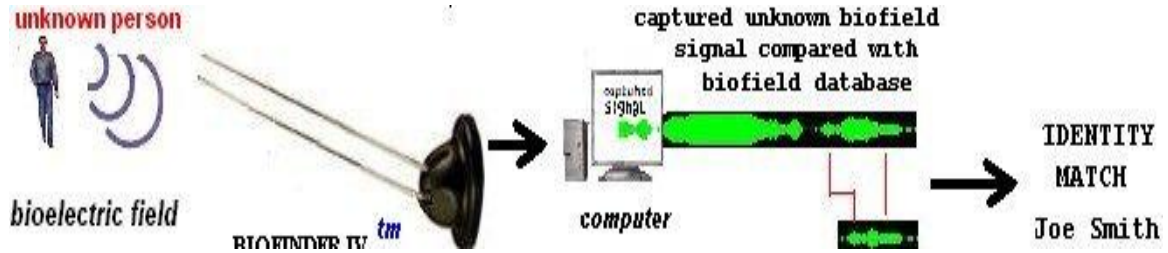
3.1.23 Identifikace uživatele střelné zbraně podle dynamiky uchopení a stisku

Další možností využití biometrie je při zabránění střelby neoprávněným uživatelem zbraně. Jedná se o US patent z roku 2005 z New Jersey institutu technologie, který popisuje biometrické parametry vyvolané rozpoznáním dynamického uchopení střelné zbraně. Uživatelé uchopí pevně pažbu zbraně obsahující tlakové snímače a tlakový profil uživatele. Snímače zaznamenají tlak a jeho rozložení v časové závislosti a srovná uložený záznam v počítači se seznamem oprávněných osob. Pokud se oprávněná osoba v seznamu nevyskytuje, bude mechanismus střelné zbraně zablokován a nebude možné zbraň použít. Zařízení bude miniaturizováno a vloženo pažby zbraně. (viz Obrázek 41)

Obrázek 41: Biodynamický identifikátor uchopení a stisku střelné zbraně

3.1.24 Bioelektrické pole

Bioelektrická pole jsou vlastně biologická hesla umožňující přímou identifikaci jedinců pomocí neviditelného bioelektrického vlnění každé jednotlivé osoby, které je jedinečný pro každého jednotlivce stejně jako DNA. Tato pole lze zaznamenat detektorem (například zn. BIOFINDER II), který zjistí bioelektrické pole konkrétní osoby a při jejím dalším průchodu prostorem identifikuje její totožnost. Nevýhodou je, že osoba musí jít sama, protože snímač nedokáže rozlišit jednotlivá bioelektrická pole více osob, které mají tato pole společná. Na obrázku 42 je znázorněn princip bioelektrické identifikace.



Obrázek 42: princip detekce bioelektrického pole

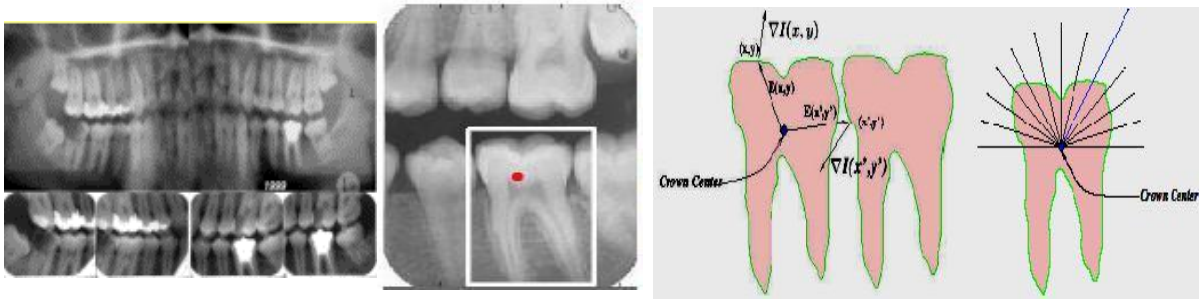
3.1.25 Biodynamický podpis osoby

Biometrická metoda vyvinutá v roce 2005 firmou Idesia, která dodala na trh snímač biodynamického podpisu osoby pod značkou BDS500 (viz Obrázku 43) vychází z principu elektrokardiogramu. Tento biosignál, podle kterého lze individuálně identifikovat osobu je sejmut při dotyku dvou prstů ruky na malé vodivé kovové kontakty. Osobou projde nepatrný elektrický výboj, podle kterého lze osobu identifikovat. Bio – Dynamic Signature (BDS) je pro každého jednotlivce jedinečné a přesný k zjištění totožnosti.

