VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA OSTRAVA

Fakulta bezpečnostního inženýrství

Katedra bezpečnostních služeb

Biometrické technologie

Technické prostředky bezpečnostních služeb

Doc. Mgr. Ing. Radomír Ščurek, Ph.D.

2015

ISBN 978-80-248-3786-4

1 Úvod

Vážený studente,

Dostává se Vám do rukou učební text modulu Technické prostředky bezpečnostních služeb – biometrické technologie. Mým cílem při psaní tohoto textu bylo, aby zájemce získal základní znalosti a přehled v oblasti biometrie a profilace osob, které nachází široké uplatnění v bezpečnostní praxi.

Tento text je zpracován formou pro „distanční vzdělávání“, tak aby práce s ním byla co nejjednodušší. Každá kapitola začíná náhledem kapitoly, ve kterém se dozvíte, o čem budeme v kapitole mluvit a proč. V náhledu kapitoly se také dovíte, kolik času by Vám studium mělo zabrat. Prosím mějte na paměti, že se jedná pouze o informativní údaj, nebuďte proto prosím rozladěni, když se budete kapitole věnovat delší popřípadě kratší dobu. Za kapitolou následuje shrnutí, ve kterém budou zdůrazněny informace, které byste si měli zapamatovat.

To že jste probíranou látku správně pochopili a že jí rozumíte si můžete ověřit formou kontrolních otázek a testů, které by Vám měly poskytnout dostatečnou zpětnou vazbu k rozhodnutí, zda pokračovat ve studiu nebo věnovat delší čas opakování kapitoly.

V průběhu studia narazíte na tzv. korespondenční úkoly. Tyto úkoly je potřeba vypracovat a v termínech daných Vaším studijním harmonogramem odevzdat. Tyto korespondenční úkoly poslouží k Vašemu závěrečnému zhodnocení.

Pro zjednodušení orientace v textu je zaveden systém ikon:

Čas pro studium

Odhadovaný čas, který budete potřebovat pro prostudování daného tématu

Shrnutí kapitoly

Shrnutí nejdůležitějších informací, které byste si rozhodně měli pamatovat

Otázky

Kontrolní otázky, pro formulace odpovědí

Správná odpověď

Správná odpověď na kontrolní otázky

Test

Test, podle kterého zjistíte, jak na tom jste

Přestávka

Samá práce, žádná legrace? Někdy je prostě potřeba trošičku polevit, abyste se ve výkladu neutopili.

Náhled kapitoly

V takto označeném textu se dovíte, co Vás čeká a nemine

Literatura

Doplňková literatura, pro kterou můžete sáhnout v případě, že něčemu nebudete rozumět, nebo Vás některé téma extrémně zaujme

Zapamatujte si

Definice, chytáky, zajímavosti, prostě důležité věci, které je potřeba zdůraznit

Rada autora

Poradíme, pomůžeme…

Korespondenční otázka

Tuto otázku je potřeba vypracovat a zaslat tutorovi podle jeho pokynů

Přeji Vám, aby čas strávený nad tímto textem byl co možná nejpříjemnější, a nepovažovali jste ho za ztracený.

Autor

2 Biometrie a základní pojmy

Cíl kapitoly

Cílem této kapitoly je získání základních informací o biometrii, možnostech jejího využití v bezpečnostní praxi, o metodách autentizace,

Vstupní znalosti

Pro nastudování této kapitoly musíte znát a vědět pouze základní poznatky nabyté na všeobecné základní škole.

Klíčová slova

Biometrie, biometrika, rozpoznání, ověření, identifikace, autentizace, token

Doba pro studium

Pro nastudování této kapitoly budete potřebovat 1 hodinu.

2.1 Úvod do problematiky

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.

2.2 Použité pojmy a jejich vysvětlení

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
-

2.3 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.**

2.3.1 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 osobou.

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.

2.3.2 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

2.3.3 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.

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

2.3.4 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.

Shrnutí

V této kapitole jste se seznámili se základními pojmy v oblasti biometriky a metod autentizace. Nabyté vědomosti budou dále používány a rozšiřovány v následujících kapitolách.

Otázky

1) Co to je biometrie ?
2) Jaký je rozdíl mezi rozpoznáváním a identifikací?
3) Jaká je nejčastěji používaná metoda autentizace?
4) Co je podstatu biometriky?
5) Jakým způsobem funguje logický token?
6) Která autentizací metoda je vhodná pro nejvyšší stupeň zabezpečení?

Test

a) Kolik je metod autentizace?
b) Vyjmenujte metody autentizace?
c) Vysvětlete pojem token?
d) Vyjmenujte druhy tokenů?
e) Uveďte alespoň 5 charakteristických znaků člověka, které využívají biometrické systémy?

Správná odpověď

a) 3
b) Autentizace heslem, autentizace předmětem, biometrická autentizace
c) Jedinečný předmět, vybavený informací nutnou pro autentizační protokol, prostřednictvím kterého se ověří identita uživatele.
d) Token pouze s pamětí, token s heslem, logické tokeny, inteligentní tokeny
e) 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

Přestávka

U téhle kapitoly jste se moc nezapotili, takže žádné zdržování a šup k další kapitole. ☺

3 Elektronické biometrické rozpoznávací systémy

Cíl kapitoly

Tato kapitola si klade za cíl seznámit čtenáře s principy fungování a využívání elektronických biometrických rozpoznávacích systémů ve forenzní a soukromé bezpečnostní praxi

Vstupní znalosti

Pro nastudování této kapitoly musíte znát a ovládat základní pojmy z oblasti biometrie, se kterými jste se seznámili v předchozí kapitole.

Klíčová slova

Otisk prstu, DNA, kontrola a řízení vstupů, měření výkonnosti biometrických systémů, bezpečnost biometrických systémů

Doba pro studium

Pro nastudování této kapitoly budete potřebovat 3 hodiny času.

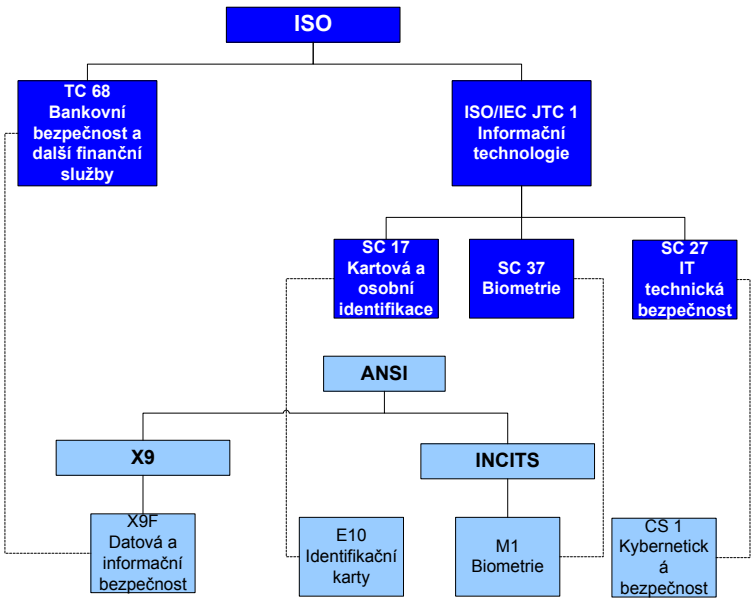
3.1 Možnosti využití biometrických systémů v praxi

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

3.2 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 ukládání:

- přímo do zařízení (do hlavní jednotky snímače)
- do vzdáleného počítače
- 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.

3.3 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.

3.3.1 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

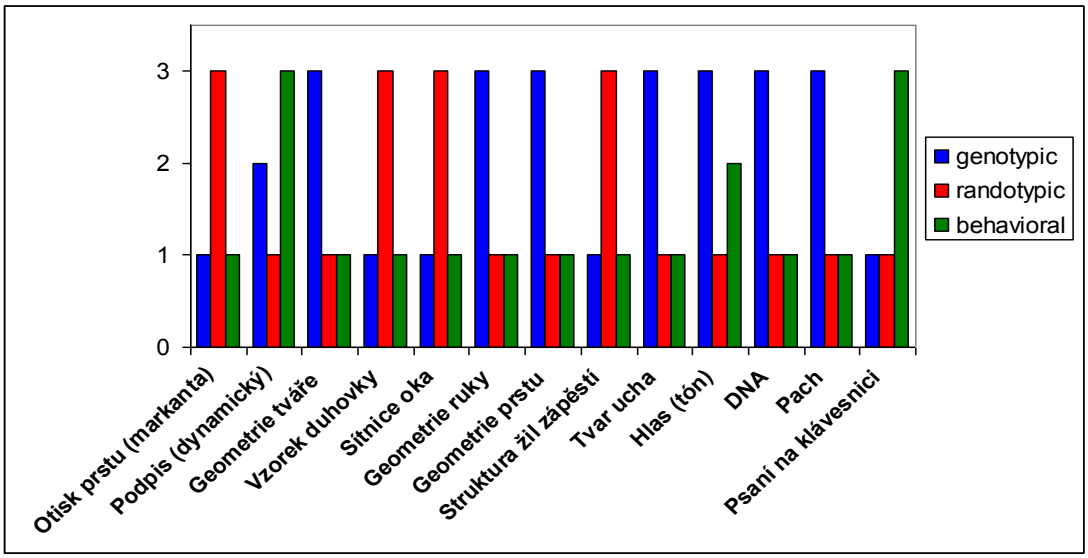
Nejlépe prozkoumané a nejvíce rozšířené biometrické vlastnosti používané pro identifikační účely jsou uvedeny níže spolu se stručným popisem toho, co se měří:

- 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

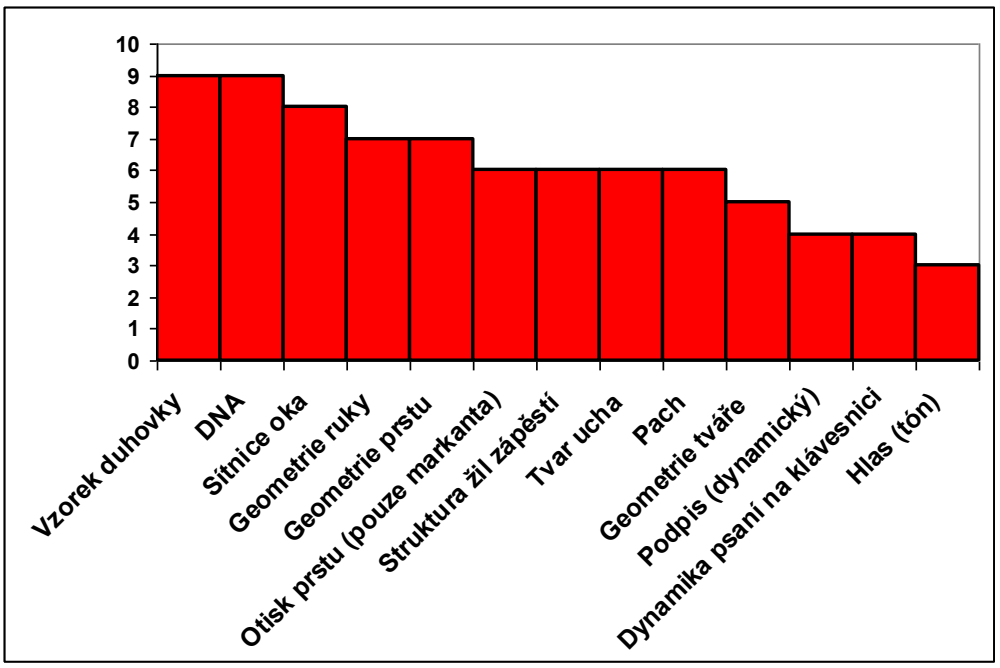
Na obrázku č. 3 jsou v tabulce přehledně popsány výhody a nevýhody jednotlivých biometrických znaků.

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)	oooooooo o(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)

Obrázek č. 3: Porovnání jednotlivých biometrických vlastností

Jak již bylo zmíněno, jedním z nejdůležitějších 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. DNA ztrácí body v komfortu snímání a také v přesnosti, protože jednovaječná dvojčata mají shodnou DNA.

3.4 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
- doba ověření.

Takových koeficientů existuje ovšem celá řada v závislosti na hloubce zkoumání problému.

3.4.1 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

3.4.2 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.

3.4.3 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:

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

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

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

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

3.4.4 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.

3.4.5 False Match rate (FMR)

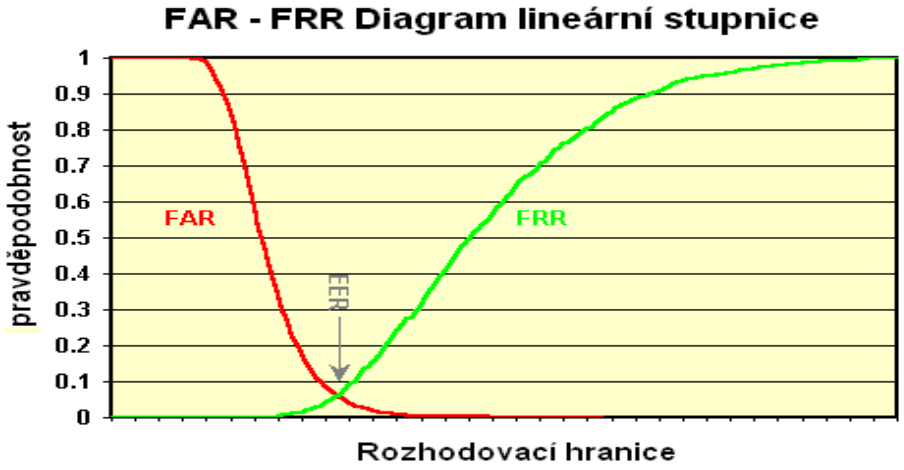
Koeficient FIR udává **poměr neoprávněných osob, které jsou nesprávně rozpoznány jako akreditované během srovnávacího procesu.** Porovnáme-li ho s koeficientem FAR, liší se v tom, že na rozdíl od FAR se do FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Znamená to tedy, že koeficienty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

3.4.6 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

3.5 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.

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

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.

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

FRRc - výsledná pravděpodobnost odmítnutí oprávněného uživatele
FAR (čidlo) - dílčí pravděpodobností odmítnuti oprávněného uživatele (záleží na počtu použitých metod)

3.6 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

Shrnutí

Kapitola byla věnována oblastem, kde se biometrické metody uplatňují, jak z hlediska soukromé, tak i forenzní praxe. Podrobně popisuje biometrické informace, které jsou za tímto účelem získávány a zpracovány. Dále pak systém řízení a kontroly vstupů, v neposlední řadě hodnotí systém měření výkonnosti uvedeného systému vstupů, včetně možností vedoucích k jeho zlepšování.

Otázky

1) V jakých sférách se uplatňují elektronické biometrické bezpečnostní systémy?
2) Kde lze využít vyhodnocování geometrie tváře v davu?
3) Pod jakou normou spadá systém ACS?
4) Jaké je třeba učinit bezpečnostní opatření při využití ukládání dat o verifikaci do vzdáleného PC?
5) Uveďte princip biometrického systému řízení a kontroly vstupu?
6) Jaký je jeden z nejdůležitějších požadavků na biometrickou

vlastnost člověka?

7) Jaký je vzorec pro vyjádření pravděpodobnosti neúspěšného sejmutí biometrické vlastnosti kontrolované osobě? (FER)
8) V jakých oblastech soukromé praxe se využívá biometrický systém rozpoznávání pro ověřování identity osob?

Test

a) Uveďte nejznámější a nejpoužívanější biometrický systém užívaný ve forenzní praxi?
b) Uveďte český překlad systému AFIS?
c) Vysvětlete pojem ACS?
d) Uveďte možnosti ukládání výsledků verifikace?
e) Uveďte, jaké parametry by měla vhodná biometrická vlastnost člověka splňovat?
f) Jakým způsobem vznikají biometrické vlastnosti člověka?
g) Uveďte výkonnostní míry měření efektivnosti biometrických systémů?
h) Co je to Křížový koeficient?
i) Uveďte možnosti, které leze využít, ke zvýšení bezpečnosti biometrických systémů?

