Počítačově podporované informační technologie v oblasti SBS

Computer-supported information technology in the private security services

Daniela Skýpalová

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Daniela SKÝPALOVÁ**
Osobní číslo:	**A08610**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačově podporované informační technologie v oblasti soukromých bezpečnostních služeb**

Zásady pro vypracování:

1. **Práci zpracujte jako edukační materiál pro potřebu soukromých bezpečnostních služeb.**
2. **Popište změny v souvislosti s užitím informačních technologií.**
3. **Rozveďte technologie podporující identifikaci osob.**
4. **Možnosti nasazení nových identifikačních technologií v praxi.**
5. **Zpracujte kritéria a možnosti použití jednotlivých biometrických metod v praktické činnosti SBS.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Perspektivní bezpečnostní technologie ochrany majetku : mezinárodní bezpečnostní konference : PYROS/ISET 2008 : Brno, 15. května 2008. Ve Zlíně : Univerzita Tomáše Bati, 2008. 1 CD-R s. ISBN 978-80-7318-699-9.**
2. **RAK, Roman; MATYÁŠ, Vašek; ŘÍHA, Zdeněk. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha : Grada, 2008. 631 s. ISBN 978-80-247-2365-5.**
3. **BITTO, Ondřej. Šifrování a biometrika, aneb Tajemné bity a dotyky. Vyd. 1. Kralice na Hané : Computer Media, 2005. 168 s. ISBN 80-86686-48-5.**
4. **MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha : ASPI, 2008. 455 s. ISBN 978-80-7357-322-5.**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.**

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

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce je vypracována jako edukační materiál pro potřebu soukromých bezpečnostních služeb. Je rámcovým pohledem na problematiku začlenění informačních technologií do činnosti SBS a jejich praktické využití. Popisuje současné metody identifikace osob s bližším zaměřením na metody biometrické, proces identifikace, princip činnosti snímačů, vhodnost užití v činnostech SBS k přihlédnutím k limitám metod a odhaduje směr vývoje. Okrajově zmiňuje legislativní náhled a zabezpečení biometrických dat a procesu snímání. Výstupem je SWOT analýza. Práce je doplněna grafickou a fotografickou dokumentací.

Klíčová slova: identifikace, verifikace, biometrie, metody snímání.

ABSTRACT

Thesis is designed as a tutorial material for the use of private security services. At issue is the framework for information technology integration in the activities of the private security services and their practical use. Describes the current methods of identification of persons with a closer focus on biometric identification methods, process, principle of the sensor, the appropriateness of the use of the activities in the activities of the private security services to take account of the thresholds under the direction of the development of methods and estimated. Marginal mentions legislative preview and the security of biometric data and the process of scanning. The output is a SWOT analysis. The work is supplemented by video and photographic documentation.

Keywords: identification, verification, biometrics, the scanning method.

Poděkování patří všem, kteří mi drželi palce a morálně a zejména časově mě podporovali. Zvláštní poděkování patří vedoucímu práce JUDr. Vladislavu Štefkovi za cenné rady a připomínky. A také mým dětem, které mi stále dokazují svou jedinečnost.

„Osobnost je charakterizována nejen tím, co dělá, ale i tím jak to dělá.“

Friedrich Engels

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, 20. května 2011 …….…….

podpis diplomanta

OBSAH

ÚVOD

Soukromé bezpečnostní služby jsou doplňující složkou výkonné moci státu zajišťující ochranu zdraví a majetku právnických i fyzických osob. Tuto svou činnost vykonávají jako podnikání za účelem zisku, jako právnické či fyzické osoby, a to bez zvláštní vyšší pravomoci. Opírají se o právo podnikatelských subjektů na ochranu svého života a majetku, využívají právní možnosti dané ústavou a občanským zákonem, obchodním zákoníkem, živnostenským zákonem a trestním zákonem. Aby mohly tyto služby vykonávat na profesionální úrovni a držely tak krok nejen s konkurencí, ale také se subjekty, které mají svou činností odhalovat, nebo jimž mají v jejich činnosti zamezovat, musí využívat a ovládat aktuální technologie a být obeznámeni s novinkami, trendy a směry vývoje nejen užívaných praktik, ale zejména s využíváním, začleněním a principy stávajících i nových technický a technologických prvků, které jsou dnes součástí počítačových technologií, nebo s počítačovými technologiemi úzce spolupracují. Mezi tyto systémy řadíme i takové, které využívají jedinečné biometrické charakteristiky jedinců.

Tyto systémy jsou schopny bezpečně rozpoznat jedince, a na základě tohoto rozpoznání provézt rozhodnutí. Jsou technickým prvkem vyskytujícím se ve všech oblastech bezpečnostního průmyslu, jako samostatný systém či technická implementace. Těchto systémů může využívat malá i velká firma či státní organizace stejně dobře jako jednotlivý občan. Rozhodujícím faktorem výběru zařízení nebo systému využívající biometrických metod je požadavek zadavatele, jeho nároky, v závislosti na bezpečnostní politiku firmy, stupeň zabezpečení, nebo jen požadavek na zavedení jednoduché, moderní, pohodlné metody přístupu.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ TECHNOLOGIE

Dnes už těžko najdeme obor či činnost člověka, do níž by nové technologické poznatky nezasahovaly. Termín technologie, z řeckého „dovednost“ a „nauka“ či „znalost“, tedy „nauka o dovednosti“ je chápán jako odvětví techniky, které se zabývá tvorbou, zaváděním a zdokonalováním výrobních postupů. V kontextu informace, jako obsahu sdělení, které je možno vysílat, přijímat a uchovávat, chápeme informační technologie jako určité know how jak funguje výpočetní technika. Tohoto názvu je však také užíváno pro jakýkoli elektronický přístroj, schopný s informacemi samostatně pracovat.