Obrázek 43: snímač biodynamického podpisu osoby

3.1.26 Verifikace podle biometrických vlastností zubů

Zatím málo využívaná v praxi je metoda identifikace osob podle biometrických vlastností zubů. Využívaná je zatím především pro identifikaci těl neznámých osob a v kriminalistické technice. Existuje několik metod zjištění totožnosti podle zubů, vždy je však nutné sroznat zjištěné údaje se záznamy. Jeden z příkladů biometrické identifikace zubu je na obrázku 44.



Obrázek 44: Postup biometrické identifikace zubů

3.1.27 Identifikace osoby podle plantogramu

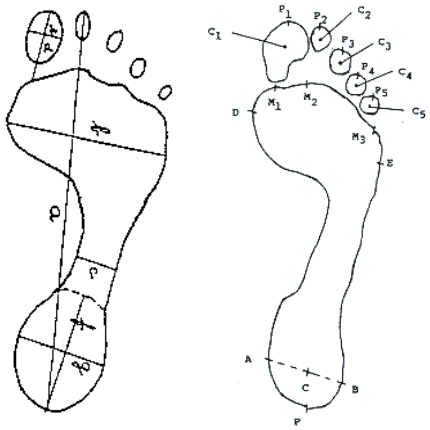
V kriminalistice je všeobecně známo, že stopy bosé nohy (plantogramy) zajištěné na místě trestného činu jsou pro každého člověka individuální, specifické a je možné je využít v identifikačním zkoumání a individuální identifikaci osob. Za „plantogram“ je tedy označován otisk bosého chodidla zatíženého vlastní váhou těla. Plantogramy odrážejí vnitřní stavbu chodidla, jako jsou různé záhyby kůže, jizvy nebo při velmi kvalitním otisku i kresbu papilárních linií. V lékařských vědách je frekventován pojem podogram, v kriminalistickém zkoumání je ale relevantnější zkoumání plantogramu bosé nohy.

Jak ukazují výzkumy, je identifikace osoby možná nejen ze stopy plošné na rovné tuhé podložce, ale i ze stopy v obuvi, z protlačené stélky obuvi. Shrnutím studia získaných

materiálů a vlastních experimentů na velkém množství plantogramů můžeme výsledky shrnout do těchto závěrů:

1. Na rozsáhlých výzkumech se prověřil a dosud potvrdil jeden z důležitých předpokladů individuální identifikace osoby, a to ten, že neexistují dva jedinci, kteří by měli tvarově stejný plantogram bosé nohy.
2. Plantogram každé osoby vykazuje několik pevně definovatelných identifikačních faktorů, které jsou ryze individuální pro dané chodidlo a s dobou a zátěží se podstatně nemění. Jsou vytvářeny v individuálním vývoji každého člověka.
3. Největší individuální odchylky byly experimentálně nalezeny v zásadě ve dvou zónách plantogramu, a to na metatarzální hranici plantogramu a v geometrii a individuálním rozložení prstů nohy.
4. Identifikaci osoby podle plantogramu je možné provést komplexním posouzením všech individuálních geometrických odchylek v přední části plantogramu – metatarzální hranice a geometrie prstů nohy. Pro vlastní identifikační zkoumání je důležitá zejména přední část plantogramu a především rozložení prstů a přední metatarzální hranice plantogramu.
5. Plantogramy zajištěné z pěšinky lokomoce jedné osoby nevykazují navzájem významné rozdíly v rozměrech identifikačních faktorů. Z toho plyne, že k identifikačnímu zkoumání lze vzít jakýkoliv čitelný a úplný plantogram.
6. Jak vyplývá z dostatečného množství experimentů a měření, je dostatečné a reálné uvažovat na každém plantogramu 19 identifikačních parametrů. Spolehlivost zjištění identifikace osoby se zvyšuje při zajištění obou plantogramů, a tedy uvažování 38 parametrů.