Správná odpověď

a) AFIS
b) Automatický systém identifikace otisku prstu (Automated Fingerprint Identification Systém)
c) Jedná se o systém kontroly a řízení vstupů

d) Výsledky verifikace je možné ukládat: přímo do zařízení, do vzdáleného PC, do tokenu
e) Vhodná biometrická vlastnost člověka by měla mít parametry: jedinečnost, univerzálnost, trvalost, měřitelnost, uživatelská přijatelnost
f) Biometrické vlastnosti člověka vznikají: genetickým vývojem, náhodnými variantami vzniku v časném stádiu vývoje embrya, skrz učení a výchovu
g) Výkonnostní míry jsou: koeficient nesprávného přijetí, koeficient nesprávného odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu, doba ověření
h) Křížový koeficient udává míru pravděpodobnosti, při jakém nastavení hranice rozhodování nastane jev FAR a FFR současně (FAR udává pravděpodobnost toho, že neoprávněná osoba je přijata jako oprávněná, koeficient FRR udává pravděpodobnost toho, že oprávněný uživatel je systémem odmítnutý), je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR.
i) Lze využít aplikace ezoterické identifikace nebo vícenásobné biometrie.

Přestávka

A máte to za sebou ☺. V klidu si udělejte kávu nebo čaj, protáhněte se a můžeme se pomalu pustit do další kapitoly.

4 Jednotlivé biometrické technologie

Cíl kapitoly

V bezpečnostní praxi je využíváno mnoho metod k individuální identifikaci osob. S výčtem a popisem nejznámějších a nejčastěji využívaných metod Vás seznámí tato kapitola.

Vstupní znalosti

Pro studium tohoto studijního textu jsou předpokládány pouze znalosti pojmů a odpovídajících souvislostí z oblasti biometrie a biometrických systémů, které byly popsány v předchozích kapitolách.

Klíčová slova

Verifikace, geometrie ruky, geometrie tváře, duhovka oka, sítnice oka, struktura žil na zápěstí, behaviometrika, dynamika chůze, plantogram

Doba pro studium

Pro nastudování této kapitoly budete potřebovat 5 hodin času.

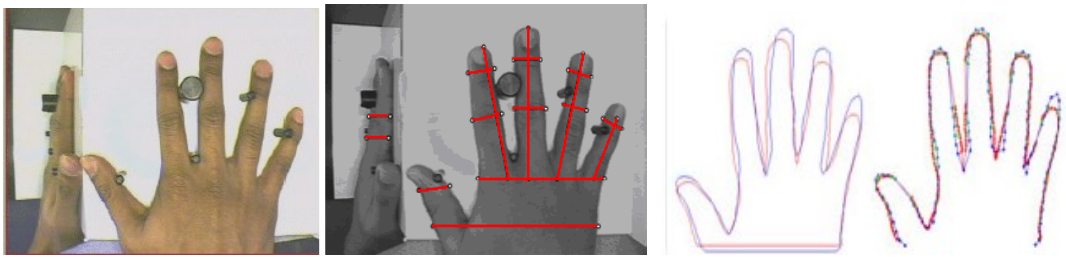
4.1 Geometrie ruky

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 č. 4) pomocí CCD kamery.



Obrázek č. 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**

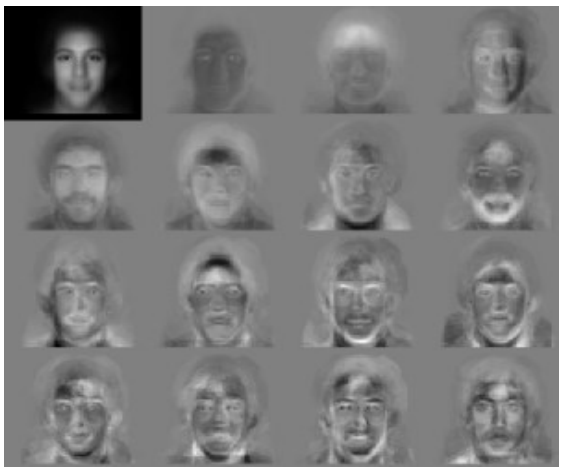
4.2 Geometrie tváře

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).



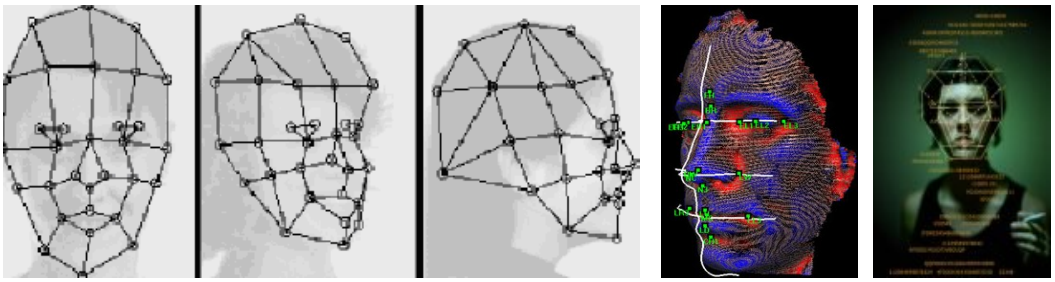
Obrázek č. 5: Standardní eigenfaces používané pro rozložení obrazu

PCA využívá vektorů tváře odvozených z 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. Obrázek č. 5). Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo.

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 Obrázek č. 6).

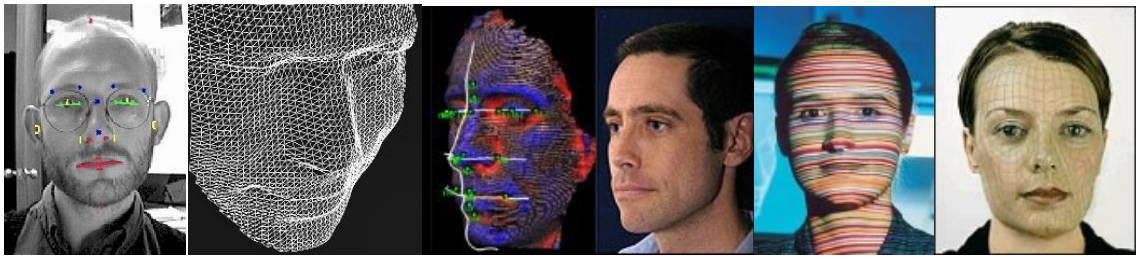
Obrázek č. 6: Příklad šesti tříd užitím LDA

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. Obrázek č. 7). 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 spolehlivosti: střední**



Obrázek č. 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 č. 8: Počítačové zpracování bioemetrických dat obličeje

4.2.1 Nepřesnosti detekce tváře

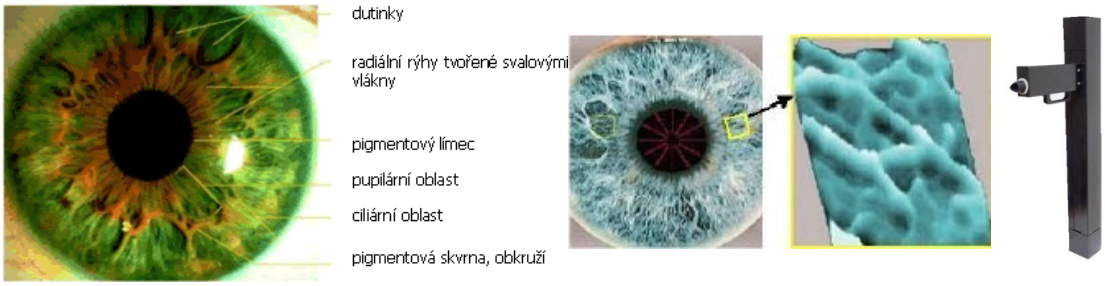
Systémy, které jsou schopny poznávat tváře, omezují rozsah možného správného výběru na třetinu všech možných kandidátů pozitivní identifikace. Jestliže je tvář osoby vyfotografována venku, a to z úhlu 45 stupňů, typický automatizovaný systém selhává v osmdesáti procentech případů,“. Vliv má také proměnlivost 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.

4.3 Duhovka oka

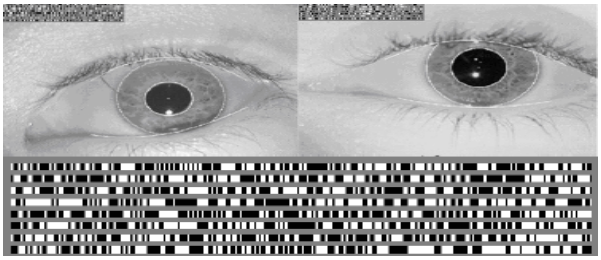
Automatické biometrické systémy pro rozpoznávání duhovky lidského oka jsou relativně nové vyvinuté. První patent je datován k roku 1994 a vyvinul ho americký Úřad pro jadernou bezpečnost včele s Dr. Johnem Daugman.

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 č. 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 č. 10) a šablony pro identifikaci.



Obrázek č. 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**

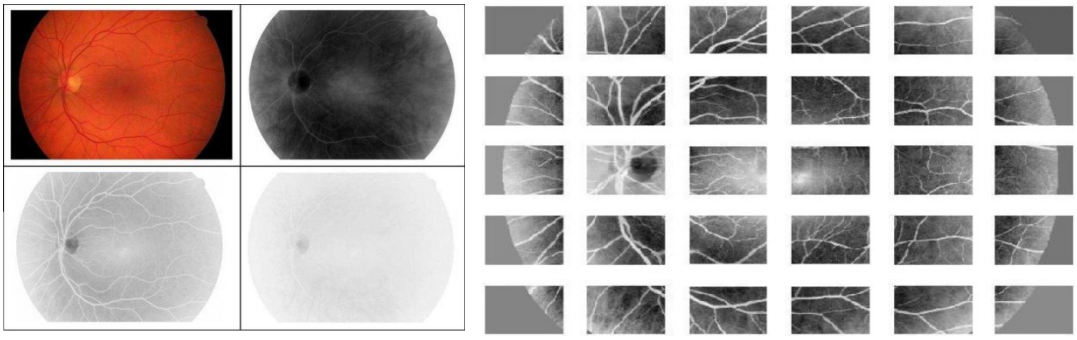
4.4 Sítnice oka

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.

Segmentace cévního systému lze proto využít i pro identifikaci osob. Další významnou oblastí využití může být i registrace retinálních snímků. V dnešní době existuje více metod pro automatickou segmentaci cévního systému ze snímku sítnice. Mezi nejznámější přístupy patří **segmentace založené na přizpůsobených filtrech, vlnkové transformaci, nebo regionově orientované segmentaci**.

Diskrétní vlnková transformace

Metody založené na přizpůsobených filtrech a regionově orientované segmentaci se vyznačují vyšší kvalitou segmentace, ale i delším časem výpočtu. Naopak metody založené na diskrétní vlnkové transformaci jsou relativně rychlé, ale segmentace nedosahuje stejných kvalit jako u výše zmiňovaných přístupů. Hlavní otázkou je, jak kvalitní segmentace je vyžadována pro danou aplikaci. Podle toho se poté zvolí vhodný přístup.



Obrázek č. 11: Vstupní RGB obraz a jeho G složka

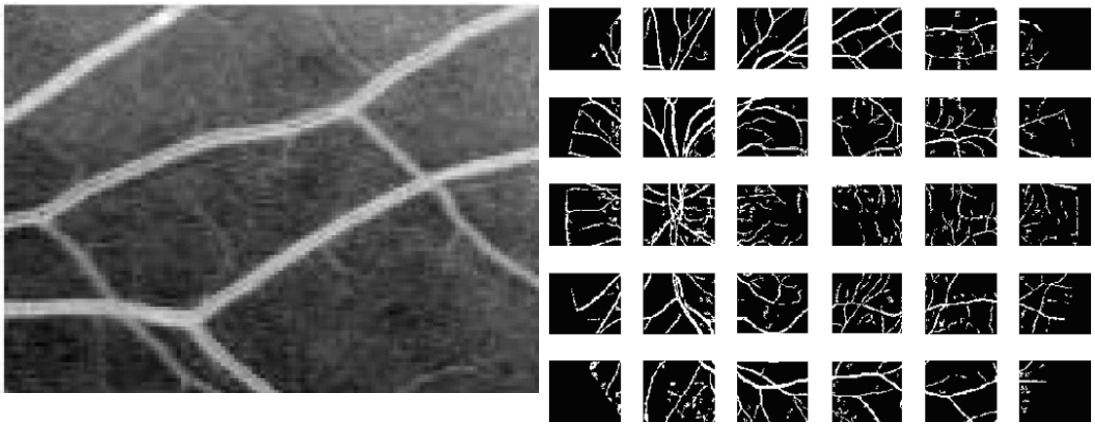
K tomu aby bylo možné cévy segmentovat, je nutné vstupní RGB obrázek rozdělit na jednotlivé R,G,B složky. Složky R a B nenesou významnou informaci o cévním řečišti. K následnému zpracování se použije pouze G složka, jelikož vykazuje nejvyšší kontrast cév vůči pozadí obrazu, jak je patrné na Obrázku č. 11 (vlevo). I nadále je však

obraz poměrně nevhodný pro další zpracování, protože nehomogenita jasu pozadí je značná a kontrast cév se v různých oblastech výrazně liší. Proto byl následně tento obraz rozdělen na menší oblasti (fragmenty), které se opět normovaly na úroveň jasu od 0 – 255 (Obrázek č. 11 – pravá část). Tímto se jednotlivé fragmenty stávají vstupními maticemi celého algoritmu. Z každého fragmentu se cévní řečiště segmentuje zvlášť a na konci celého procesu se jednotlivé fragmenty s binární reprezentací cévního řečiště složí ve výsledný obraz. Mozaika fragmentů byla nastavena na 5 horizontálních a 6 vertikálních oblastí. Tento poměr je vhodný proto, že každý fragment by měl obsahovat alespoň jednu cévu. Cévy obvykle tvoří nejsvětlejší objekty v obraze. Kdyby fragment neobsahoval cévu, mohlo by díky normování dojít k nežádoucímu zvýraznění šumu.

Dekompozice fragmentu a nespojitost cévního řečiště

Princip je založený na 2D diskrétní vlnkové transformaci. Pro detekci cév je zvolena reverzní biortogonální mateřská vlnka. Tvar vlnky nejlépe odpovídá náběžné hraně cévy. Díky tomu, že vlnková transformace v tomto případě detekuje náběžné hrany cév, nikoli cévy samotné, dochází k detekci oblastí větších, než jsou samotné cévy. Bohužel není k dispozici vlnka, která by dokázala cévy detekovat, aniž by zvětšila jejich průměr. Dekompozicí fragmentu se tím pádem získá mapa oblastí s výskytem cév. Po následném prahování se vytvoří binární reprezentace oblastí s výskytem cév (Obrázek č. 12). Když se binární reprezentace vynásobí se vstupním fragmentem, vznikne výsledný obraz, ve kterém jsou cévy zachovány, ale oblasti vyplňující jejich meziprostor jsou odstraněny i s případným šumem, nebo nehomogenním pozadím.

Na vzniklý fragment se aplikuje prahování s hysterezí, čímž se odstraní šum v blízkosti cév. Díky normování jednotlivých fragmentů postačuje prahování s hysterezí s pevně nastavenými prahy. Prahy jsou nastaveny heuristicky tak, aby byl poměr segmentovaných cév vůči segmentovanému šumu z pozadí obrazu co nejmenší. Protože fragmenty jsou normovány od hodnoty 0 – 255 úrovní jasu a cévy patří mezi nejsvětlejší objekty v obraze, jsou zvoleny prahy 140 a 220.

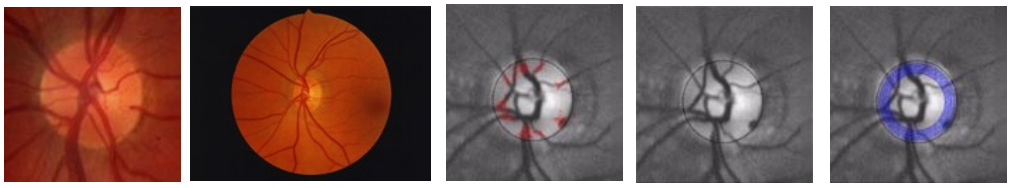


Obrázek č. 12: Jeden fragment vstupní G složky a fragmenty s binární reprezentací cév

Výhoda tohoto postupu je, že velikost segmentované cévy odpovídá velikosti cévy v originálním obrazu. Posledním krokem celého procesu je složení všech fragmentů do výsledného obrazu binární reprezentace cévního řečiště celého očního pozadí. Nespojitost cévního řečiště způsobuje prahování, kde pixely příslušící k cévě nedosahují jasové hodnoty nižšího prahu. Tím dochází k jejich potlačení. Bohužel není možné práh zvýšit, protože by docházelo k zvýraznění artefaktu segmentovaného pozadí obrazu. Mezi oběma artefakty je nutné zvolit kompromisní hodnotu prahu. Nespojitosti jsou příliš velké k tomu, aby je bylo možné doplnit jinou např. morfologickou metodou. Navíc jsou takové operace náročné na dobu výpočtu, což je také nežádoucí. K artefaktu segmentovaného pozadí obrazu dochází principielně opačně

jako k artefaktu nespojitých cév. Jasová hodnota pixelu, který nepřísluší k cévě (tzn. pozadí obrazu) převyšuje hodnotu prahu a dochází k falešně pozitivnímu vyhodnocení cévy. Každý fragment vstupního obrazu je segmentován zvlášť. Tím, že se fragment na začátku algoritmu normuje na jasové hodnoty 0 - 255, může dojít k tomu, že céva v jednom fragmentu vykazuje jiný kontrast, než stejná céva v sousedním fragmentu. Rozdílný kontrast může způsobit, že v jednom fragmentu je céva detekována pozitivně a v druhém nikoli. K tomuto artefaktu dochází jen ve fragmentech, kde je velký výkyv jasových hodnot, jako je například oblast v blízkém okolí optického disku.