1.1 Informační technologie v SBS

Úkolem SBS je ochrana osob a majetku. Na ochranu je nahlíženo jako na soubor opatření, kde o případném zásahu rozhoduje člověk, nikoli technologie. Ta má funkci podpůrnou a indikující. Nové informační technologie konkrétně biometrické systémy jsou technickými prostředky zabezpečovací techniky a jsou v SBS využívány zejména jako přístupové identifikační systémy sloužící k ochraně objektu nebo vymezeného prostoru řízením přístupu nebo střežením prostoru. Technologie může být včleněna do systému ochrany, jako prvek samostatný nebo prvek komunikující se systémem.

1.2 Technická ochrana a její prostředky

SBS můžeme dělit dle oblastí působnosti, nebo dle sektorů poskytujících služeb. Pro potřeby této práce je vhodné ponechat si náhled na bezpečnost a ochranu, jako na opatření, která se vykonávají pomocí prostředků fyzických, technických a režimových. Provázanost a vzájemná podpora těchto opatření zajišťují bezpečnost komplexně. Technické prostředky je možno dále dělit na prostředky klasické ochrany (mechanické zábranné systémy) a technické (poplachové systémy).

Technická ochrana podporuje ochranu klasickou s cílem co nejvíce zdržet, odradit či včas indikovat nebezpeční nebo případného pachatele. Míra ochrany, použitých prostředků a technologií je úměrná chráněnému zájmu, tedy míře rizika a předpokládaným vzniklým škodám.

Technickými prostředky ochrany jsou:

- IAS – poplachové zabezpečovací systémy
- HAS – poplachové tísňové systémy

- SAS – přivolání pomoci
- CCTV – uzavřené televizní okruhy
- ACS – systém kontroly vstupu
- EPS – elektrická požární signalizace

Příklady nasazení biometrických prvků či systémů jsou uvedeny v závěru práce.

1.2.1 Dostupnost technologie

Vývoj nových technologií a jejich zavádění do praxe jde vysokým tempem. Je to dáno snahou o co největší rozšíření, uplatnění a variabilitu technických a technologických prvků s cílem dosáhnout co nejnižší ceny na trhu a tento trh ovládnout, určit základní směr a technologii, následně poskytnou vyšší aplikace a nadstavby komunikující také s jinými systémy a to i z jiných oblastí.

2 BERTILONÁŽ A BIOMETRIE

V boji o lepší místo ve společnosti je snahou každého jedince i skupiny získat nejlepší pozici a tuto pozici si udržet, dobře znát své spolupracovníky a osoby, kterým lze důvěřovat. Nepřátele odhalit, označit nebo dobře včas rozpoznat. K metodám označení nepřátel, odsouzených či zrádců patřilo usekávání částí těl (rukou, prstů, uší, nosu) později označování cejchem - rozpáleným železem či tetováním. Cílem takovéhoto znetvořování bylo buď znemožnění v pokračování nekalé činnosti, nebo jasné označení osoby, se snahou z řádné společnosti ji vyloučit.

2.1 Bertilonáž

Milníkem moderního rozpoznávání osob byla metoda měření Alphonse Bertillona – zakladatele antropometrické metody zjišťování totožnosti na základě měření vybraných tělesných rozměrů, také známé jako bertilonáž, bertilonie či antropometrie. Jeho metoda byla první vědecky podloženou metodou identifikace. Prosazování metody bylo zdlouhavé a obtížné a metoda samotná se nepraktikovala dlouho. Přesto, můžeme Bertillona považovat za zakladatele biometrie. Tedy rozpoznávání jedinců na základě měření jejich fyzických parametrů a dnes i chování. Podobnost je zřejmá zejména u měření veličin ruky, obličeje a ucha.

Antropometrii brzy nahradila daktyloskopie. Konkrétně v Čechách se antropometrie užívala 8 let, do září 1908. Poté bylo prováděno pouze daktyloskopování. Daktyloskopie, tedy rozpoznávání jedinců na základě otisků prstů zvítězila svou jednoduchostí a možností srovnávat zanechané stopy na místě činu s konkrétním jedincem.

2.2 Technologický boom

První zařízení, schopné sejnou a rozpoznat biometrický údaj, porovnat ho a vykonat následnou akci, např. rozpoznat jedince a zamezit mu v přístupu, vzniklo koncem šedesátých let. Lidské zkoumání tedy dospělo až ke vzniku zařízení přijatelných rozměrů, schopné pracovat samostatně dle předem definovaných instrukcí a vykonávat rozhodnutí.

Vývoj počítačové techniky můžeme datovat do doby vzniku prvních počítačů schopných zpracovávat zadané úlohy samostatně. Vznikaly v 30tých létech 20tého století. Jednalo se o počítací stroje jednotného uspořádání vykonávající výpočetní operace. Programovatelné automaty užívané k řízení procesů vznikly koncem let 60tých. Osobní počítač počátkem let

70tých. A příliv osobních počítačů do domácností odstartoval vývoj osobní výpočetní techniky. Počítačový nadšenci začali své přístroje rozšiřovat, propojovat a jinak zkoumat jejich možnosti a hranice a vznikla silná zpětná vazba mezi výrobci a trhem. Internetové sítě vznikaly koncem let 80tých a přelomovým rokem je rok 1991, kdy došlo k nasazení WWW (World wide webu) v evropské laboratoři CERN.