1. Délka chodidla, šířka přední části DE, šířka paty AB	- 3 rozměry
2. Vzdálenosti PP_1, ..., PP_5	- 5 rozměrů
3. Vzdálenosti CC_1, ..., CC_5	- 5 rozměrů
4. Vzdálenosti CM_1, CM_2, CM_3	- 3 rozměry
5. Vzdálenosti PM_1, PM_2, PM_3	- 3 rozměry



Obrázek 45: Parametry plantogramu

4 Použití biometrie v praxi

Jednoznačným trendem současné doby je návrat biometriky do praxe. Biometrie má jednoznačně před sebou velkou budoucnost, protože neexistuje jiná metoda takto blízce spojená s identifikací konkrétní osoby. Německo v roce 2004 vydalo na biometriku 12 milionů eur, v roce 2009 už to má být 377 milionů eur.

Největším světovým advokátem biometriky jsou dnes Spojené státy. Od roku 2005 chtěly zavést biometrické pasy, ale prozatím od tohoto kroku musely ustoupit. Důvodem se staly mezinárodní nejasnosti ohledně toho, jaká data mají být shromažďována a v jaké podobě. Samozřejmě, že každý stát hájí na daném poli své zájmy a bez konsenzu alespoň podstatné většiny se projekt těžko podaří realizovat.

I turisté a běžní občané v USA se tak díky biometrice setkávají s tím, co dříve bylo vyhrazeno pouze podezřelým a kriminálníkům. Spojené státy navíc už dnes vydávají pro každého legálního zahraničního pracovníka identifikační kartu, která by v budoucnu měla obsahovat biometrické prvky. Toto rozšíření bude snadnější než v případě pasů, protože nevyžaduje žádný mezinárodní souhlas, jde jen o vnitřní věc USA.

Od roku 2004 byly každopádně odebrány otisky prstů a fotografie 23 milionů zahraničních návštěvníků na 115 amerických mezinárodních letištích. Roční náklady na veškerou americkou biometriku přitom dosahují závratných osmi miliard dolarů.

Ministerstvo obrany USA používá pro všechny vojenské osoby a kontraktory identifikační kartu CAS (Common Access Card), která obsahuje biometrická data i digitalizované fotografie držitelů, navíc pak jako ochranný prvek proti padělání hologramy. Dosud bylo těchto karet vystaveno přes deset miliónů kusů.

Ve Spojených státech je také flotila jednoho sta nákladních vozidel sloužících k dopravě nebezpečných materiálů (biologické, chemické, radioaktivní…), přičemž přístup do nich je možný pouze přes biometrické systémy. Navíc jsou jejich řidiči (podružný produkt biometriky) sledováni, zda nejsou stresovaní apod. Pro zajímavost: další systémy sledují dodržování trasy těchto vozidel, plánované i neplánované zastávky apod.

Biometrika si ale našla cestu i do komerční sféry. Třeba hotel Ceasars Palace v Las Vegas ji používá pro přístup hostů do pokojů. A jak Disney Land (Kalifornie), tak Walt Disney World (Florida) používají biometriku - k tomu, aby osoby se zakoupeným nepřenosným lístkem ho nemohly předat dále.

Z USA pojďme do Německa. V květnu 2005 schválila horní komora parlamentu vydávání ePassu, který obsahuje biometrickou technologii. ePass se vydává od listopadu 2005, od března 2007 bude obsahovat také biometrické prvky – otisky prstů (jeden z každé ruky). Stejně tak musí mít všichni návštěvníci země s dobou pobytu delší než tři měsíce biometrickou identifikační kartu. A na olympijských hrách v roce 2004 v Athénách byl přístup všem hostům do Německého domu umožněn jen na základě biometrické identifikace.

Biometricky nesmírně rozvinutým státem je Izrael. Hranice s pásmem Gazy denně překračuje za prací devadesát tisíc Palestinců, kteří mají speciální identifikační dokumenty vydané izraelskou armádou. Obsahují biometrické údaje otisků prstů, dále tváře a siluety ruky. Kromě toho je na nich nejen vytištěná fotografie, ale v digitalizované podobě je umístěná i na čipu.