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.**

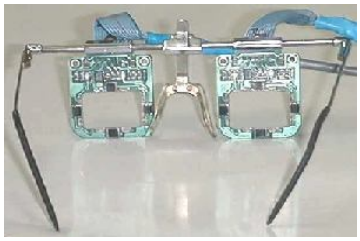


Obrázek č. 13: Lokalizování sítnice a znázornění charakteristických parametrů

4.5 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.

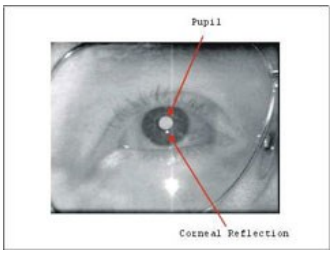
Upravené brýle pro tuto potřebu jsou na Obrázku č. 12. Tento způsob zatím není však využíván komerčně.

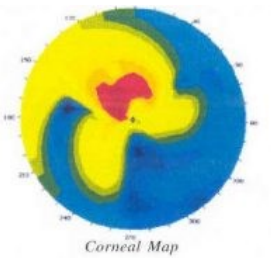


Obrázek č. 12: Brýle ke sledování pohybu očí

4.6 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 č. 14: Princip verifikace při povrchové topografii rohovky

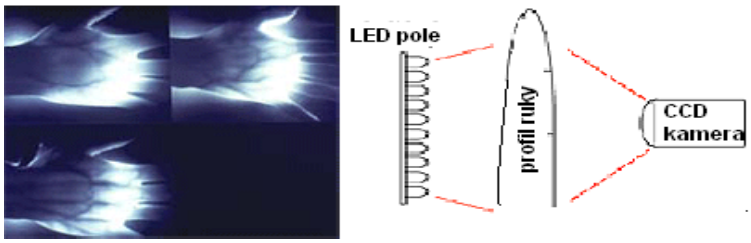
4.7 Struktura žil na zápěstí

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 č. 15) 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 č. 15: 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 č. 15. 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 č. 16.

Obrázek č. 16: 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**.

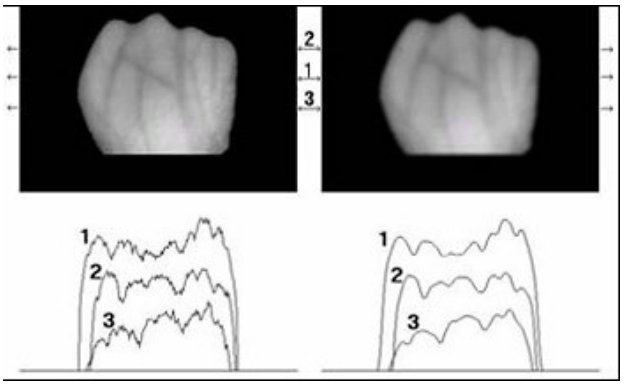
- **Segmentace obrazu**

Účelem tohoto primárního kroku je rozdělit nasnímaný obraz na část ruky, tj. požadované části, a pozadí obrazu. Na Obrázku č. 17 je část ruky zobrazena bíle a pozadí černě. Poslední část obrazu napravo je výstup tohoto kroku, tj. obraz s vycentrovanou částí ruky.

Obrázek č. 17: 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.

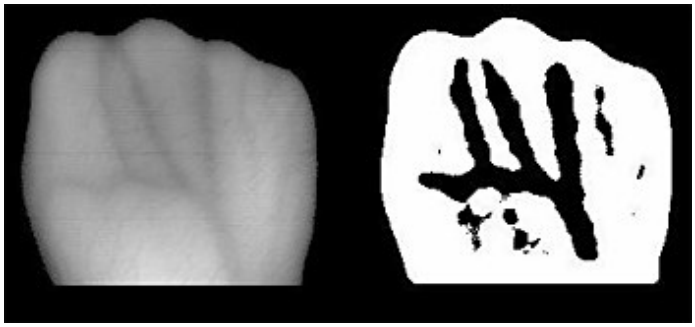


Obrázek č. 18: Vyhlazení obrazu hřbetu ruky

- **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 č. 19: 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 č. 20 je zobrazena (v pravé části obrázku) výsledná šablona, která se při verifikaci porovnává s uloženou šablonou uživatele.

Obrázek č. 20: 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 č. 21. Snímač je schopen zachytit obraz dlaně bez ohledu na pozici a pohyb dlaně.

Obrázek č. 21: Snímač dlaně

Nejdříve se zachytí **snímek dlaně infračerveným paprskem**, jak je vidět na Obrázku č. 22. Síť tmavších čar (zvýrazněná krev obsahující odkysličený hemoglobin) zde představuje vzorec žil dlaně.

Obrázek č. 22: IR snímek dlaně

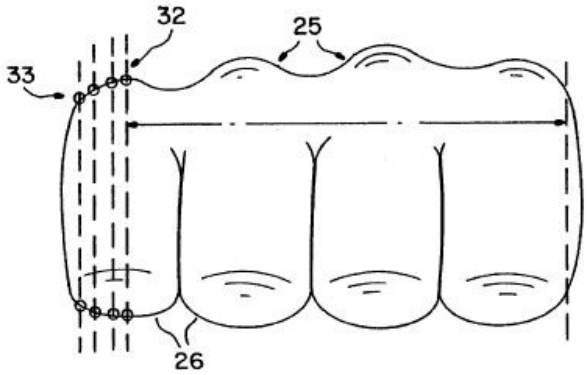
Z tohoto obrazu **systém extrahuje vzorec žil dlaně do nového obrazu**, viz Obrázek č. 23. Takovýto obraz se následně dle potřeby

transformuje a porovná s uloženou šablonou registrace uživatele.

Obrázek č. 23: Extrahované žíly dlaně

4.8 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 č. 24 jsou uvedeny příklady možných měření.

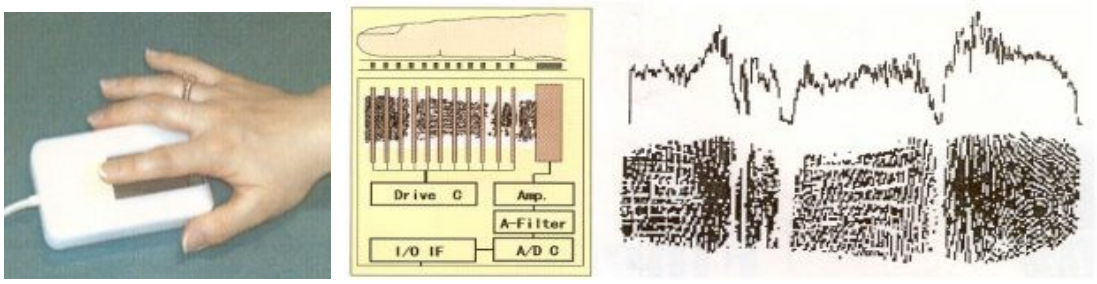


Obrázek č. 24: Biometrické parametry sevřené dlaně k verifikaci totožnosti.

4.9 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 č. 25.



Obrázek č. 25: Snímač vrásnění článků prstu

4.10 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.

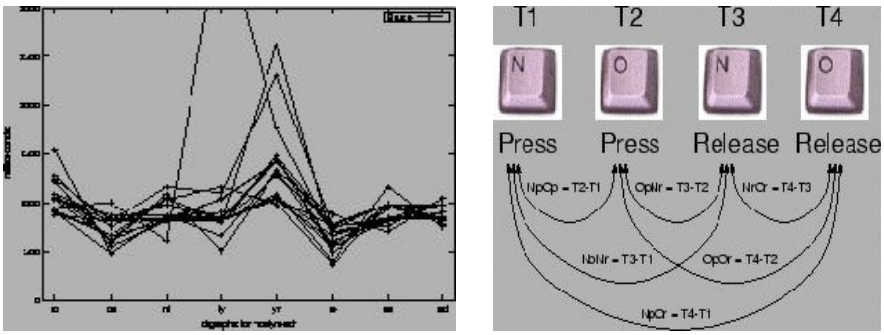
Jinak behaviometrika obsahuje třeba **studium stylu chůze, gest, typických znaků**. Můžete tak identifikovat osobu i na velkou vzdálenost

(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**.

4.10.1 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 č. 26: Dynamika psaní na klávesnici a diagram, který jí zachycuje

4.10.2 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 č. 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 č. 27: Princip dynamického podpisu; uživatel, měření a SW srovnání

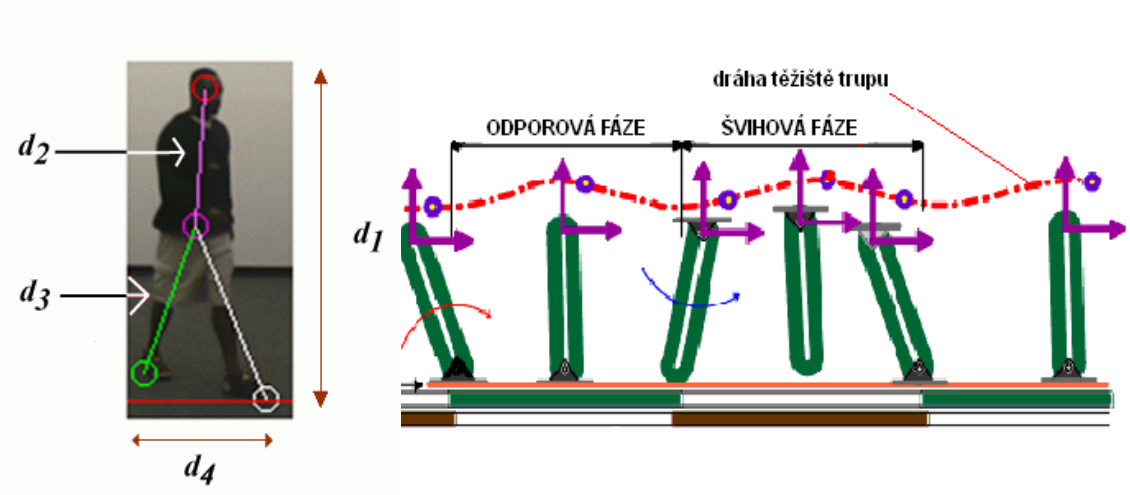
4.10.3 Dynamika chůze

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 č. 28



Obrázek č. 28: Postup vytváření dráhy těžištětrupu ¨při bipedální lokomoci

4.11 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.

4.11.1 Metody zachycení otisku prstů

- **Otisk získaný pomocí inkoustu a papíru**

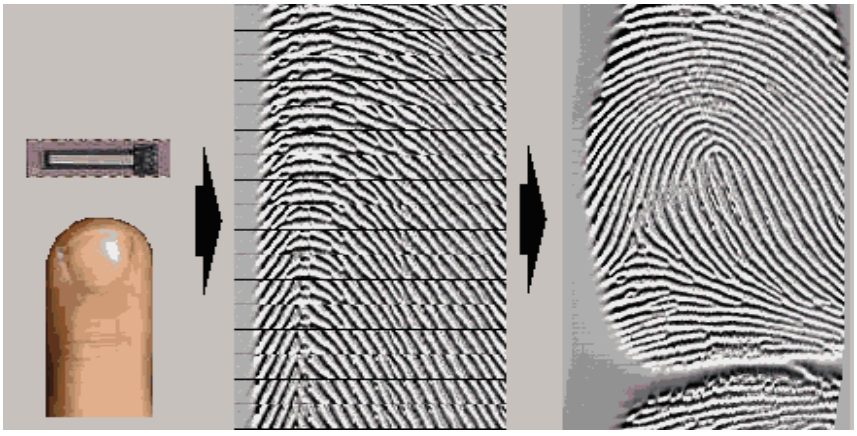
Klasická metoda (rolled finger). Tato metoda se používá pouze ve forenzní sféře, policií při vyšetřování. Používá se inkoustu a papíru. Prst se po papíře roluje, aby se získal otisk celého prstu (prakticky od nehtu po nehet) s co možná nejvíce použitelnými markantami a aby se tím zvýšila i rychlost rozpoznání 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 č. 29). 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.

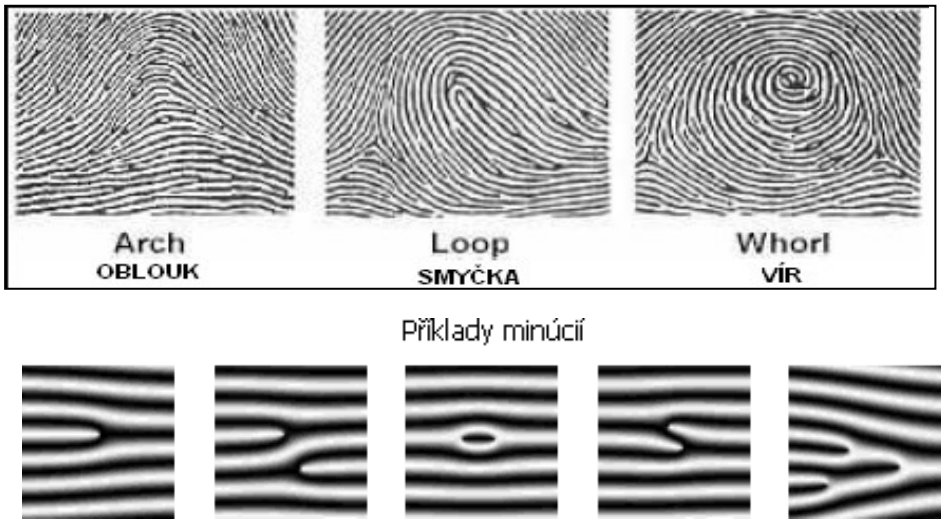


Obrázek č. 29: Postup zachycení obrazu otisku prstu šablonováním

4.11.2 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

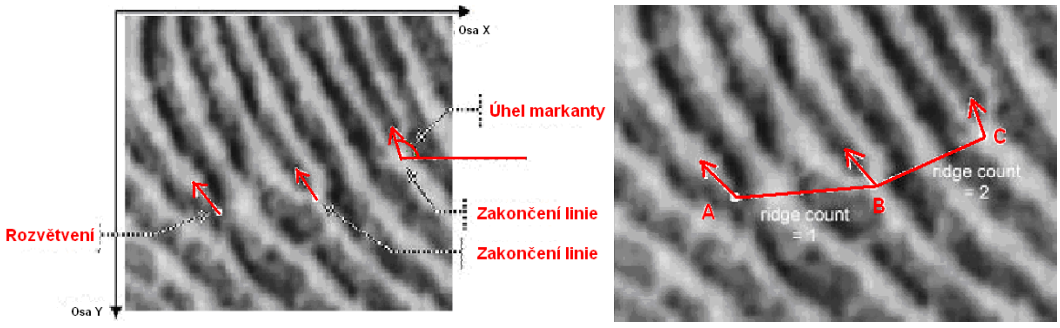
(seskupení papilárních linií). Jedná se o **smyčky, víry a oblouky** (loop, whorl, arch) viz Obrázek č. 30.