Zpřístupnění nových technologií veřejnosti vždy podstatným způsobem ovlivnilo další vývoj a výzkum. Vyto vývojové vlny vždy souvisely s masovým využíváním nových technologií. Masové využívání jakýchkoli technologií má vždy za následek klesající ceny produktů a tím ještě masovější používání a následné další snižování cen. Tak tomu bylo u zpřístupnění špionážní techniky po skončení studené války, stejně jako u uvedení na trh osobních počítačů, mobilních telefonů a biometrických systémů. Dříve označované strategické technologie rozvíjené na základě státních zakázek pro vojenské a zpravodajské účely za vysokého stupně utajení, dnes může využít kterýkoli občan za přijatelnou cenu. Překonané či všeobecně známé technologie je jednoduše ekonomicky výhodné zpřístupnit veřejnosti, zvýši tím zisk a možná i odhalit nové možnosti použití.

Otevření se světu, propojení technologií šlo ruku v ruce s ochranou dat a rozvojem kryptografie tj. šifrovacích technik, programů a protokolů. Kryptografie hojně využívá algoritmů - matematických operací, návodů a postupů, kterými lze řešit úlohy porovnávající sebrané údaje.

2.3 Změny v kontextu SBS

Zatímco dříve bylo prací detektivních kanceláří a bezpečnostních agentur fyzické sledování a střežení osob či objektů, infiltrování vyzvědačů a kontaktování osob, u nichž byl předpoklad, že utrousí cennou informaci založeno na znalosti konkrétního prostředí a osob. Dnes může být detektivem i zkušený hacker (počítačový pirát). Toto vidění však není tak černobílé, činnosti v bezpečnostním průmyslu jsou činnosti komplexní a bezpečnostní pracovník musí ovládat jednotlivé postupy a techniky, znát co je možné a co už ne, a mít povědomí o znalostech a možnostech protistrany.

3 TECHNOLOGIE PODPORUJÍCÍ IDENTIFIKACI OSOB

Identifikačními technologiemi je myšleno využití technických prostředků pro proces identifikace, jako automatického či automatizovaného procesu, prostřednictvím různých metod nebo jejich kombinací.

3.1 Terminologie

Identifikace – v komerční bezpečnosti je proces, určování totožnosti neznámého jedince za pomoci sejmutého vzorku, tedy naměřených hodnot, porovnávaných se všemi uloženými vzorky (šablonami). Jedná se o režim 1:N, tedy porovnávání jednoho vzorku se všemi ostatními.

Pozitivní identifikace – systém, kdy uživatel dokazuje, že někým je, např. že má povolení k přístupu, vyhodnocuje se shoda s přiloženým vzorkem.

Negativní identifikace – systém, kdy uživatel dokazuje, že někým není, jeho vzorek je systému neznámý (databáze osob mající přístup zamezen).

Verifikace – je proces, při kterém systém potvrzuje totožnost jedince srovnáváním sejmutého vzorku s již dříve zapsaným. Pracuje v režimu 1:1, porovnává sejmutý vzorek s jedním konkrétním, vybraným jiným druhem identifikace.

Autentizace – případně autentifikace či legalizace, je proces rozpoznávání, při kterém je výsledkem určitý statut (oprávněný/neoprávněný).

Biometrie – automatická metoda rozpoznávání subjektu tj. živé osoby na základě jedinečných biologických charakteristik (fyzických parametrů). Tyto charakteristiky jsou v průběhu lidského života neměnné a člověk je svým chováním nemůže ovlivnit.

3.2 Autentizační metody

Identifikace v prostředí SBS je doménou automatizovaného přístupu a odhalování přítomnosti nežádoucích osob ve vymezených prostorách. Mechanismem automatizovaného přístupu je ověřováním identity uživatele, na základě jeho znalosti, vlastnictví předmětu, nebo charakteristice. Podle toho pak rozlišujeme metodu autentizace heslem, předmětem nebo biometrií.

3.2.1 Metoda autentizace heslem

Je založená na znalosti hesla. Heslo je informace jako posloupnost znaků, kterou je nutno zadat do přístupové jednotky. Nevýhodou je riziko detekování speciálními programy, zapomenutí nebo vysledování neoprávněnou osobou, do značné míry je rizikem samotný uživatel, který je nucený pamatovat si celou řadu hesel, a často tak užívá jen jedno pro všechny aplikace. Použití autentizace heslem je však stále nejrozšířenější a používá se přibližně ze 70%.

3.2.2 Metoda autentizace předmětem

Je založená na vlastnictví předmětu – tokenu. Token informaci potřebnou k autentizaci obsahuje. Výhodou i nevýhodou je jeho přenositelnost, často je užíván jen v kombinaci s heslem nebo jako nositel biometrického vzorku uživatele. V praxi jsou užívány tokeny s pamětí jako karty magnetické, elektronické nebo optické, nebo USB tokeny. Poslední jmenované jsou hardwarovým autentizačním prostředkem disponujícím paměťovou oblastí pro úschovu chráněných dat např. šifrovacích klíčů. Jsou chráněny šifrováním a často využívají technologie sdíleného tajemství.