Letiště Bena Guriona v Tel Avivu má pro časté cestující coby součást programu "frequent flyer" kartu rychlého odbavení, která obsahuje informace o siluetě ruky a otisky všech prstů. Přístup do uzavřených prostor díky ní trvá jen deset sekund.

V Iráku se vydává identifikační karta s biometrickými prvky, která je imunní vůči falšování. Při vytvoření šablony je tato odeslána i do centrální databáze – takže pokud je karta ztracena, data se dají z této databáze ověřit. Databáze obsahuje i další doplňkové informace, zvláště pak osobní historii dotyčné osoby – např. zda už někdy měla konflikt s vojenskými či policejními jednotkami.

V Japonsku zase došlo k zavedení bankomatů pracujících na principu biometrické identifikace dlaně. Podle zkušebního provozu dochází jen v 0,01 procentech k odmítnutí oprávněného uživatele a jen v 0,00008 procentech k akceptaci neoprávněné osoby.




Obrázek 45: Příklady použití biometrie

5 Jak obejít biometrické systémy

Výzkumník Cutomu Macumoto z Jokohamské národní univerzity prokázal, jak ošálit biometrické systémy. Údajně byl následujícími postupy úspěšný v osmdesáti procentech případů. Do zahřáté plastické hmoty udělal otisk prstu. Do takto vytvořené formy pak nalil želatinu, kterou nechal vychladnout. Získal tak umělý prst, který následně mohl úspěšně použít. Další případ je, kdy stačí získat otisk, třeba na sklenici. Ten se posype kriminalistickým aluminiovým práškem a otiskne na průhlednou fólii. Fólie se přiloží na fotocitlivou PCB desku pro výrobu tištěných obvodů. Desku osvítíte a vyvoláte, čímž získáte plastický otisk prstu. Zatímco notebook se ukázal jako velmi spolehlivý, dveře se otevřely po pouhém přiložení na papíře vytištěného otisku prstu.

5.1 Sledovaný biometrický atribut zahrnuje následující vlastnosti:

- Univerzálnost – každá osoba by tuto charakteristiku měla mít.
- Unikátnost – každá osoba by měla mít tuto charakteristiku jinou (tento rozdíl přitom musí být měřitelný).
- Stálost – charakteristika by měla být odolná proti změnám v čase (stárnutí).
- Získatelnost – tato vlastnost vypovídá o tom, jak snadno lze příslušnou charakteristiku získat pro měření.
- Přesnost – s jakou přesností a rychlostí lze charakteristiku změřit.
- Přijatelnost – stupeň přijetí technologie do každodenního života. Otisk prstu působí méně kontroverzně než třeba DNA.
- Odolnost – hodnota vypovídající o tom, jak snadné je příslušný systém obalamutit.

Seznam zkratek

ACS	Access Control Systems - Systémy řízení a kontroly vstupů
AFIS	Automated Fingerprint Identification System - Automatický systém identifikace dle otisku prstu
ANSI	American National Standards Institute - Americký národní standardizační ústav
CCD	Charged Coupled Device - Zařízení s nábojovou vazbou
CCTV	Closed Circuit TV - Uzavřený televizní okruh
CMOS	Complementary Metal Oxide Semiconductor - Polovodič s vrstvou kysličníku křemíku
DIN	Deutsches Institut für Normung - Německý normalizační ústav
DNA	Deoxyribonucleonicacid - Deoxyribonukleová kyselina
EBGM	Elastic bunch graph matching - Elastický srovnávací diagram
FAR	False Acceptance Rate - Koeficient nesprávného přijetí
FIR	False Identification Rate - Koeficient nesprávné identifikace
FMR	False Match Rate - Koeficient nesprávného rozpoznání
FNMR	False None-Match Rate - Koeficient nesprávné nerozpoznání
FRR	False Rejection Rate - Koeficient nesprávného odmítnutí
FTA	Failure To Acquire - Koeficient selhání přístupu
FTA	Fault Tree Analysis - Analýza stromem poruch
IEC	International Electrotechnical Commision - Mezinárodní komise pro elektrotechniku
INCITS	International Committee for Information Technology Standards - Mezinárodní komise pro standardizaci informačních technologií
ISO	International Organization for Standardization - Mezinárodní organizace pro standardizaci
OASIS	Organization for the Advancement of Structured Information Standards - Organizace pro rozvoj strukturovaných informačních standardů
PIR	Pasive Infrared - Pasivní infračervené čidlo
TFT	Thin Film Transistor - Tenkovrstvý tranzistor