Obrázek č. 30: Ukázka hlavních seskupení papilárních linií

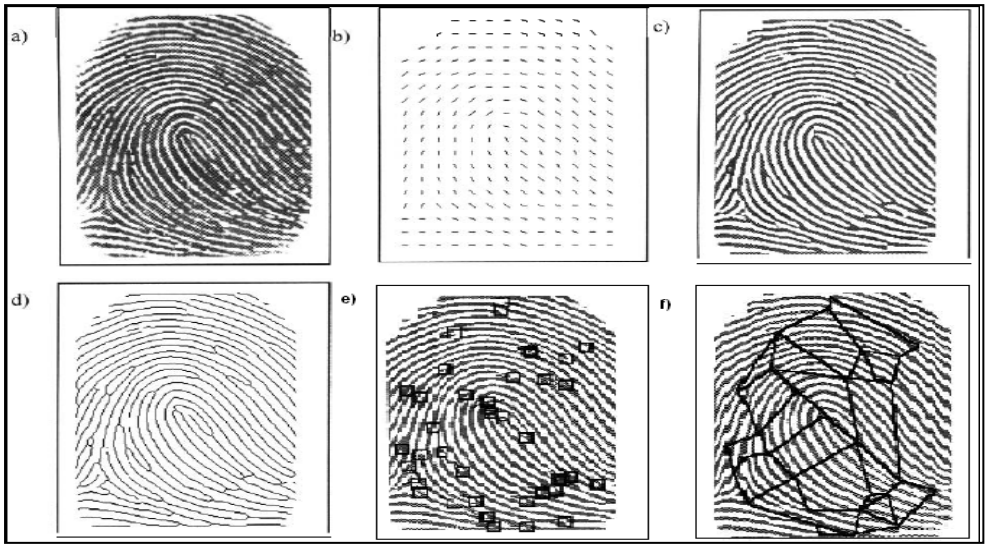
Některé algoritmy ukládají pro pozdější srovnávání pouze pozice (s=[x;y]) a směr (úhel Θ) markant, což vede k redukci dat nutných pro zápis (viz Obrázek č. 31a).

Jiné algoritmy namísto vzdálenosti znaku vypočítané z pozice, sčítají počet vyvýšených rýh mezi dvěma konkrétními body, zpravidla markantami (viz Obrázek č. 31b).



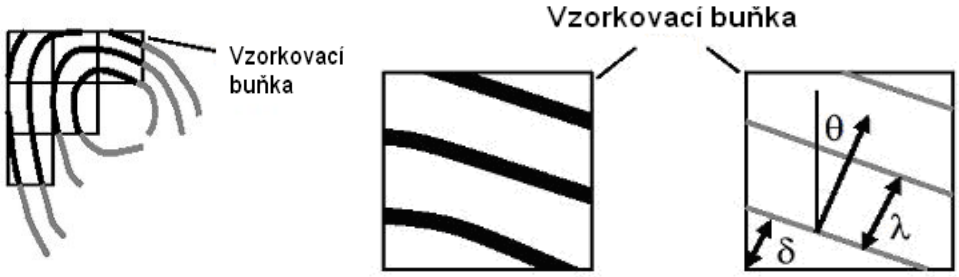
Obrázek č. 31: a) Příklady vzorkování markant b) Příklad sčítajícího algoritmu

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 č. 32).



Obrázek č. 32: 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. Obrázek č. 33). Velmi často používají algoritmy, které jsou kombinací několika metod.



Obrázek č. 33: 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**.

4.11.3 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}

4.11.4 Snímače otisků prstů

Existují desítky metod snímání otisku prstu využívající 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:

Optické senzory

- Na základě odrazu (reflexní)
- Reflexní se skládáním obrazu
- Bezdotykový odraz
- Transmisní

1. **Elektro-optické snímače**
2. **Kapacitní snímače**

- TFT optické

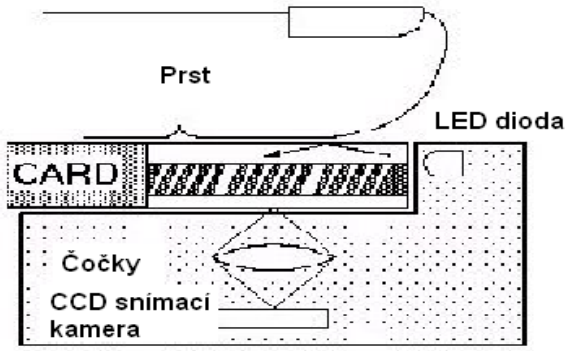
3. **Tlakové snímače**

- Vodivá membrána na silikonu
- Vodivá membrána na TFT
- Dotekové mikro-elektro-mechanické spínače

4. **Rádiové snímače**
5. **Teplotní senzory**
6. **Ultrazvukové snímače**
7. **Fotonové krystaly**
8. **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 č. 34). 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 č. 34: 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.

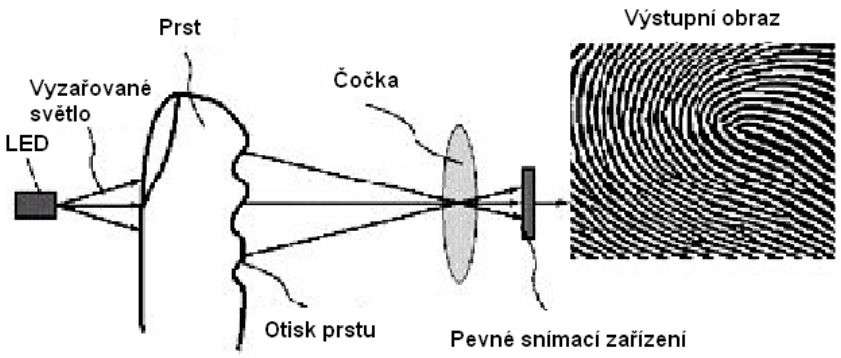
- **Optické bezkontaktní snímače**

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 35) 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 č. 35: 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)

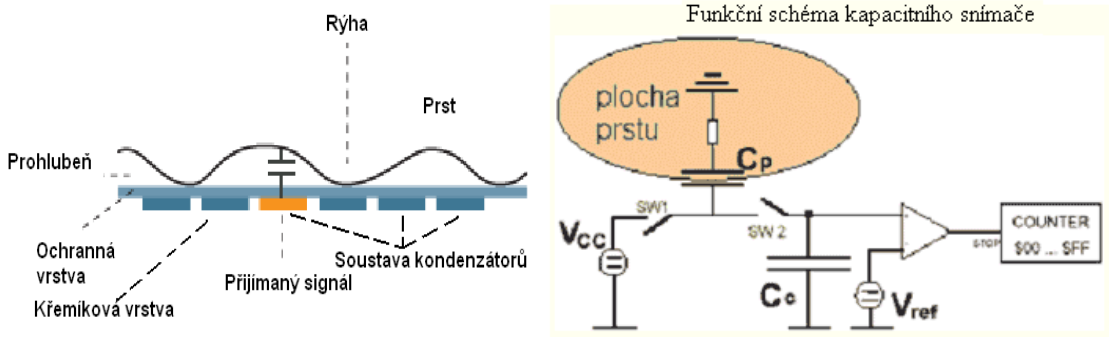
.

- **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 č. 36) 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 č. 36: 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. Taje vyrobena z křemíkového čipu pokrytého pyroelektrickým materiálem, neboli materiálem, který je citlivý na změny teploty. Na křemíku je nanesen v podobě přiléhajících pixelů. Teplotní diference se díky pyroelektrickému 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 na rozdíl 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.

4.11.5 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.

4.12 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.

4.13 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.

4.14 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.

Nejprve se ze vzorku tkáně vypreparuje 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.

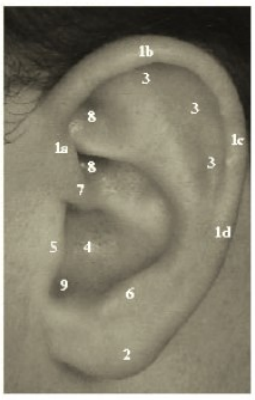
Takto získaná informace slouží k řešení celé řady otázek od přiznání otcovství až po identifikaci těl. Mnohé armády či záchranářské sbory proto budují databáze DNA svých zaměstnanců. Pro kontrolu přístupu v reálném čase však zatím tato technologie není použitelná.

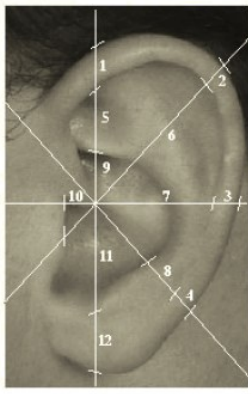
4.15 Biometrie ušního boltce

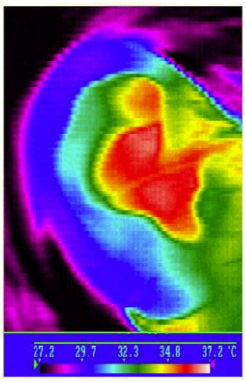
Identifikace člověka využívající biometrii ušního boltce je založená na **individuálním tvaru a morfometrické stavbě ušního botce každého jedince**. Obecně existují 3 metody biometrické identifikace podle ušního boltce:

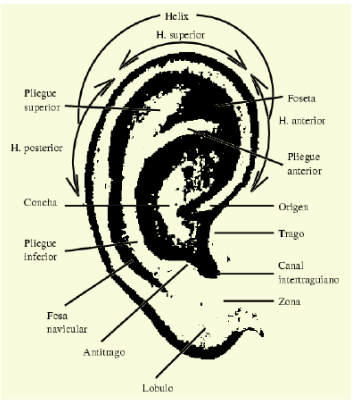
1. **Podle morfometrických vztahů** – geometrii ušního boltce, v 2D nebo 3D formě
2. **Podle otisku struktur ušního boltce** (podobně jako u otisků prstů) – tato metoda ale pro praxi není příliš "komfortní", její využití je ve forenzní oblasti
3. **Podle termogramu ušního boltce** – termografického snímku,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

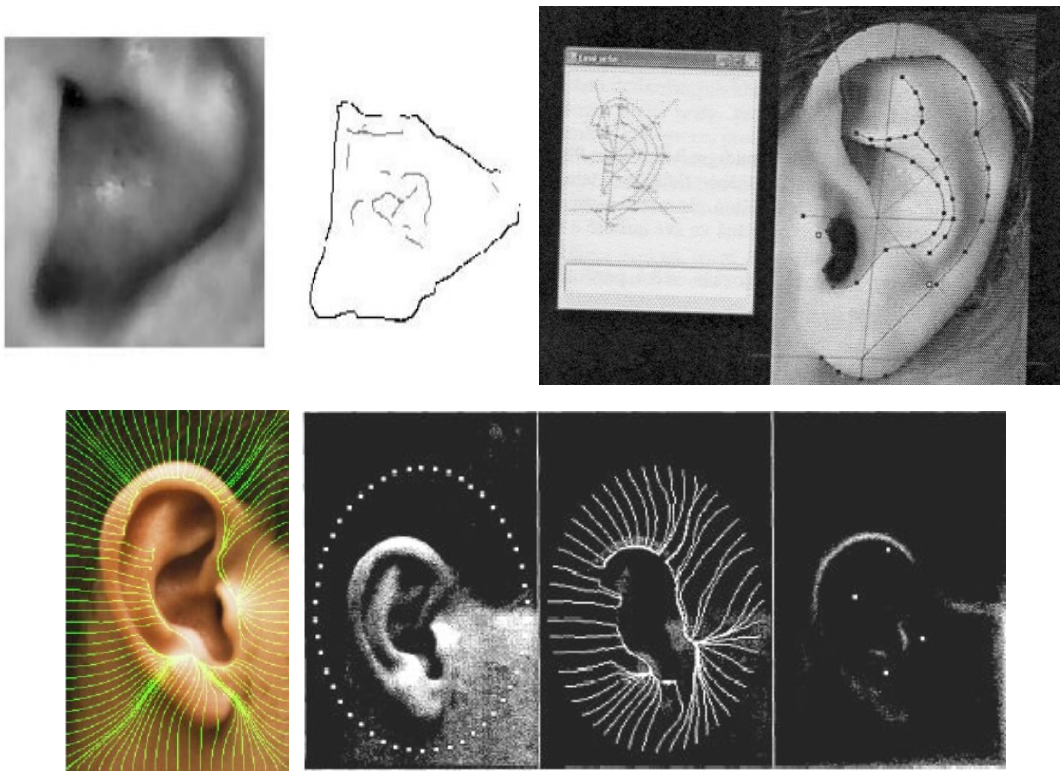
Použitelnou metodou pro komerční využití, tak aby byla komfortní pro uživatele, je identifikace podle morfometrických vztahů – geometrie ušního boltce. V tomto případě je uživateli ušní boltec nasnímán speciálním optickým snímacím zařízením, ze vzdálenosti cca 0,5 - 1 m. Data zanesená na snímku (morfometrické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







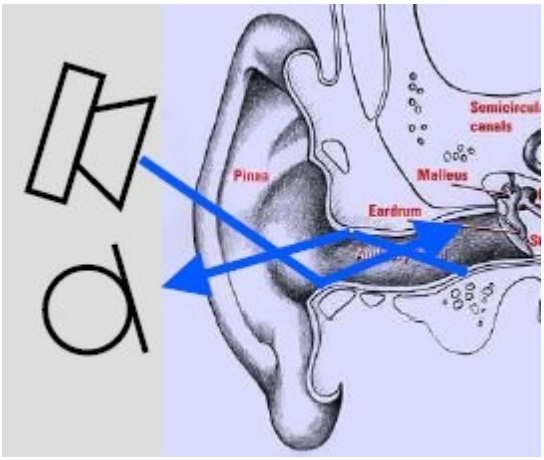




Obrázek č. 37: Biometrické měření parametrů ušního boltce

4.16 Verifikace odrazem zvuku v ušním kanálku

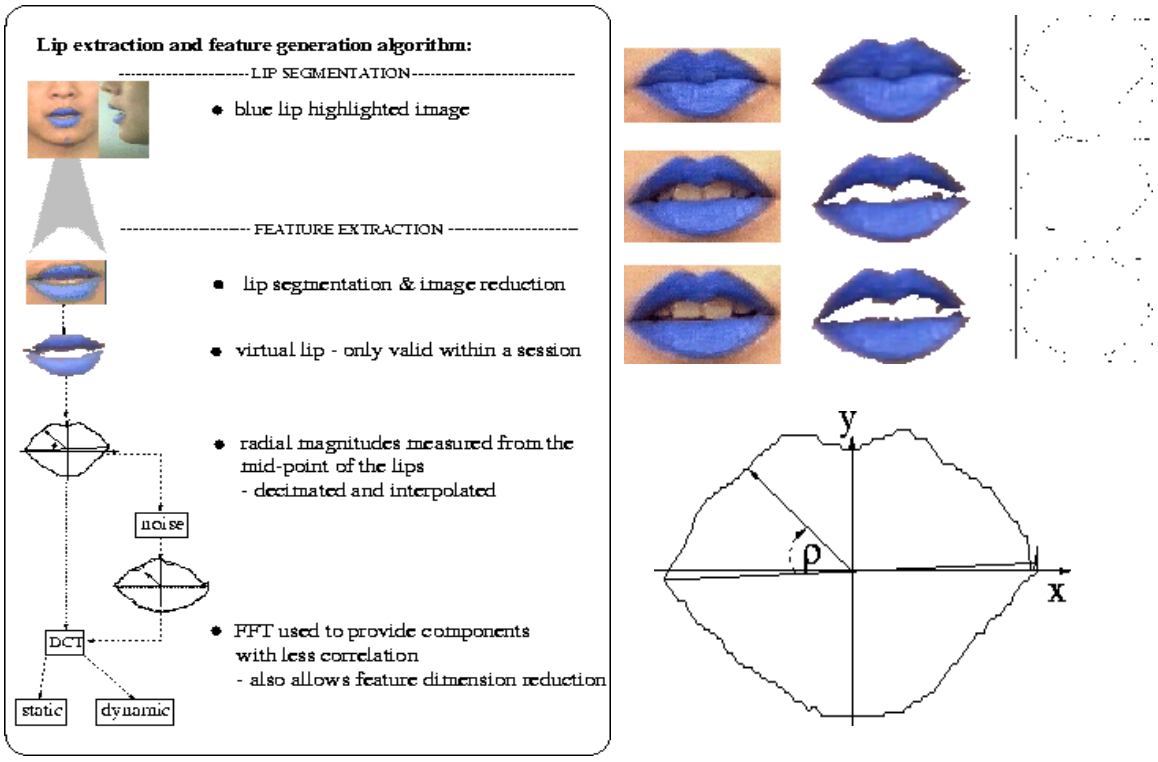
Jde o novou metodu, dosud málo využívanou v praxi. Při verifikaci osoba přiloží ucho k reproduktoru. **Zvuk se odráží od stěny zvukovodu a jeho část se vrací odrazem ušní stěny zpět**. Intenzita **pohlcení zvuku v ušním kanálku je u jednotlivců individuální** a podle této intenzity lze individuálně identifikovat osobu a ověřit její totožnost. Schéma je na Obrázku č. 38.