3.2.3 Metoda autentizace biometrií

Je založená na jedinečných biometrických charakteristikách člověka, není nutné pamatovat si několikamístné kombinace hesel či neustále u sebe nosit snadno zcizitelný token. Biometrická autentizace je rychlou, pohodlnou a velice přesnou metodou. Biometrické údaje lze dělit dle různých parametrů či pohledů. Jedním z nich je způsob, jak biometrická vlastnost u člověka vzniká. Hovoříme pak o vlastnosti genotypické, randotypické a behaviorální.

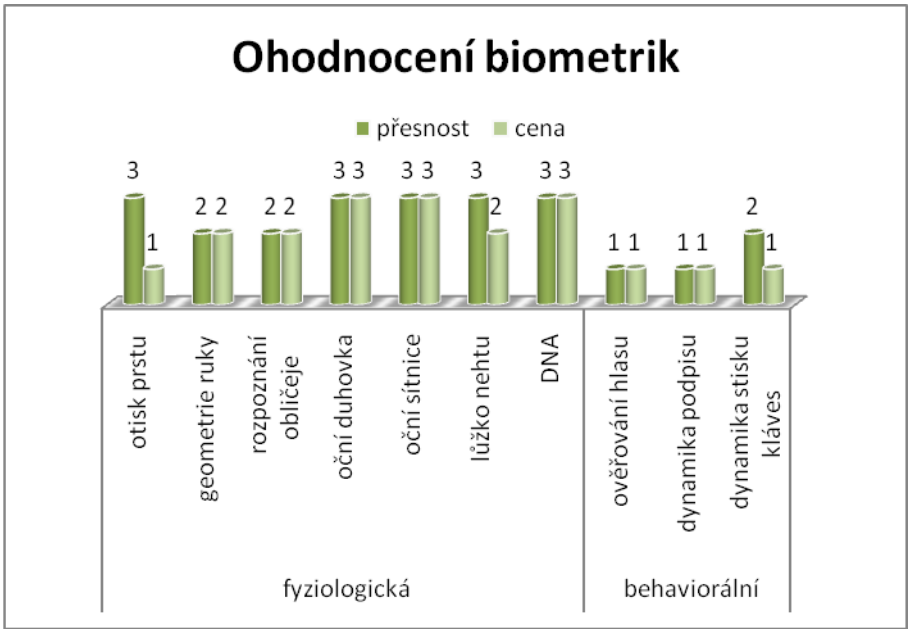
Genotypická vlastnost – vzniká genetickým vývojem, rozhodný vliv má dědičnost (DNA).

Randotypická vlastnost – vzniká v časném stádiu vývoje embrya, náhodně.

Behaviorální vlastnost – vzniká učením a výchovou, je to projev chování jedince. Lze ji do určité míry ovlivnit.

První dvě jmenované vlastnosti můžeme zahrnout společným termínem fyziologické, tedy týkající se fyziologického těla, nikoli projevu či umu, jak je tomu u vlastnosti behaviorální. Je prokázáno, že všechny tři přispívají k vývoji biometrické vlastnosti, i když každá v jiné míře. Tyto hodnoty mají podíl na přesnosti či spolehlivosti metody. Podíl vlivu nebudeme

rozebírat podrobně, ovšem pracovník SBS by měl vědět, že podíl behaviorální vlastnosti, tedy té, kterou lze do určité míry ovlivnit je označován za významný u metody dynamického podpisu či psaní na klávesnici. Poměr přesnosti a ceny základních biometrických zřízení znázorňuje Obr.1. (hodnoty jsou převzaty z [1], hodnota 1 je nízká a 3 vysoká hodnota).



Obr. 1. Ohodnocení biometrik.

U biometrických metod se setkáváme s řadou pojmů:

Biometrický vzorek – odraz fyziologických nebo behaviorálních charakteristik člověka do vnějšího světa. Mohou to být otisky prstu, dlaně, krev, podpis, křivka EKG, EEG a další.

Biometrické charakteristiky (data) – všechny jakýmkoli způsobem měřitelné údaje z biometrického vzorku. Jejich měřitelnost ještě neznamená jejich použitelnost.

Biometrické markanty – ta část biometrických charakteristik, jíž lze efektivně využít pro identifikaci či verifikaci člověka. V biometrickém vzorku je většinou více použitelných markantů, než je pro verifikaci potřebné.

Biometrická šablona – naměřené hodnoty, charakteristiky, funkční závislosti minimálního počtu markantů, které plně postačují pro jednoznačnou identifikaci či verifikaci. Je to konečný výsledek maximálního zúžení vzorku pro účely identifikace či verifikace.

3.3 Proces autentizace

Proces autentizace na základě biometrických údajů probíhá v pěti krocích. Nejprve je však třeba vytvořit databázi, se kterou se budou sejmuté šablony porovnávat. Kroky potřebné k vytvoření databáze, můžeme ztotožnit s kroky autentizace s absencí kroku rozhodovacího.

Kroky procesu autentizace:

- sběr – snímání
- přenos dat
- zpracování naměřeného signálu
- proces rozhodování
- uložení dat

3.3.1 Sběr dat

Sběr dat nebo také snímání charakteristik probíhá buď s vědomím či bez vědomí uživatele, kontaktně či bezkontaktně. Biometrické informace, jsou snímány různými technikami, v podstatě na principu vyhodnocování zaznamenané veličiny (obrazu, zvuku), či měření veličin vyslaných a odražených od subjektu například od přiložené části těla.