Použitá literatura

1. BOHÁČEK, Petr. *Systémy AFIS a rozpoznávání otisků prstů*. [s.l.], 2005. 10 s. VÚT Brno - Fakulta Informačních technologií. Semestrální práce.
2. BOSH Security Systems [online]. IP produkty – HW. 2008. Dostupný z www: <http://bosch-securitysystems.cz/produkty.php?sel_skup=178#>.
3. BROMBA, Manfred. *BIOIDENTIFICATION* [online]. 2007 [cit. 2007–11-10]. Dostupný z WWW: <http://www.bromba.com>
4. CONET [online]. Přístupové systémy. 2001. Dostupný z www: <http://www.conet.cz/pristupove_systemy.html>
5. ČSN EN 50131-1: *Poplachové systémy – Elektrické zabezpečovací systémy. Část 1: Všeobecné požadavky,* 1999, Změna Z7:2008, Český normalizační institut
6. ČSN EN 50133-1: *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Část 1: Systémové požadavky,* 2001, Změna A1:2003, Český normalizační institut.
7. ČSN P ENV 1627: *Okna, dveře, uzávěry – odolnosti proti násilnému vniknutí. Požadavky a klasifikace,* 2000. Český normalizační institut
8. *FBI Biometric: Center of Excellence* [online]. [1995] [cit. 2007-12-11]. Dostupný z www: <http://www.fbibiospecs.org/fbibiometric/biospecs.html>.
9. GALBAVÝ, Martin. *Vizualizace a vzdálené řízení v síti LonWorks*. [s.l.], 2006. 61 s. České vysoké učení technické v Praze – Fakulta elektrotechnická. Bakalářská práce.
10. JABLOTRON [online]. Detektory. 2005. Dostupný z www: <http://www.jablotron.cz/ezs.php?pid=products/ja-60p>
11. JAIN, Anil, BOLLE, Ruud, PANKANTI, Sharath: *BIOMETRICS - Personal Identification in Networked Society*. London : Kluwer Academic Publisher, 2002. 422 s. ISBN 0-792-38345-1.
12. MUL-T-LOCK [online]. Mechanické zabezpečovací systémy. 2006. Dostupný z www: <http://www.multlock.cz/cz/kategorie/produkty>
13. NSTC Subcommittee: *Biometrics Foundation Documents*. [s.l.] : [s.n.], [200-?]. 167 s.
14. PETÍK, L.: *Použití biometrické identifikace při zabezpečení objektu*, 2008. 46 s. VŠB TU Ostrava - Fakulta bezpečnostního inženýrství. Bakalářská práce.
15. SANDSTROM, Marie: *Liveness Detection in Fingerprint Recognition Systems*. Linkoping, 2004. 149 s.

16. SAPELI [online]. Dveře a zárubně. 2006. Dostupný z www: <http://www.sapeli.cz/index.asp?obsah=15&amp>
17. SOUMAR, C. *Biometric system security*. In *Secure*. [s.l.] : [s.n.], 01/2002. s. 46-49.
18. ŠČUREK, R.: *Přednášky z předmětu Ochrana objektů.* 2007.
19. UHLÁŘ, J.: *Technická ochrana objektů, I. díl, Mechanické zábranné systémy.* Praha, 2001. ISBN 80-7251-172-6.
20. UHLÁŘ, J.: *Technická ochrana objektů, II. díl, Elektrické zabezpečovací systémy.* Praha, 2001. ISBN 80-7251-076-2
21. VANĚK, R,: *Technologie digitálního snímání prstů*. [s.l.], 2007. 37 s. Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky. Bakalářská práce.