Obrázek č. 38: Odraz zvuku ve zvukovodu, jako prostředek individuální identifikace

4.17 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 č. 39.

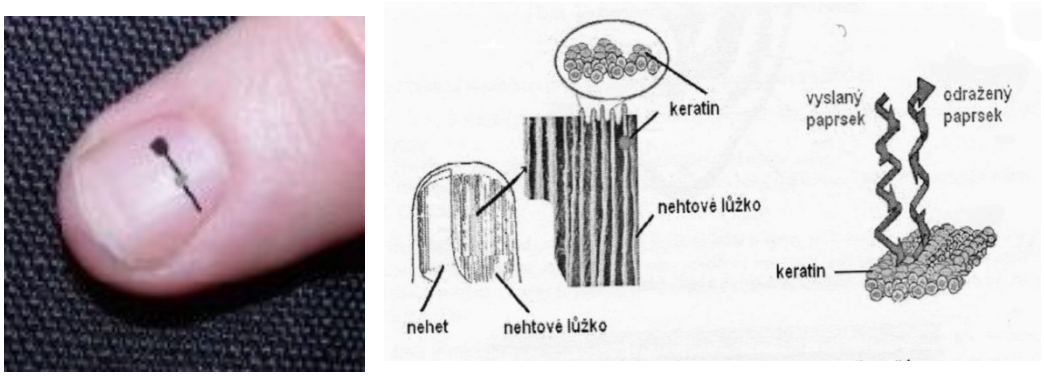


Obrázek č. 39: Algoritmus snímání charakteristického pohybu rtů

4.18 Identifikace podle podélného rýhování nehtů

Na první 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 č. 40)



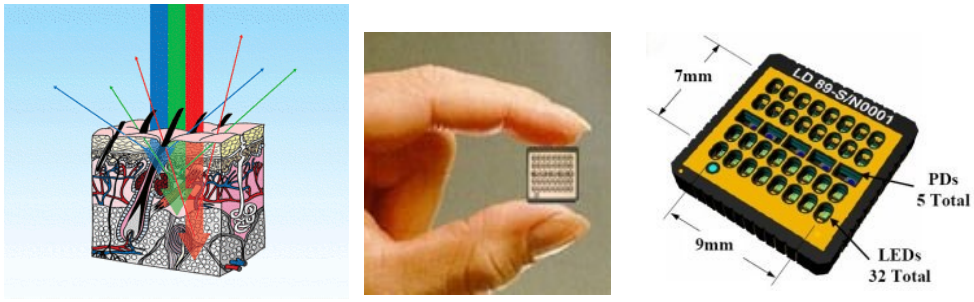
Obrázek č. 40: Identifikace podle podélného rýhování nehtů

4.19 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 č. 40)



Obrázek č. 41: Princip skin spektroskopu se senzorem zn. Lumidigm

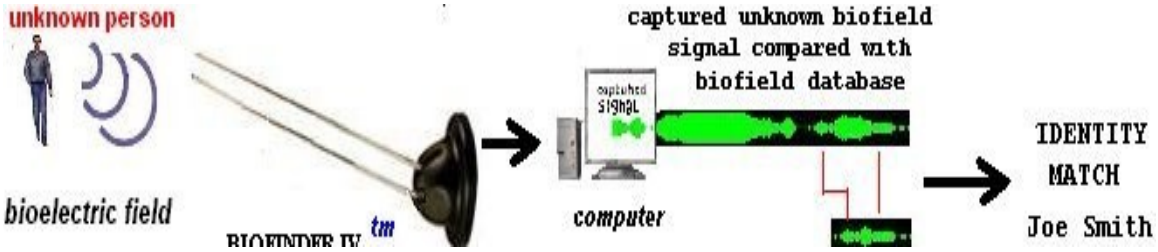
4.20 Identifikace uživatele střelné zbraně podle dynamiky uchopení a stisku

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 č. 42)

Obrázek č. 42: Biodynamický identifikátor uchopení a stisku střelné zbraně

4.21 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 č. 43 je znázorněn princip bioelektrické identifikace.



Obrázek č. 43: princip detekce bioelektrického pole

4.22 Biodynamický podpis osoby

Biometrická metoda vyvinutá v roce 2005 firmou Idesia, která dodala na trh snímač biodynamického podpisu osoby pod značkou BDS500 (viz Obrázku č. 44) 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 č. 44: snímač biodynamického podpisu osoby

4.23 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 srovnat zjištěné údaje se záznamy. Jeden z příkladů biometrické identifikace zubu je na Obrázku č. 45.

Obrázek č. 45: Postup biometrické identifikace zubů

4.24 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.

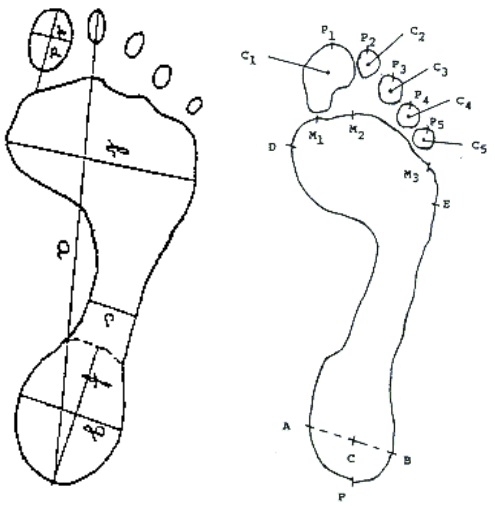
Jak ukazují výzkumy, je identifikace osoby možná nejen ze stopy plošné na rovné tuhé podložce, ale i ze stopy v obuvi, z protlačené stélky obuvi. Shrnutím studia získaných materiálů a vlastních experimentů na velkém množství plantogramů můžeme výsledky shrnout do těchto závěrů:

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 č. 46: Parametry plantogram

Shrnutí

Kapitola seznamuje čtenáře s jednotlivými metodami verifikace osob. Jsou zde přiblíženy metody známé, hojně využívané, ale také metody, které jsou prozatím předmětem odborného studia a na své využití v praxi stále čekají. Popisuje principy, kterými jsou data využívaná k identifikaci osob, získávány, zpracovány a uchovávány, včetně míry spolehlivosti jednotlivých systémů.

Otázky

1) Která bezpečnostní metoda je nejstarší implementovaný biometrický princip?
2) Jaké existují přístupy, které se uplatňují při rozpoznávání geometrie tváře?
3) Jaký je rozdíl mezi metodou PCA a EBGM?
4) Jaké vlastnosti ovlivňují spolehlivost detekce podle tváře?
5) Prostřednictvím čeho je snímána duhovka?
6) Jaké parametry se ukládají v systému identifikace, který využívá strukturu žil?
7) Jaké biometrické druhy snímání lze využít pro identifikaci osoby prostřednictvím dlaně?
8) Co je to behaviometrika? Co tato metoda studuje?
9) Jaká metoda zachycení otisku prstu se užívá ve forenzní praxi?
10) Co je to markantograf?
11) Jaké existují požadavky na senzory využívané v oblasti daktyloskopie?
12) V jaké oblasti se využívá DNA jako identifikační prvek?
13) Jaký je rozdíl mezi plantogram a podogram?

Test

a) Jaké parametry se porovnávají (měří a uchovávají) při využití metody verifikace prostřednictvím geometrie ruky?
b) Uveďte, jaké techniky se využívají při verifikaci obličeje?
c) Uveďte všechny algoritmy užívané k rozpoznání tváře?
d) Co je duhovka? Co ovlivňuje její funkci?
e) Jaký biometrický systémy vykazují vysokou míru spolehlivosti identifikace osoby?
f) Jaké metody se užívají při identifikaci člověka za pomoci sítnice oka?
g) Z kolika kroků (uveďte jakých) se skládá fáze rozpoznávání žil ruky?
h) Uveďte základní dynamické vlastnosti podpisu?
i) Vyjmenujte metody zachycení otisku prstu?
j) Jak se jmenuje nauka o pachu?
k) Vyjmenujte metody využívané při biometrické identifikaci ušního boltce?

Správná odpověď

a) Parametry snímané a posuzované v rámci verifikace rukou: snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka
b) Techniky užívané při verifikaci obličeje jsou: měření geometrických vlastností, párové porovnávání šablon
c) Algoritmy užívané k rozpoznání tváří: Analýza hlavních částí (PCA), Lineární diskriminační analýza (LDA), Elastický srovnávací diagram (EBGM)

d) Duhovka je sval uvnitř oka, který reguluje velikost čočky na základě intenzity světla dopadajícího na oko
e) Systémy vykazující vysokou míru spolehlivosti využívají k verifikaci: duhovku oka, sítnici oka, způsob pohybu očí, povrchovou topografii rohovky, daktyloskopické metody
f) Metody využívané v procesu verifikace pomocí sítnice oka: Segmentace s přizpůsobivými filtry, vlnová transformace a regionově orientovaná segmentace.
g) Metoda rozpoznávání žil má 4 kroky: segmentace obrazu, vyhlazení a redukce šumu, lokální prahování, postprocessing
h) Dynamické vlastnosti podpisu jsou: rychlost, akcelerace, časování, tlak a směr tahu
i) Metody využívané pro zachycení otisku prstu jsou: pomocí inkoustu a papíru, statické snímání, snímání šablonováním
j) Odorologie
k) Metody využívané k verifikaci ušního boltce jsou: morfometrické vztahy, otisk struktur ušního boltce, termogram ušního boltce

Přestávka

Ufff a máš to za sebou. ☺

Byla to dřina, tak si trošku odpočiň, protáhni se, udělej si radost něčím dobrým a můžeme se pustit do další kapitoly ☺

5 Metody profilace osob a biosignály

Cíl kapitoly

Seznámení se s využitím biometrických metod v bezpečnostní praxi, přiblížení současných bezpečnostních trendů.

Vstupní znalosti

Při studiu této kapitoly jsou využívány pojmy a vědomosti, se kterými se čtenář seznámil v předešlých kapitolách.

Klíčová slova

Profilace, radexový model, biosignály, videoanalýza, MALNTENT, WeCU, analýza hlasu, metoda vedení pohovoru

Doba pro studium

Pro nastudování této kapitoly budete potřebovat 3 hodin času.

5.1 Profilace

Profilace je **preventivní metoda** v oblasti bezpečnosti, která umožňuje identifikovat **nestandardní fyziologické projevy a chování u posuzovaných osob** a na základě analýzy těchto odchylek identifikovat potenciální ohrožení chráněných aktiv.

Úroveň profilování závisí na kvalitě informací potřebných pro vytvoření profilu. Primárním důvodem vytváření profilu je **selekce podezřelých osob z páchání trestné činnosti**. Profilování však **nezaručuje přesnou identifikaci pachatele**. Nastavení parametrů pro profilaci se liší dle oblasti aplikace. Profilace a typování podezřelých osob se hojně využívá v prostředí civilního letectví, kde slouží k minimalizování pravděpodobnosti teroristického útoku, či jiných protiprávních činů,

v souvislosti s bezpečností civilního letectví, na co nejnižší možnou míru.

Před samotnou aplikací profilace je potřeba znát profil běžného cestujícího, aby bylo možno hodnotit co největší míru odchylek u nestandardních reakcí.

Před realizací profilace by se měly učinit následující kroky:

1. **Analýza ohrožení** – definice letů s největším potenciálním rizikem ze strany pachatelů (teroristů).
2. **Znalost profilu standardního cestujícího** – profil cestujícího, který definovanou linku standardně využívá k přepravě.
3. **Vizuální profil potenciálních pachatelů** – na základě zkušeností, odborných publikací a dat z historie vytvořit profil vzhledu a chování potenciálního pachatele (teroristy).
4. **Znalost informací o každém cestujícím** – dle cestovní dokumentace (rezervace, letenka, doklady, atd.) – důležité informace o cestujícím a charakteru jeho cesty.
5. **Znalost postupu při pohovoru („questioning“)** – získání informací o cestujícím a jeho cestě, srovnání s údaji z cestovní dokumentace, ověření pravdivosti údajů, ověření reakcí na úmyslně aplikované podněty.

Pro určení **profilu standardního cestujícího** je potřeba znát odpovědi na následující otázky:

- O jaký druh letu se jedná (obchodní, charterový, atd.)?
- Jaký druh cestujícího standardně využívá tento let?
- Jak je běžný cestující tohoto letu oblečen?
- Jak se běžně chová cestující daného letu?
- Jaký je jeho běžný etnický původ?
- Jaká zavazadla standardně používá (typ, vzhled, počet)?
- Standardní trasa cesty cestujícího tohoto letu?
- Jaký je nejčastěji udávaný účel cesty daného letu?

Odpovědí na výše uvedené otázky je možné získat profil standardního cestujícího. Nestandardní projevy vybočující z normálního stavu, pak mohou být projevem záměru konat trestný čin proti bezpečnosti letecké dopravy.

5.2 Historie profilace

Původ oboru profilování je přisuzován americké FBI (Federal Berau of Investigation). Profilování **z pohledu kriminalistiky** lze charakterizovat jako **analýzu vzorců chování, charakteristik místa činu a vztahujících se trestných činů**. Ve vědeckém prostředí existují dva rozdílné přístupy k profilaci pachatelů, a to jednak tzv. „Škola FBI“ v USA, ale i takzvaná „Škola investigativní psychologie“ ve Velké Británii. Oba přístupy jsou odlišné v používaných metodách profilace a Škola investigativní psychologie vznikla na základě studií kritizujících metody FBI.

5.2.1 Profilování v pojetí FBI (Federal Berau of Investigation)

Profilování v pojetí FBI (deduktivní metoda) je definováno jako **proces interpretace forenzních důkazů a důkladné studium**

jednotlivého pachatele za účelem přesné rekonstrukce chování na místě činu.

Tento proces silně závisí na možnostech rozpoznání vzorců chování hledaných pachatelů. Způsob profilování **vychází z obecných pravidel chování pachatele**. Profilování v pojetí FBI rozděluje pachatele trestných činů na organizované a neorganizované. Poprvé bylo toto rozdělení užito pro pachatele vražd, později se začalo přenášet také na pachatele jiných typů trestných činů.

5.2.2 Profilování v pojetí tzv. Liverpoolské školy

Ve Velké Británii se profilováním pachatelů zabývá obor **investigativní psychologie** v Liverpoolu (Centre for Investigative Psychology). Cílem tohoto oboru je vytváření teorií pro policejní vyšetřování, které jsou zakotvovány do empirické a vědecké psychologie.

Tento způsob se nezaobírá pouze výzkumem trestných činů, ale také rozhodováním policie během vyšetřování a řízením informací. Metodika profilování vychází z empirických výsledků výzkumů daného počtu pachatelů určitého trestného činu. Získané údaje umožňují **vytvářet vzorce chování pachatelů určitých druhů trestných činů**.

5.2.3 Historie profilování v České republice

Počátky profilování pachatelů trestných činů v České republice sahají do 30. let 20. století. Poprvé bylo profilování zmíněno v knize Kriminální psychologie z roku 1930 od autora Josefa Šejnohy. V této knize autor popsal potřebu vyšetřovatele porozumět psychologické stránce pachatele (motiv trestného činu). Později se vzhledem k politické situaci v zemi vývoj profilování pachatelů pozastavil a další kniha Základy soudní

psychologie byla publikována až v roce 1964. Velký rozvoj nastal v osmdesátých letech, kdy se vyšetřovatelé a odborníci na trestnou činnost začali soustředit na dílčí aspekty kriminálního chování. V tomto období se tak objevilo velké množství publikací s tématem profilování. V roce 1981 definoval termín profilování J. Pješčak. Ve své knize Způsob páchání trestné činnosti a jeho význam (z roku 1982) napsal J. Musil: „ Způsob páchání trestné činnosti může být ovlivněn osobními rysy, intelektem či temperamentem pachatele.“ Další významnou publikací se stala kniha O. Suchého Osobnost pachatele I a II, ve které popisuje osobnost delikventa a recidivisty, jako pachatele trestných činů. Na počátku 90. let bylo publikováno několik článků zabývajících se užitím profilování v praxi. V tomto období byly napsány například publikace Kriminální agresor (Netík, 1990) a Psychologické profilování: mýtus a skutečnost (Čírtková, 1995). Velmi podrobný popis profilování pachatelů byl publikován v knize Vybrané kapitoly z kriminalistické psychologie od autorek I. Gillernové a H. Boukalové vydané v roce 2006.