Při nebo před snímáním může systém vyžadovat zadání hesla či použití tokenu, mohou také probíhat operace na ochranu před předkládání zfalšovaných záznamů biometrických charakteristik. Jde o mechanizmy detekce živosti snímaného subjektu. Například u snímačů oční duhovky, se systém brání případnému předložení fotografie platného oka tím, že v krátkém čase mění intenzitu přisvícení a sleduje odezvu v oku. Živé oko zareaguje kontrakcí, či expanzí oční pupily. Nasnímaný vzorek je určen k vytvoření šablony.

3.3.2 Přenos dat

Některé aplikace mají oddělená místa snímání a zpracování biometrických charakteristik. Pak je nutné zajistit bezpečný přenos dat. Data jsou přenášená v komprimované podobě (snížení objemu dat) po přenosu jsou opět dekomprimována. Jestliže biometrická aplikace má být otevřená a vyměňovat si údaje s ostatními, pak komprimační, dekomprimační a

přenosové protokoly musí být standardizovány tak, aby každá další aplikace byla schopna rekonstruovat originální biometrický signál (vzorek) [2].

3.3.3 Zpracování naměřeného signálu

Sejmutá biometrická informace není obrazem či měřením jako takovým, je v systému uložena jako odpovídající matematický kód, který vznikl extrakcí unikátních znaků z nasnímaného vzorku. Vzorky (šablony, etalony) reprezentují osoby oprávněné k přístupu. První nasnímání je provedeno několikrát a vybrán je nejkvalitnější vzorek a kvalita a přesnost sejmutých měření je ihned ověřována. Šablona se ukládá na nosiče informací např. čipy, identifikačních karet, do počítačových databází apod. Velikost biometrické šablony uložené na záznamovém nosiči se udává pomocí základní informační jednotky byte. Na základě těchto šablon probíhá vyhodnocování shody. Nasnímaná extrahovaná šablona potřebné kvality je odeslána do porovnávacího procesu k porovnání s již dříve zavedenými šablonami. Porovnávání je procesem identifikace či verifikace.

3.3.4 Proces rozhodování

Při každém přístupu je tedy sejmuta biometrická informace, převedena na matematický kód a porovnána s existující databází a následně vyhodnocena shoda. V procesu rozhodování se stanoví identifikační závěr a vykoná následná akce.

Snímání a vyhodnocování biometrik nepobíhá s absolutní přesností. Nasnímaný vzorek je i pro téhož uživatele principielně při každém snímání trochu odlišný. Biometrický systém pracuje s určitou mírou tolerance nepřesnosti shody mezi referenčním vzorkem a aktuálně nasnímanou charakteristikou a jako platný bere vzorek, jehož míra korelace (porovnání dvou hodnot) překročí určitou prahovou hodnotu s uloženou vzorovou šablonou. Tato míra nepřesnosti má přímou souvislost s jedním z nejdůležitějších parametrů biometrických systémů – FRR a FAR.

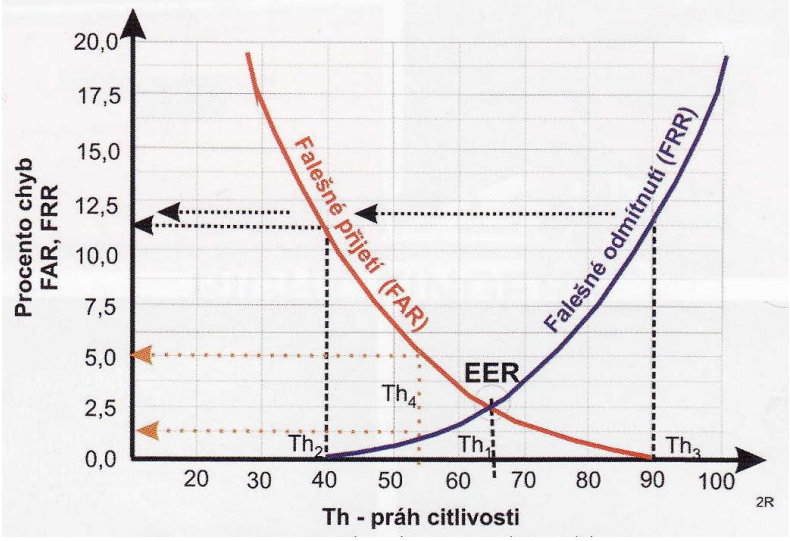
FRR (*False Reject Rate*) označuje míru chybných odmítnutí, pravděpodobnost, že známý vzorek bude vyhodnocen jako neplatný.

FAR (*False Acceptance Rate*) označuje míru chybných přijetí, pravděpodobnost, že neplatný vzorek bude vyhodnocen jako známý.

Některé biometrické systémy, typicky snímače otisků prstů, mohou poměr mezi FRR a RAR měnit dle požadavku uživatele.

K porovnání přesnosti vyhodnocení různých biometrických charakteristik je užíváno údaje **ERR (*Equal Error Rate*)** označující míru rovné chyby, jako průsečík křivek FRR a FAR.

Následující obrázek zobrazují závislost procenta chyb na citlivosti přístroje u reálné aplikace.



Obr. 2. Reálná biometrická aplikace [2].

3.3.5 Uložení dat

V komerčně bezpečnostních aplikacích se neukládají obrazy sejmutých biometrických charakteristik jako takové, ale zpracované markanty v podobě šablon z důvodů minimalizace objemu dat a zvyšování rychlosti zpracování. Šablona je uložena v databázi, která je součástí čtecího zařízení, nebo je uložena vzdáleně v centrální databázi. Nutné je pak zajistit bezpečnou komunikaci mezi zařízeními a ukládání dat v šifrované podobě. Nezajištěna mohou být pouze zařízení považovaná za důvěryhodná. Ukládána je i historie událostí.

3.4 Metody biometrické identifikace

Metody biometrické identifikace pro komerční využití vycházejí převážně z aplikací primárně používaných v kriminalistice v procesu důkazního řízení a odhalování pachatelů. Nepočítáme-li otisky prstů užívané již ve staré Číně, před 9ti tisíci léty, otištěné do hlíny či na dokumenty namísto podpisu. Při důkazním řízení museli průkopníci nových metod

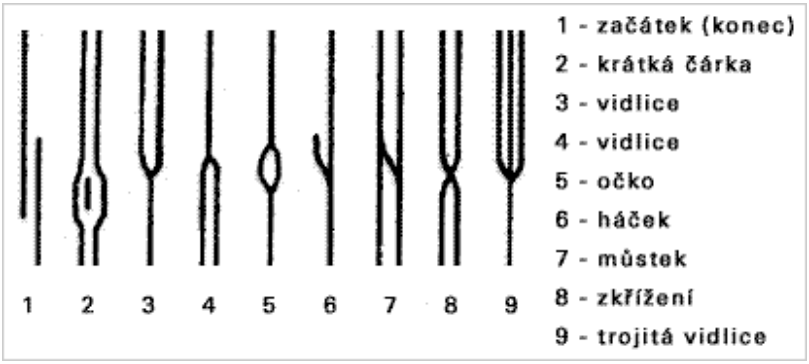
identifikace dokazovat přesnost své metody a ta byla následně prověřena i dějinami. Při sběru dat a stop zanechaných pachateli na místě trestných činů byla zřejmá jedinečnost biometrických stop, a s nasazením výpočetní techniky a potřebných aplikací, nebylo daleko ke komerčnímu využití. Konkrétně historicky první aplikací s využitím biometriky byl přístupový systém na základě biometrie ruky. Počet metod založených na biometrických charakteristikách jistě není konečný, ovšem metody jsou již dostatečně prověřeny svou vhodností pro konkrétní použití s ohledem na přesnost, spolehlivost, cenu či uživatelskou přívětivost, a tak můžeme očekávat maximálně změnu v pořadí v četnosti užívání.

Metody užívané k identifikaci pomocí biometrických charakteristik jsou:

- metoda založená na snímání otisků prstů
- metoda založená na snímání tvaru ruky
- metoda založená na snímání krevního řečiště hřbetu ruky
- metoda založená na snímání tváře
- metoda založená na snímání tvaru ucha
- metoda založená na snímání ručního písma a podpisu
- metoda založená na snímání hlasu a řeči
- metoda založená na snímání oční duhovky
- metoda založená na snímání oční sítnice
- metoda založená na snímání dynamiky stisku počítačových kláves
- metoda založená na snímání lokomoce
- metody založené na jiných charakteristikách

3.4.1 Metoda založená na snímání otisků prstů

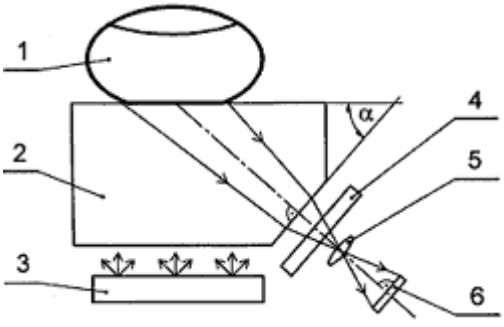
Rozlišování jedinců na základě otisku prstů je založeno na jedinečné kresbě papilárních linií na bříšku prstu, papilární linie je prostorově členitá, linie vystupují na povrch a mezi nimi jdou brázdy, které vytvářejí prostorové prohlubně. Brázdy a linie vytvářejí různé vzory; očka, háčky a můstky. Snímání je založeno právě na plastičnosti povrchu a fyzikálních vlastnostech kůže a na četnosti výskytu vzorů.



Obr. 3. Vzory papilárních linií [3].

Snímače otisků prstů jsou implementovány do nejrůznějších zařízení a jsou realizovány pomocí senzorů. Senzory pracují na různých fyzikálních principech a jsou buď kontaktní (optické, elektronické, opto-elektrické, kapacitní, tlakové, teplotní) nebo bezkontaktní (optické a ultrazvukové). Fyzikální princip a konstrukce snímače se podílejí na vlastnostech konkrétní metody snímání a určují vhodnost použití v konkrétním prostředí.

Senzory optické - jsou nejstaršími používanými senzory. Pracují na technologii FTIR, kdy laserový paprsek zespodu osvětluje snímanou plochu, respektive přiložený povrch prstu, jeho kresbu linií a odražený světelný tok je snímán CCD prvkem. Detekuje se množství odraženého světla dle papilárních linií a brázd. Citlivost CCD prvku je nastavena tak, aby nereagovala na odražené světlo od brázd.



Obr. 4. Optický snímač [4].

1. prst
2. snímací hranol
3. osvětlovací soustava
4. optický filtr

5. snímací objektiv
6. maticový CCD detektor

Optické snímače mohou využívat i jiné technologie než FTIR, například hustý svazek optických vláken postavených kolmo k rovině snímací plochy senzoru. Princip osvitu a odrazu je pak stejný.