5.2.4 Psychologické aspekty kriminálního chování

Je důležité uvědomit si variace mezi pachateli a trestnými činy:

- dlouhodobě připravovaný trestný čin je odlišný od spontánního,
- motivy trestných činů jsou u různých pachatelů různé,
- organizovaná a neorganizovaná trestná činnost,
- pachatelé nejsou specializováni pouze na jeden typ trestné činnosti.

Dále je možno podle multidimenzionálního pohledu detailněji specifikovat pachatele dle následujícího postupu:

kriminální x nekriminální chování

⇩

TČ spáchán na osobě x na majetku

⇩

druh trestné činnosti (vloupání, atd.)

⇩

vzorec kriminálního chování

⇩

způsob páchání trestného činu s jeho specifickými znaky

(modus operandi)

⇩

kriminální podpis

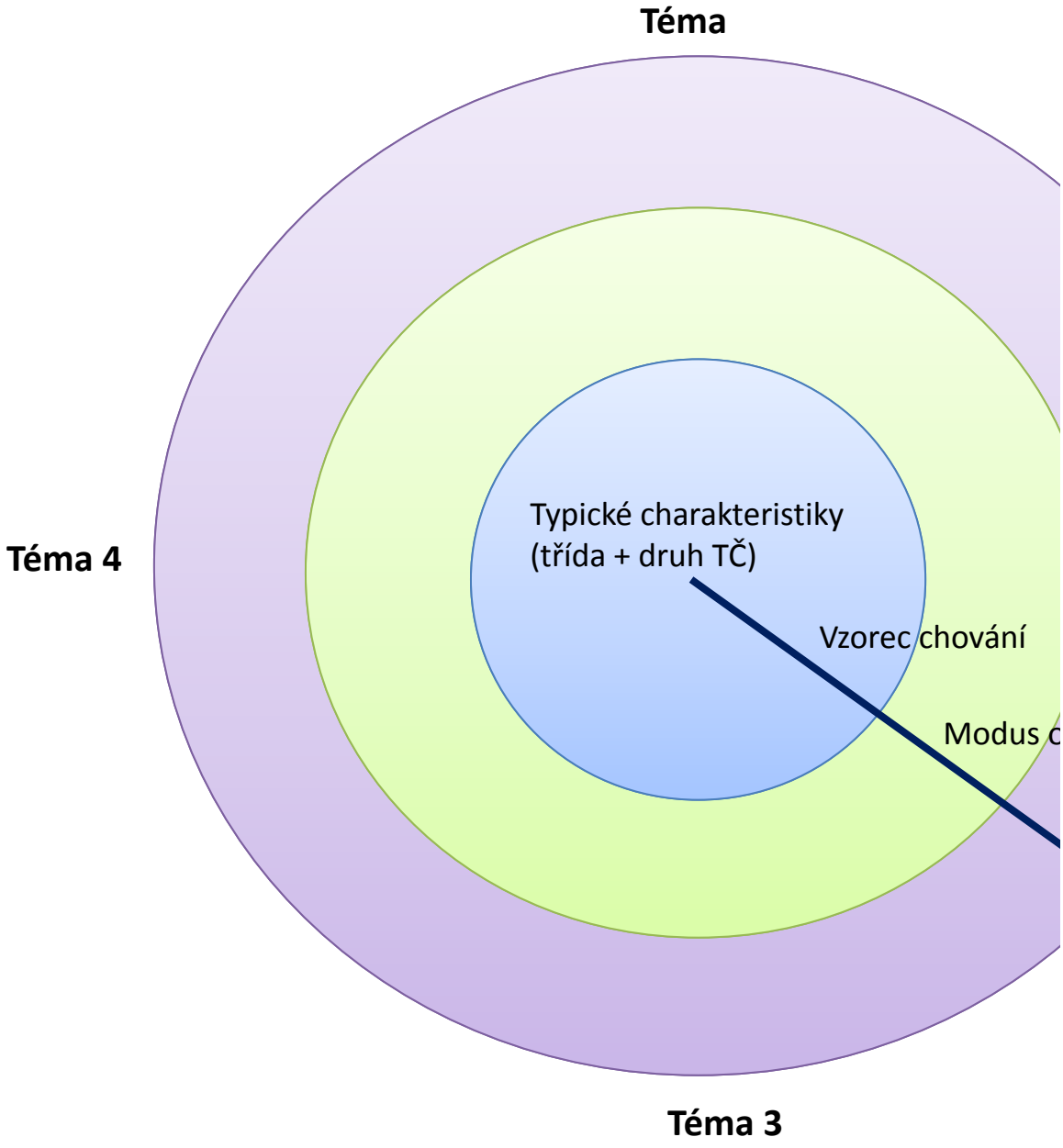
Multidimenzionální přístup vychází ze dvou aspektů trestné činnosti:

- aspekt specifičnosti,
- aspekt tematický.

Aspekt specifičnosti vychází z výše zmíněného postupu definice pachatele. **Na počátku jsou typické společné znaky pro pachatele trestných činů, na kanci pak specifické znaky pro daného pachatele** (kriminální podpis).

Aspekt tematický vychází z **jednotlivých kriminálních podpisů pachatelů trestných činů**. Propojením těchto dvou aspektů a přenesením do grafického znázornění získáme takzvaný radexový model, který poprvé popsal v roce 1954 Louis Gutman.

Radexový model je možno využít pro analýzu multidimenzionálního škálování (MDS), která je statistickou metodou pro získání tématu kriminálního chování, frekvence a vazby k dalším trestným činům, nebo pro analýzu SSA (Smallest Space Analysis – analýza nejmenšího prostoru), která vyjadřuje vztahy mezi proměnnými vyjádřením v geometrickém prostoru.



Obrázek č.47: Radexový model

5.3 BIOSIGNÁLY

Aby bylo možné exaktně měřit **míru reakce člověka na vnější podněty**, lze využít takzvané **fyziologické funkce a jejich biosignály**. Tyto signály jsou proměnné v čase dle míry působení vnějšího podnětu a citlivosti daného jednice na daný podnět. Různí lidé reagují na stejný podnět rozdílným způsobem.

Biosignály je možno rozdělit na typy podle původu či vzniku:

- elektrické,
- impedanční,
- magnetické,
- akustické,
- chemické,
- mechanické,
- optické,
- tepelné,
- radiologické,
- ultrazvukové.

5.3.1 Elektrické biosignály

Generují nervové a svalové buňky jako výsledek elektrochemických procesů. Při působení stimulu přesahující prahovou hodnotu buňky je generován akční potenciál (tok iontů), který lze změřit například mikroelektrodami. Potenciál je předáván okolními buňkami a umožňuje vytvářit elektrické pole v tkáni, které je měřitelné na povrchu těla.

5.3.2 Impedanční biosignály

Lze měřit aplikacemi elektrického proudu o nízkých hodnotách proudů (mikro až miliampéry) do lidského těla. Z vypočítaného odporu lze poté určit nervovou a endokrinní aktivitu, objem krve, nebo skladbu tkání.

5.3.3 Magnetické biosignály

Jsou generovány orgány, jako například mozek či srdce a vypovídají o aktivitě těchto tkání. Přesné měření generovaných magnetických polí je však v současnosti velmi obtížné vzhledem k nízkým hodnotám ve srovnání s geomagnetickým polem Země.

5.3.4 Akustické biosignály

Jsou generovány například průtokem krve srdečními chlopněmi a cévami, průtokem vzduchu dýchacími cestami, zažívacím ústrojím nebo klouby. Měření těchto signálu probíhá prostřednictvím mikrofonů a vypovídá o funkci zkoumaných orgánů.

5.3.5 Chemické biosignály

Bývají reprezentovány stanovením koncentrací iontů v buňkách prostřednictvím speciálních elektrod, stanovením parciálních tlaků plynů a měřením hodnoty pH. Získané hodnoty vypovídají o stavu zkoumané tkáně.

5.3.6 Mechanické biosignály

Jsou odvozeny z mechanického pohybu nebo průtoku. Prostřednictvím mechanických mikrosnímků lze změřit například tlak krve.

5.3.7 Optickými biosignály

Se rozumí změna optických vlastností organismu. Například okysličení krve lze měřit na základě intenzity odraženého světla (dle vlnových délek) od tkáně nebo užívání abiotických tekutin (barvící tekutiny) při získávání informací o plodu.

5.3.8 Tepelné biosignály

Vypovídají o stavu fyzikálních a biochemických procesů v organismu a jejich rozložení po těle je různé. Měření je možno provádět kontaktním způsobem klasickými teploměry nebo bezkontaktně například termokamerou.

5.4 Radiologické biosignály

Lze využít pro získání informací o vnitřních anatomických strukturách. Vznikají reakcí ionizujícího záření s buňkami organismu.

5.4.1 Ultrazvukové biosignály

Vznikají interakcí ultrazvuku s buňkami (tkáněmi) a umožňují získání informací o velikosti objektu a charakteru pohybu. Měření probíhá piezoelektrickými senzory.

V oboru typování a profilace osob lze při současném stavu poznání využívat především informace o tělesné teplotě, srdeční frekvenci, frekvenci dechu, impedanci a mechanických pohybech v souvislosti s vystavením specifickým podnětů a měřením míry reakce.

5.4.2 Tělesná teplota

Tělesná teplota vyjadřuje rovnováhu mezi vyráběným teplem, které produkuje organismus (např. prostřednictvím metabolických přeměn) a jejím výdejem a ztrátami.

Ovlivňují ji následující faktory:

- věk,
- denní doba,
- tělesná aktivita,
- hormony,
- psychický stav (stres),
- vlivy okolního prostředí (podněty).

Z pohledu typování a profilace potenciálních pachatelů hraje důležitou roli **změna tělesné teploty v reakci na uměle vytvořený podnět, kterým je osoba testována**.

5.4.3 Srdeční frekvence

Srdeční frekvence (neboli tepová frekvence) **vyjadřuje počet srdečních pulzů za jednotku čas** (1 minutu). U zdravého dospělého člověka se tato hodnota pohybuje v intervalu **od 70 do 80 pulzů za minutu**.

Srdeční frekvenci ovlivňují následující faktory:

- věk,
- pohlaví,
- tělesná teplota,
- kondice,
- přítomnost krvácení,
- stres (psychický stav),
- podněty z okolního prostředí.

Z bezpečnostního hlediska jsou důležité **změny vyvolané reakcí na podněty z vnějšího prostředí a přítomnost stresu, které reflektují**

nestandardní stav osoby – zvýšená srdeční frekvence. Příkladným využitím může být promítnutí obrazového vjemu (nebo akustický vjem) posuzované osobě s následným bezkontaktním změřením změny srdeční frekvence (reakce na podnět). Bezkontaktní měření srdeční frekvence umožňuje například metoda **balistografie**, kterou lze aplikovat i přes oděv, nebo měření prostřednictvím infračervené kamery. Další možnou metodou měření je snímání intenzity pohlcování zeleného světla hemoglobinem v krvi. K měření lze také využít princip snímání elektrického potenciálu vygenerovaného elektrickou aktivitou srdeční tkáně.

5.4.4 Frekvence dýchání

Frekvence dýchání **vyjadřuje počet nádechů a výdechů za jednotku času** (1 minutu). U zdravého dospělého člověka se hodnota pohybuje v rozmezí mezi **14 až 20 nádechy a výdechy za minutu**.

Frekvenci dýchání ovlivňují tyto faktory:

- věk,
- pohyb,
- stres (psychický stav),
- podněty z okolního prostředí,
- nadmořská výška,
- životní styl.

Z bezpečnostního hlediska při typovaní a profilování osob hraje roli především **změna frekvence dýchání vyvolaná vnějšími podněty nebo z důvodu stresových faktorů (psychický stav) jedince**. Stejně jako v případě srdeční frekvence a tělesné teploty lze využít měření změn frekvence dýchání v reakci na vnější podněty, případně využít naměřených nestandardních hodnot z důvodu psychického stavu jedince.

Bezkontaktní měření frekvence dechu umožňuje například metoda **bioradiolokace**, která využívá odrazu rádiových vln v relaci s pohyby lidského těla při dýchání.

5.5 Inovativní metody profilace na letištích

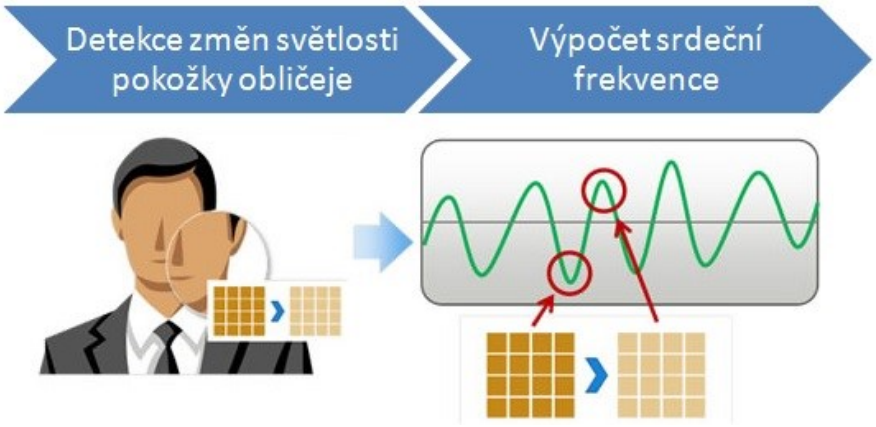
Současný stav zajištění ochrany civilního letectví před protiprávními činy vypovídá o skutečnosti, že již není možné spoléhat výhradně na klasickou bezpečnostní kontrolu na letištích. Postupy teroristů a jiných pachatelů s cílem páchání protiprávního činu proti civilnímu letectví jsou stále propracovanější. Na základě této skutečnosti je využíváno stále větší množství metod, s cílem zajistit snížení pravděpodobnosti spáchání takovýchto činů.

5.5.1 Real-Time Pulse Monitor

Společnost Fujitsu Laboratories vyvinula a v březnu roku 2013 publikovala technologii pro **měření srdeční frekvence osob v reálném čase** (Real Time Pulse Monitor – RTPM). **Systém je založen na detekci změn světlosti obličeje způsobených průtokem krve**. Měření vyhodnocuje pohlcování zeleného světla hemoglobinem, který je součástí krve. Systém snímá videosekvenci daného subjektu a následně propočítává průměrné hodnoty barevných složek (RGB – červená/zelená/modrá) v oblasti obličeje pro každý snímek sekvence. V dalším kroku odstraní irelevantní data pro výpočet ze všech tří barevných složek a extrahuje křivku jasu zelené složky. Tepová frekvence se poté vypočte na základě amplitud průběhu křivky jasu zelené složky (viz Obrázek č. 48).

Systém dokáže automaticky rozpoznat data, která jsou ovlivněna pohyby obličeje či celého těla (pohyby hlavou, mluvení, chůze) a automaticky

tato data eliminuje z výpočtů. Proces probíhá zcela bezkontaktně s danou osobou. Kompletní procedura trvá přibližně 5 sekund.



Obrázek č.48: Grafické znázornění průběhu analýzy RTPM

Technologie je zajímavá především svou jednoduchostí, jelikož pro snímání obrazu lze využít standardní digitální kamery (například integrovanou kameru v mobilním telefonu nebo notebooku). Pro účely profilování osob je zapotřebí výstupy systému zpracovat vhodným analytickým SW, který dokáže vyhodnotit změny srdeční frekvence na základě vnějších podnětů. Široký potenciál využití lze předpokládat od aplikací ve zdravotnictví až po bezpečnostní aplikace. V bezpečnosti lze tento systém využít nejen pro vyhledávání osob s podezřelým chováním, ale i jedinců ve špatném zdravotním stavu, kteří by mohli představovat riziko pro ostatní cestující. První praktické aplikace systému by se měly začít instalovat v průběhu roku 2013.

5.5.2 Systém WeCU

WeCU Technologies je Izraelská společnost, zabývající se výzkumem a vývojem technologií pro „čtení mysli“ pro účely detekce potenciálních teroristů na letištích. Systém WeCU vznikl z důvodu obnovení teroristických útoků v Izraeli v roce 2002.

Metoda je založena na **hodnocení reakcí osob na specifické obrazové**

vjemy ve spojení s potenciální hrozbou. Systém dokáže snímat fyziologické signály lidského těla, jako teplotu těla, srdeční frekvenci a rychlé oční pohyby a vyhodnocovat jejich změny na základě vnějších podnětů. Detekce je časově nenáročná, postačuje přibližně dvacet až třicet sekund, a pro dotčenou osobu je tento proces nezpozorovatelný.