Místo CCD prvku je užíváno i technologie CMOS. Jedná se o snímače zpracovávající světlo. Pomocí fotocitlivých buněk na ploše čipu převádějí světlo na elektrické pulzy. Rozdíl je při zpracování dat z čipu. U CCD odchází data z jednotlivých buněk postupně do řídící elektroniky, u CMOS má každá buňky jednoduchý obvod, ten signál zesílí a přenese do procesoru, pro každou buňku samostatně. CMOS je technologie méně náročná na prostor i odběr energie a tím rychlejší a levnější. CCD má lepší rozlišení.

Bezkontaktní metoda snímání otisku prstu snímá otisk ve vzdálenosti 30 až 50 mm. Tento způsob eliminuje znečištění snímacího senzoru dotyky špinavých prstů a ulpívání papilárních linií na povrchu snímače. Optické senzory snímají otisk dvourozměrně tedy 2D a jsou náchylné k použití padělků.

Senzory elektronické – (radiofrekvenční), pracují na principu vzniku elektrického pole mezi dvěma paralelními vodivými a elektricky nabitými deskami. Díky papilárním liniím se změní původní plochý tvaru desky na vlnitý a tím se změní tvar elektrického pole. Horní desku tvoří povrch kůže, do které je pouštěn řídící elektrický signál. Kolem senzoru je vodivý prstenec, a jakmile dojde k dotyku, uzavře se elektrický obvod. Husté pole snímacích antén zachycují elektrické pole deformované tvarem povrchu kůže, respektive pod povrchem růže. Signál je transformován do elektronického obrazu. Výhodou je odolnost vůči nečistotám, nehraje roli vysušená pokožka a drobně poškozená kůže. Technologie pořizuje několik snímků, které jsou postupně optimalizovány až do doby přesného přijetí, nebo odmítnutí šablony.

Snímače optoelektrické - skládají se ze dvou vrstev. Horní vrstva, která má kontakt s kůží verifikované osoby je vyrobena z polymeru TFT. Což je průhledný film z miniaturních tranzistorů, jež umožňují přepínání jednotlivých pixelů, tj. obrazových bodů mezi stavy

zapnuto a vypnuto. TFT má tedy schopnost po dotyku eliminovat světlo, to je zachyceno v další skleněné vrstvě, do které jsou v hustém poli zataveny fotodiody, které převádějí světelný impuls na impuls elektrický. Tímto způsobem je vytvořen elektronický obraz daktyloskopického otisku. Rozměry snímače jsou větší a limitující pro implementaci do malých a přenosných zařízení. Výhody jsou vysoká kvalita, odolnost proti statickým výbojům a minimální vliv okolního prostředí.

Snímače kapacitní - využívají k měření elektrické kapacity. Senzor je složen s velkého počtu vodivých ploch, které jsou mezi sebou odizolovány. Dotykem kůže papilární linie přemosťují jednotlivé vodivé plošky v závislosti na kresbě papilárních linií. Brázdy se pak chovají jako izolanty. Měří se napětí a kapacitní úbytky mezi jednotlivými vodivými ploškami. Nevýhodou je nízká životnost cca 3 roky, zničení snímače vlivem statické elektřiny, a nevhodnost použití ve vlhkém prostředí. Výhodou je malý rozměr, jednoduchý princip funkčnosti, vysoká kvalita snímání v 3D.

Snímače tlakové - reagují na tlak, povrch snímače je tvořen elastickým, piezoelektrickým materiálem (krystaly), který tlak papilárních linií transformuje do elektrického signálu a tak vytváří obraz daktyloskopického obrazu. Pracují stejně dobře v suchém i mokrém prostředí. Je možné je implementovat i do platebních karet.

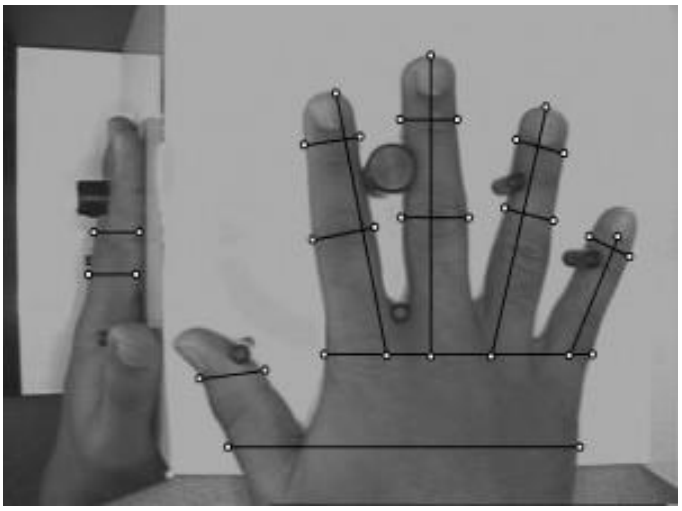
Snímače teplotní - citlivě reagují na teplotní rozdíly mezi papilárními liniemi, které se dotýkají snímaného povrchu a brázdami, ty se povrchu nedotýkají. Teplota, je rovněž ukazatelem živosti. Prstem se přejíždí přes citlivou plochu. Výstupem je obraz otisku ve formě digitálních pásů. Digitální obrazy se následně skládají do výsledného obrazu otisku. Nevýhodou je nízká kvalita a problém s algoritmy pro zpracování markant. Metody je však možné využít i ve venkovním prostředí, označuje se za méně vhodnou pro použití v přístupových systémech.