Technologie zahrnuje promítnutí infračerveného podprahového obrazového vjemu, který by rozpoznal pouze terorista (symbol teroristické organizace, obrázek výbušniny, atd.). Celý princip fungování je založen na **faktu**, že **lidé vždy reagují na jim dobře známý obrazový vjem, pokud ho spatří na neobvyklém místě**. Například pokud člověk nečekaně spatří obraz své matky na obrazovce, jeho tvář a tělo na tuto skutečnost zareagují. Pro účely detekce teroristů jsou reakce lidí vyhodnocovány bezpečnostním personálem, ale také skrytými kamerami a senzory, které jsou schopny detekovat mírný nárůst tělesné teploty, srdeční frekvence a pohyby očí.

Databáze promítaných obrázků je velmi rozsáhlá a rozmanitá, a také výběr míst pro promítání musí být různorodý, aby bylo možné v co nejvyšší míře eliminovat připravenost teroristů na přítomnost tohoto systému. Dokonce trénovaní teroristé dle prozatímního výzkumu společnosti nedokázali ovládat svá těla do té míry, aby změny jejich fyziologických parametrů systém nedokázal detekovat.

Metoda fungování je založena na principu propojení detekčních elektrických senzorů se znalostmi získanými z behaviorálních studií. Během rutinních činností na letišti, jako je například Check-in u automatického letištního kiosku je cestující podrobován téměř neviditelnému stimulu, který ihned spouští fyziologické reakce těch osob, které skrývají svůj úmysl. Senzory umístěné v tomto kiosku

snímají reakce dotyčné osoby a upozorňují bezpečnostní personál. Systém také dokáže rozlišit pouze vystresovanou osobu.

Princip fungování (viz Obrázek č. 49)**:**

1. Systém senzorů je založen na měření srdeční frekvence, tělesné teploty a frekvence dýchání cestujícího.
2. Systém vystavuje osobu nenápadným podnětům. Jako příklad lze uvést situaci, kdy je u check-in kiosku uživatel vyzván „Zadejte jméno“ ale krátce se objeví příkaz „Zadejte skutečné jméno“ („Enter name“ -> „Enter real name“). Většina cestujících by na tento podnět neměla reagovat s výjimkou těch, kteří skrývají svou pravou identitu.
3. Senzor měří pohyby očí a zaznamená jakékoli zrychlení pohybu nebo mrkání v reakci na podněty.
4. Infračervená kamera měří teplotu cév, shromažďuje údaje o teplotě a srdeční frekvenci. Tato data pak porovnává s referenční hodnotou.
5. Systém upozorňuje bezpečnostní personál prostřednictvím blikajících světel. Zelená barva signalizuje normální stav, červená označuje zareagování na podněty, oranžová nejednoznačné vyhodnocení reakcí.

Obrázek č. 49: Lidské tělo s vyznačením snímaných fyziologických parametrů systémem WeCU

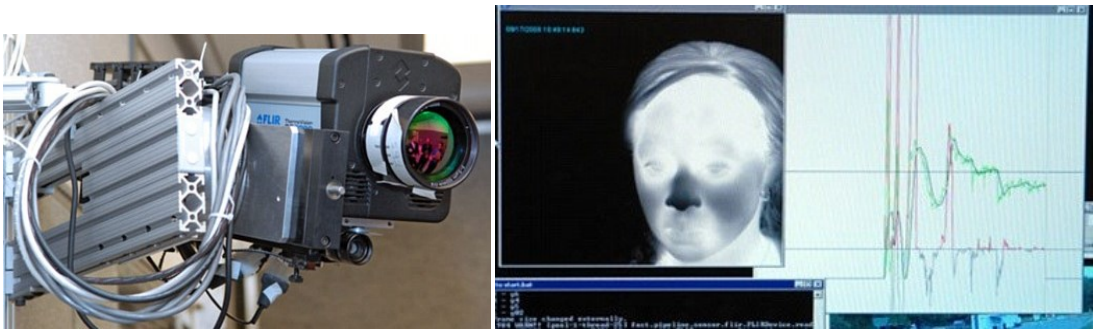
WeCU je pouze detekční systém, nikoli detektor lži, či celotělový skener. Jeho funkcí je pouze označení podezřelých cestujících na základě jejich fyziologických projevů. Ve vztahu k ochraně osobních údajů výrobce uvádí, že systém neuchovává žádná personální data. Systém nelze vnímat jako diskriminační, jelikož nedochází k profilování podle jména, rasy, národnosti, náboženství, oděvu, atd. Účelem je zajistit bezpečnější leteckou dopravu.

5.5.3 MALINTENT

Jedná se o technologický systém pro detekci potenciálně podezřelých

osob z terorismu, který byl vyvinut ministerstvem vnitra Spojených států. Umožňuje na dálku detekovat stav mysli člověka a jeho případný „špatný“ úmysl prostřednictvím senzorů. **Systém snímá tělesnou teplotu, srdeční frekvenci, frekvenci dýchání, tělesný pach a nonverbální projevy (mimika obličeje, pohyby těla)**. Využívá se velké množství snímačů pro detekci a analýzu lidské mimiky s následným vyhodnocením potenciálu páchání trestné činnosti. Systém může obsahovat také senzory pro analýzu pohybu osoby, oční skener a senzor feromonů. Celá procedura trvá maximálně v řádu jednotek minut

Při vývoji byl kladen důraz také na rozeznání vystresovaného jedince od osoby s úmyslem páchání trestného činu. Skenovaná osoba není schopna rozeznat proces snímání. V případě vyhodnocení poplachu je tato informace předána bezpečnostnímu personálu, který rozhodne, zdali bude osoba podrobena dalšímu posouzení (například metoda dotazování).



Obrázek č. 50: Příklad užití termokamery pro MALINTENT

5.5.4 Videoanalýza

Moderním prostředkem pro zajištění bezpečnosti s omezením vlivu lidského faktoru a úsporou nákladů na provoz je využití inteligentní videoanalýzy kamerového záběru. IP kamery disponují digitálním

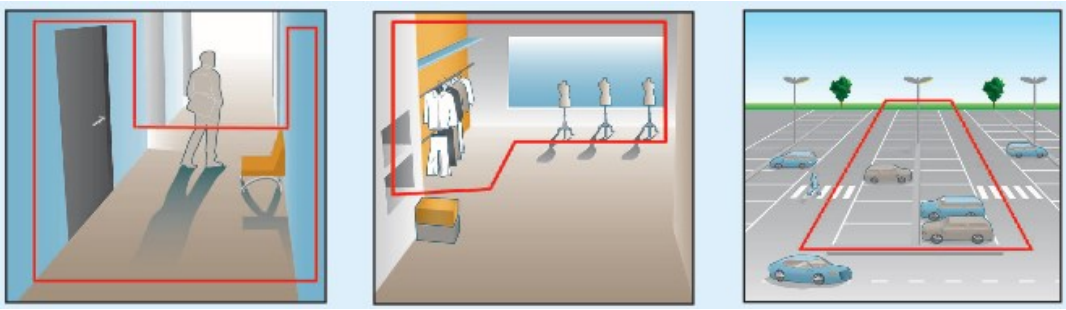
obrazovým výstupem, který je možné prostřednictvím analytického software zpracovávat a vyhodnocovat. Poté je obsluze systému nebo PCO (pult centralizované ochrany) poskytnuta informace o překročení prahové hodnoty a ta má možnost provést další opatření. Sofistikovanější systémy dovolují automatizaci reakce na vyvolaný poplach například spuštěním mechanických zábranných prostředků, elektrické požární signalizace atd.

Pro potřeby zajištění ochrany civilního letectví před protiprávními činy lze využít následující funkce videoanalýzy:

- zónování monitorovaného prostoru,
- vzdálený monitoring předmětů,
- počítání osob,
- heat mapping.

- **Zónováním monitorovaného prostoru**

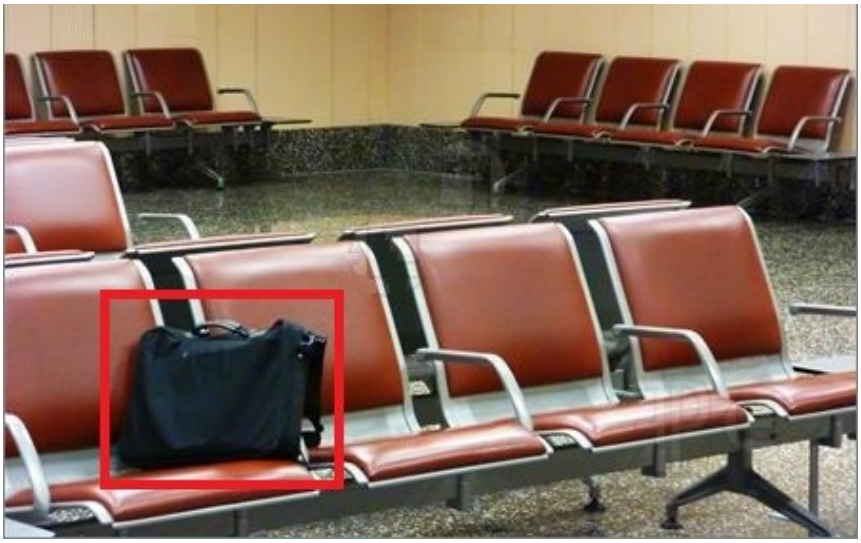
SW (dále jen softwarové) rozdělení obrazu kamerové jednotky na oblasti. **Jakmile dojde ke vstupu osoby do střežené zóny, kamerový systém vyvolá poplach** a dále je postupováno dle nastavených opatření (upozornění na lokální dispečink nebo PCO s online přenosem obrazu, upozornění na mobilní telefon vybrané osoby, atd.). Pro realizaci popsané funkcionality je zapotřebí zvolit vhodnou kombinaci hardware a software, která toto umožňuje.



Obrázek č. 51: Příklad zónování monitorovaného prostoru

- **Vzdálený monitoring předmětů**

Lze využít ve dvou rovinách. První možností je **střežení vybraného předmětu** umístěného v obrazu kamerové jednotky s aplikovanou videoanalýzou. **Jakmile dojde k odstranění nebo přemístění předmětu ze záběru, kamerový systém tuto změnu detekuje a vyhlásí poplachový stav**. Druhou možností z pohledu zajištění bezpečnosti letiště daleko zajímavější je **detekce ponechaného předmětu v prostoru monitorovaném kamerovým systémem**. Systém umožňuje rozpoznat **změnu obrazu vzhledem k původním parametrům** a zároveň eliminovat dynamické vlivy (průchod osob se zavazadly). Tuto vlastnost lze využít například pro detekci umístěná nástražného výbušného systému (NVS) do monitorovaného prostoru s následným informováním bezpečnostního personálu.



Obrázek č. 52: Příklad realizace analýzy odložení předmětu

- **Počítání osob** (neboli people counting)

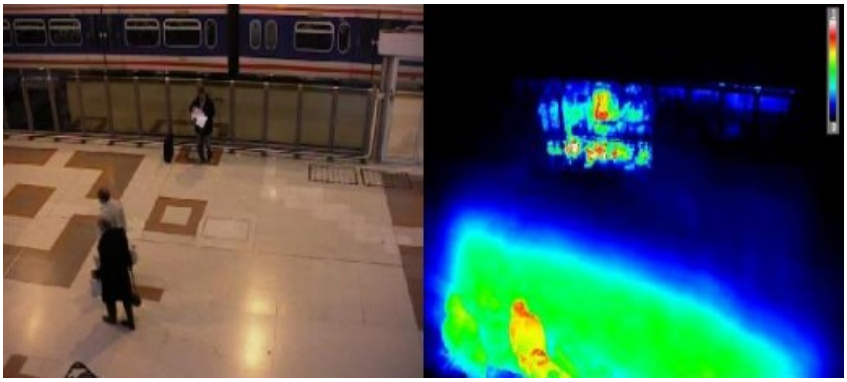
Lze zajistit prostřednictvím **aplikace úsečky (úseček) do zorného pole kamerové jednotky**, a pokud dojde k jejímu překročení (v nastaveném směru, možno i oběma směry), je tato informace zaznamenána. Problém nastává při aplikaci na větší skupinu osob, kdy systém není schopen stoprocentně rozeznat veškeré pohybující se objekty. Počítání osob lze využít pro sledování prostor s omezeným pohybem nebo pro zjištění počtu osob v daném úseku v případě evakuace, kdy je možno porovnat počet osob, které vstoupily do objektu s počtem osob, které ho opustily, a vyhodnotit rozdíl.

Obrázek č. 53: Příklad výstupu videoanalýzy počítání osob

- Funkce **heat mapping**

Byla původně vyvinuta pro marketingové účely. Prostřednictvím propojení IP kamer a analytického software umožňuje **grafické znázornění pohybu osob po monitorované scéně a grafické odlišení prostor scény dle hustoty pohybu**. V marketingu je tato funkce

využívána pro efektivní rozmístění reklamy a zboží. Využití v oblasti bezpečnosti lze uplatnit při profilování osob v případě analýzy nestandardního pohybu jedince po monitorované scéně, včetně analýzy trajektorie pohybu.



Obrázek č. 54: Výstup analýzy heat mapping

5.5.5 Analýza hlasu

Jednou z moderních technických metod pro zajištění bezpečnosti je také technologie analýzy hlasu, kterou vyvíjí například izraelská společnost Nemesysco, která se zabývá výzkumem a vývojem technologií pro analýzu hlasu za účelem odhalování emocí, předcházení podvodům, zvládání stresu a jiné. Nezaobírá se analýzou obsahu řeči, ale prvků a abnormalit toku lidské řeči, které jsou charakteristické pro různé situace, proto není závislá na jazyku, kterým posuzovaná osoba hovoří.

Technologie funguje na principu přednastaveného **setu vokálních parametrů definovaných výzkumem v korelaci s klíčovými lidskými emocemi v různých kombinacích**, aby byla schopna odhalit podvodné úmysly v běžných situacích. Mnoho z posuzovaných parametrů je přitom ve světě fonetiky nových a zaměřených na prozatím neobjasněné vlastnosti lidského hlasu. Analýza může být provedena v reálném čase na uskutečněném hovoru nebo telefonátu, ale také na nahraném vokálním materiálu. Technologie není

detektorem lži.

Používanou analýzou je takzvaná LVA (Layered Voice Analysis), neboli vrstvená analýza hlasu. Užívána je například při bezpečnostních kontrolách, kontrolách vstupu, sběru informací nebo zákonném odposlouchávání. Technologie je schopna zachytit emoční křivky v lidském hlasu, čímž lze analyzovat duševní stav a emoční rozpoložení posuzované osoby.

Identifikované jevy:

- různé typy stresu,
- nadšení,
- zamyšlení,
- zmatenost,
- kognitivní (myšlenkové, rozumové) procesy,
- emocionální reakce,
- atd.

} specifické vlastnosti lidského hlasu

Detekované jevy jsou matematicky vyhodnocovány a přiřazeny emočním stavům. Z těchto informací je možno získat náhled na myšlenkové pochody pachatele, příčiny jeho trápení, nadšení, nejistoty v projevu, témata přitahující jeho pozornost, citlivá témata, atd.

5.5.6 Metoda vedení pohovoru

Důležitou součástí profilace pachatelů je metoda vedení pohovoru (neboli „Questioning“) s již vytipovaným subjektem. **Úspěšnost metody**

závisí především na osobě, která pohovor provádí. Vzhledem k velké závislosti pouze na lidském faktoru nelze vyloučit chyby této metody. Pozitivní dopad hraje mimo jiné preventivní účinek metody.

Úspěšnost metody závisí na několika aspektech:

1. Správnost určení hrozby daného letu.
2. Znalost standardního cestujícího daného letu a profilu teroristy.
3. Precizní provedení kontroly cestovních dokladů cestujícího.
4. Pozorování cestujícího (chování, vzhled), zavazadel, spolucestujících.
5. Správná technika vedení pohovoru.

Otázky **by měly být kladeny systematicky** dle naučeného scénáře (nikoli nahodile), aby bylo možné co nejefektivněji rozlišit nestandardní reakce, a měly by vycházet z informací získaných prvotním pozorováním a kontrolou cestovních dokladů. Pro ověření pravdivosti odpovědí je možné otázku v jiné fázi rozhovoru znovu zopakovat pro ověření pravdivosti odpovědi.

Využívají se čtyři základní typy otázek:

1. Kontrolní otázky
2. Neutrální otázky
3. Relevantní otázky
4. Symptomatické otázky

Kontrolní otázky jsou pokládány z důvodu ověření výpovědi metodou, kdy **osobu přivedeme cíleně ke lživé odpovědi, abychom mohli porovnat reakci při pravdivé a lživé výpovědi** (například otázka: „Lhal jste někdy partnerovi?“).

Neutrální otázky umožňují navrátit posuzovanou osobu do neutrálního fyziologického stavu, pokud předtím reagovala na jiný podnět. Tento postup je aplikován z důvodu potřeby **zvýraznění rozdílů mezi reakcemi na relevantní otázky**. Stejný typ otázky může vyvolávat u různých osob různé reakce, proto je zapotřebí ptát se systematicky.

Relevantní otázky jsou cíleny k jádru problému a jejich úkolem je vyvolat fyziologickou reakci doprovázenou registrovatelným projevem. U posuzované osoby mohou navíc vyvolat pocit podezření kontrolní osoby s možností zmaření plánů. Příkladem může být otázka: „Jste terorista?“

Symptomatické otázky se užívají pro zjištění nepřirozených reakcí posuzované osoby. Následná reakce se porovnává s reakcí na relevantní otázku. Příkladem otázky může být: „*Je něco v nepořádku?“*

Porovnávají se nejen reakce na otázky, ale rovněž projevy nonverbální komunikace. Nejdůležitější jsou **optické a akustické vjemy** kontrolující osoby, proto musí posuzovanou osobu neustále sledovat a poslouchat obsah a formu odpovědí. Kontrolující osoba musí být připravena na tendence kontrolovaného odbočovat od tématu, přehnaně reagovat (přílišná přátelskost nebo naopak neochota ke spolupráci), zastírat úmysly, přehánět, předstírat rozhořčenost, bagatelizovat atd. V odborné literatuře existuje výčet nonverbálních a verbálních projevů rozrušení osob, na které mají pro kontrolující osobu důležitou vypovídající hodnotu.

Vnější projevy rozrušení osob (nonverbální)

- Dává si nohy křížem a brzy se vrací do běžného postoje
- Dotýká se, uhlazuje nebo masíruje jakoukoli část těla
- Hraje si se šperky
- Husí kůže
- Intenzivně se potí (pokud k tomu není příčina prostředí, oblečení nebo činnosti)
- Ježí se mu chlupy na rukou nebo vlasy na zátylku
- Klopí zrak
- Kouše se do rtů
- Křiví ústa
- Mhouří se
- Mne si nos, nebo se jej dotýká
- Mne si ruce nebo prsty
- Mračí se
- Není schopen udržet pohled na jednom místě
- Neudrží chodidla v klidu
- Neudrží paže v klidu
- Neustále přenáší váhu z jedné nohy na druhou
- Neustále si čistí oblečení
- Neustále sleduje hodinky
- Olizuje si rty
- Opakovaně nebo příliš často polyká
- Opakovaně se škrábe
- Otírá si ruce
- Podupává si
- Pohybuje se ztuhle nebo strnule
- Poklepává si na hruď
- Popleskává si rukou o tváři
- Popotahuje ušní lalůčky
- Popotahuje za oděv nebo část těla
- Přehnané pohyby
- Přílišné mrkání
- Pulzující krční tepna
- Rozšířené zorničky (zejména při relevantní otázce)
- Ruce neklidné, neustále v pohybu
- Ruce v oblasti rozkroku
- Sedí na okraji židle
- Sedí si na rukou nebo je jinak ukrývá
- Těká pohledem z místa na místo
- Uhlazuje si nebo upravuje knírek

- Ukazuje na něco jiného (gesto odvedení pozornosti)
- Upravuje a uhlazuje si vlasy
- Věnuje pozornost nehtům
- Viditelně se třese
- Všeobecně neklidný
- Vyhledává kamery v místnosti
- Vyhýbá se pohledu z očí do očí
- Vypoulené oči
- Zakrývá oči
- Zakrývá si oblast hrdla rukama
- Zakrývá si ústa
- Zakrývá si uši
- Založí si paže křížem přes hruď
- Zavírá oči
- Zblednutí
- Zčervenání v obličeji
- Zívání (intenzivní zívání je velmi silným ukazatel

Verbální projevy rozrušení osob (akustické)

- Hluboce vzdychá
- Koktá
- Mluví váhavě
- Není schopen odpovědět
- Neodpoví na položenou otázku
- Neustále vás žádá o bližší vysvětlení otázek
- Odpoví na otázku otázkou
- Opakovaně si odkašlává
- Pomlaskává
- Přerývaný hlas
- Skřípe zuby
- Třese se mu hlas
- Váhá s odpovědí
- Zadrhává se v řeči
- Zívá (velmi důležitý znak)
- Zopakuje otázku a opět požádá o zopakování.

5.5.7 BEMOSA

BEMOSA (zkratka anglického Behaviour Modelling for Security in Airports) neboli **Behaviorální modelování pro bezpečnost na letištích** je celoevropský výzkumný projekt zaměřený na zvýšení bezpečnosti na letištích. Projekt je spolufinancován ze zdrojů Evropské unie a na realizaci se podílí experti z oblasti letectví, bezpečnosti, sociálních věd, akademického prostředí, atd.

BEMOSA vyvíjí behaviorální **SW model, jehož cílem je popsat, jak lidé realizují rozhodnutí v bezpečnostních otázkách za standardních podmínek nebo při krizových situacích**. Hlavním cílem projektu je zvýšení bezpečnosti na letištích a optimalizace nákladů.

Součástí projektu je vývoj školení letištního personálu, které je zaměřeno na přípravu těchto osob pro případy potřeby důležitých a citlivých rozhodnutí. Hlavním cílem školení je snížení počtu planých poplachů a zlepšení bezpečnosti a koordinace v případech ohrožení bezpečnosti.

BEMOSA provedl hloubkovou studii různých evropských letišť s cílem získat data o postupu při zvládání bezpečnostních hrozeb. Výsledky byly posléze porovnány se standardními postupy. Kvalitativní a kvantitativní data pro studii byla získána prostřednictvím pozorování, rozhovorů a dotazníkového průzkumu. Do výzkumu byli zahrnuti zejména zaměstnance letiště a bezpečnostní personál. Získané výsledky tvoří základ modelu chování projektu BEMOSA.

Na základě všech těchto dat bude vytvořen počítačový program pro dynamické modelování sociálního chování a přijímání opatření proti hrozbám na letišti. SW poskytne modelování chování ve stresových situacích a bude sloužit jako tréninková platforma bezpečnostního a

letištního personálu. Vše je směřováno k modelování rozhodnutí k udržení bezpečnostní úrovně letiště.

5.5.8 Systém řízení bezpečnostních pracovníků

Systém řízení bezpečnostních pracovníků (neboli Guard management system) umožňuje efektivně a dynamicky reagovat na poplachové stavy systémů technické ochrany v případě potřeby zásahu bezpečnostního personálu letiště. **Monitoruje polohu a stav jednotlivých bezpečnostních pracovníků a případě vzniku mimořádné události umožňuje dispečerovi zvolit bezpečnostního pracovníka, který je nejblíže místu poplachu a má možnost zasáhnout**. Systém je založen na principu přenosných zařízení s integrovaným mobilním telefonem, GPS, tísňovým tlačítkem, fotoaparátem, atd. (například v provedení PDA), kterými disponují bezpečnostní pracovníci. Toto zařízení umožňuje příjem poplachového stavu ze systému profilace v dané lokaci.

Shrnutí

Civilní letectví představuje moderní způsob přepravy osob i zboží. Denně se tímto způsobem přepraví několik miliónů osob. S rostoucími potřebami lidské civilizace je kladen stále větší důraz mimo jiné na rychlost, kvalitu a bezpečnost přepravy. V současné době již není možné spoléhat se při zajištění bezpečnosti civilního letectví pouze na standardní bezpečnostní kontroly realizované bezpečnostními pracovníky, jelikož metody pachatelů protiprávních činů jsou stále sofistikovanější. Jednou z možností pro zajištění preventivní ochrany před pachateli protiprávních činů je metoda profilace a typování podezřelých osob s využitím moderních biometrických metod.

Otázky

1. Jaké kroky by se měli učinit, pokud budeme chtít využít metody profilace k ochraně prostoru letiště?
2. Z čeho vychází profilace pachatele dle FBI?
3. Jaké aspekty se využívají při aplikaci multidimenzionálního přístupu?
4. Co to jsou biosignály?
5. Kde se využívá metoda bioradiolokace?
6. Jak se nazývá bezpečnostní systém, který "umí" číst myšlenky?
7. Jaké faktory ovlivňují úspěšnost Metody vedení pohovoru?

Test

a) Co lze identifikovat pomocí metody profilace?

b) Jaký výstup přináší profilování pachatelů trestné činnosti prostřednictvím Liverpoolské školy?

c) Co je to radexový model?

d) Vyjmenujte alespoň 5 druhů biosignálů?

e) Jakým bezkontaktním měřením lze provést měření srdeční funkce?

f) Co vyhodnocuje systém RTPM?

g) Na jakém principu funguje technologie pro analýzu hlasu?

Správná odpověď

a) Pomocí profilace jsme schopni identifikovat nestandardní fyziologické projevy a chování u posuzovaných osob

b) Vypracovává vzorce chování pachatelů určitých druhů trestných činů

c) Propojení aspektu specifičnosti a tematického aspektu
d) Druhy biosignálů: elektrické, impedanční, magnetické, akustické, chemické, mechanické, optické, tepelné, radiologické, ultrazvukové
e) Balistografie
f) Měření srdeční frekvence osob v reálném čase
g) Porovnání vokálních parametrů hlasu ve srovnání s lidskými emocemi v různých kombinacích

Přestávka

Gratuluji Ti k nově nabytým informacím z oblasti biometrie a profilace osob a přeji Ti hodně studijních úspěchů. ☺

Literatura

1. BOHÁČEK, P. (2005), *Systémy AFIS a rozpoznávání otisků prstů*, Brno: VÚT Brno - Fakulta Informačních technologií. Semestrální práce, 2005, 10s.
2. BOSH Security Systems [online]. *IP produkty – HW*, 2008 [cit. 21.8.2013]. Dostupný z: http://boschsecuritysystems.cz/produkty.php?sel_skup=178#
3. BROMBA, M. (2007), *BIOIDENTIFICATION* [online]. 2007 [cit. 23.8.2013]. Dostupný z: http://www.bromba.com
4. CONET [online]. *Přístupové systémy*. 2001[cit. 22.8.2013]. Dostupný z: 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 [online], *Center of Excellence*. 1995 [cit. 22.8.2013]. Dostupný z: http://www.fbibiospecs.org/fbibiometric/biospecs.html>.
9. GALBAVÝ, M. (2006), *Vizualizace a vzdálené řízení v síti LonWorks*, Praha: České vysoké učení technické v Praze – Fakulta elektrotechnická. Bakalářská práce, 2006, 61s.
10. JABLOTRON [online]. *Detektory*. 2005 [cit. 23.8.2013]. Dostupný z: http://www.jablotron.cz/ezs.php?pid=products/ja-60p

11. JAIN, A., BOLLE, R., PANKANTI, S. (2002), *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 [cit. 23.8.2013]. Dostupný z: http://www.multlock.cz/cz/kategorie/produkty
13. PETÍK, L. (2008), *Použití biometrické identifikace při zabezpečení objektu*, Ostrava: VŠB TU Ostrava - Fakulta bezpečnostního inženýrství, Bakalářská práce, 2008. 46 s.
14. SANDSTROM, M. (2004), *Liveness Detection in Fingerprint Recognition Systems*. Linkoping, 2004. 149 s.
15. SAPELI [online]. *Dveře a zárubně*. 2006 [cit. 22.8.2013]. Dostupný z: http://www.sapeli.cz/index.asp?obsah=15&amp
16. SOUMAR, C. (2002), *Biometric system security*. In *Secure*. 01/2002. s. 46-49.
17. ŠČUREK, R. (2007), *Přednášky z předmětu Ochrana objektů,* Ostrava: VŠB – TUO, Fakulta bezpečnostního inženýrství, 2007.
18. UHLÁŘ, J. (2001), *Technická ochrana objektů, I. díl, Mechanické zábranné systémy.* Praha: Policejní akademie České republiky v Praze, 2001. ISBN 80-7251-172-6.
19. UHLÁŘ, J. (2001), *Technická ochrana objektů, II. díl, Elektrické zabezpečovací systémy.* Praha: Policejní akademie České republiky v Praze, 2001. ISBN 80-7251-076-2
20. VANĚK, R. (2007), *Technologie digitálního snímání prstů*. Zlín: Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky. Bakalářská práce, 2007, 37s.
21. CARR, J., BROWN M. (2000), *Introduction to biometrical Equipment Technology, Fourth Edition*. New Jersey: Prentice Hall, 2000. ISBN 0-13-010492-2.

22. FUJITSU LABORATORIES LTD. Fujitsu Laboratories Develops Real-Time Pulse Monitor Using Facial Imaging. In: *FUJITSU*[online]. Kawasaki, 2013, 18.3.2013 [cit. 25.8.2013]. Dostupné z: http://www.fujitsu.com/global/news/pr/archives/month/2013/20130318-01.html
23. KARLSSON, M.(2012), *SAFE SECURITY MANAGEMENT SYSTEM: Situation awareness for enhanced security. In: SAAB* [online]. 2012 [cit. 25.8.2013]. Dostupné z: http://www.saabgroup.com/en/Civil-security/Prison-Security/Security-Management-Solutions/SAFE-Security-Management-System/
24. POLIŠENSKÁ, V. (2013), *Profilování pachatelů trestných činů* [online]. 2013 [cit. 25.8.2013]. Dostupné z: http://www.mvcr.cz/clanek/profilovani-pachatelu-trestnych-cinu.aspx
25. ŠČUREK, R., MARŠÁLEK D. (2013). *Profilace cestujících jako bezpečnostní metoda na letištích* [online]. 2013 [cit. 25.8.2013].
26. WeCU Technologies Advances Airport Security [online]. *In: CARMON, Irin. Fast Company*. 2010 [cit. 26.8.2013]. Dostupné z: http://www.fastcompany.com/1659118/wecu-technologies-advances-airport-security
27. NEMESYSCO [online]. *Nemesysco: voice analysis technologies*. 2012 [cit. 26.8.2013]. Dostupné z: http://www.nemesysco.com/
28. BEMOSA [online]. *Bemosa: Behaviour Mdelling for Security in Airports*. 2012 [cit.26.8.2013]. Dostupné z: http://www.bemosa.eu
29. VYTEJČKOVÁ. *Sledování a hodnocení fyziologických funkcí*. [online]. 2013 [cit. 25.8.2013]. Dostupné z: http://www.lf3.cuni.cz/opencms/export/sites/www.lf3.cuni.cz/cs/prac

oviste/osetrovatelstvi/vyuka/studijni-materialy/CNSKOS1/studijni-materialy/Mxenx_a_hodnocenx_fyziologickxch_funkcx.pdf
30. ANISHCHENKO, L.. D'YACHENKO,A.(2013), *The experiment "BIORASCAN": Remote measurements of breathing parameters* [online]. Mars500 [cit. 26.8.2013]. Dostupné z: http://mars500.imbp.ru/en/520_sci_experiments/520_bioraskan.html
31. HAZELTON, L.(2008), *MailOnline* [online]. 2008 [cit. 26.8.2013]. Dostupné z: http://www.dailymail.co.uk/sciencetech/article-1060972/The-airport-security-scanner-read-mind.html
32. AXIS COMMUNICATIONS [online]. *AXIS Communications*, 2013 [cit. 27.8.2013]. Dostupné z: http://www.axis.com/
33. CHUMCHAL T. (2013), *Zajištění bezpečnosti na letišti pomocí profilace a identifikace osob*, Ostrava: VŠB – TUO, Fakulta bezpečnostního inženýrství, Diplomová práce, 2013.

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA OSTRAVA

Fakulta bezpečnostního inženýrství

Katedra bezpečnostních služeb

Název: **Biometrické technologie – technické prostředky bezpečnostních služeb**

Autor: Ščurek Radomír, docent, Mgr. Ing. Ph.D.

Místo, rok, vydání: Ostrava, 2015, 1. vydání

Počet stran: 115 stran

Vydala: Vysoká škola báňská -Technická univerzita Ostrava

Verze on - line

Neprodejné

Neprošlo jazykovou úpravou

ISBN 978-80-248-3786-4