Snímače ultrazvukové - ultrazvukové snímání je bezkontaktní metodou zalkoženou na principu odrazu ultrazvukových vln od snímaného povrchu. Nemá nedostatky některých jiných metod. Podstatou je vyslání zvukových vln s vysokou frekvencí generovaných

zdrojem směrem ke snímané ploše a vyhodnocení odražených zvukových vln přijímačem, ležícím v rovině kolmé k vysílanému paprsku. Vysílaný signál má charakter velice krátkých impulsů (4 až 25 MHz). Na plastickém povrchu prstu dochází k interakci zvukových vln s papilárními liniemi a brázdami. Snímání oražených a deformovaných vln je realizováno rotující hlavou nebo hustou sítí pevných, v rovině umístěných čidel. Vyhodnocuje se funkční závislost mezi vyslanými a dopadajícími zvukovými vlnami. Obraz otisku prstu je trojrozměrný s vysokým kontrastem. Snímání má vysokou přesnost. Metoda je vhodná i pro otisky dlaní.

3.4.2 Metoda založená na snímání tvaru ruky

Metoda identifikace na základě snímání tvaru ruky byla uvedena do praxe již v 70-tých letech minulého století. Spočívalo v měření délek jednotlivých prstů, jednalo se tedy o jednorozměrnou geometrii. Druhá řada přístrojů přidala měření šířky prstů a dnes se užívá 3D měření, tedy kombinace šířky, délky a tloušťky. Délka nehtů je při snímání ignorována.



Obr. 5. Snímání biometrie ruky [5].

Uživatel klade ruku na horizontální desku opatřenou kolíky, které fixují ruku, aby snímaná poloha byla pokaždé pokud možno stejná. Je proveden osvit infračervenými LED diodami a přes soustavu zrcadel je nasnímán obraz CCD digitální kamerou. Scanner snímá pouze siluetu ladně s prsty. Jeden obraz je snímán shora, kolno na rovinu snímací desky, druhý pomocí postranního zrcadla vykresluje pohled na dlaň z boku. Mikroprocesor převádí naměřené geometrické rozměry do biometrické šablony o velikosti 9 bitů.

Referenční šablona je aritmetickým průměrem trojího snímání, je ukládána do stálé interní paměti společně s PIN kódem (použita může být i čipová karta či jiný prostředek). Jde tedy o systém verifikační. Uživatel zadá svůj PIN a přiloží ruku dle návodu na snímací desku mezi distanční kolíky. Provede se sejmutí charakteristik, porovnává se pak skóre těchto identifikačních markantů. Měření se provádí pouze u pravé ruky. Případné změny biometriky jedince jsou způsobeny změnou tloušťky prstů nebo dlaně jako takové některým nemocemi či úrazy.

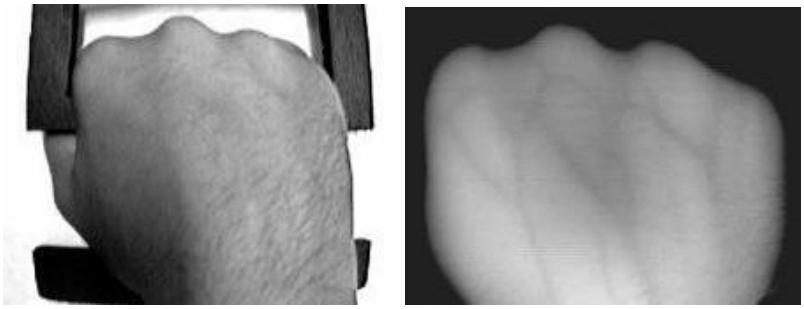
Zařízení disponuje širokými funkcemi od výmazu šablony až po nastavení prahu citlivosti i pro konkrétní osobu. Výhodou metody je její psychologická uživatelská akceptovatelnost. Je vhodná pro větší databáze uživatelů nebo pro uživatele s ne příliš častým přístupem a méně disciplinovaným z hlediska správného použití biometrického systému. Přesnost může být, je-li to žádoucí, velmi vysoká.

V praxi se vyskytují i scannery pro snímání pouze dvou prstů (ukazováku a prostředníku). Tyto scannery sice snižují jednoznačnosti identifikace, ale podstatně zvyšují rychlost verifikace. Nasazují se do prostředí s vysokou rychlostí průchodnosti (10 osob za minutu) s nároky na nižší stupeň bezpečnosti.

3.4.3 Metoda založená na snímání krevního řečiště hřbetu ruky

Je novější metodou, založená na rozpoznávání pomocí specifického obrazu cév na povrchu hřbetu ruky. Cévami rozumíme tepny rozvádějící po těle okysličenou krev a žíly vracející tuto krev opětovnému okysličení. Jejich tvar, velikost a orientace je specifická pro každou sobu.

Uživatel kladu ruku hřbetem nahoru na snímací plochu scanneru. Pořizuje se celkový plošný obraz rozložení cév v blízkosti povrchu hřbetu ruky. Hřbet ruky je nasvěcován polem infračervených diod a snímán černobílou CCD kamerou v šestnácti stupních šedi. Infračervené snímkování je citelné na vyzařované teplo, ceny teplo rozvádějí po těle a na snímku kontrastně vystupují na pozadí a jsou dobře viditelné.



Obr. 6. Zobrazení hřbetu ruky viditelným a IR světlem [6].

Následně se pomocí algoritmů provádí různé obrazové konverze (potlačuje se šum, ostře se vykreslují cévy – peletizace kresby řečiště), a vytvoří se binarizovaná podoba biometrické šablony. Obraz je snímán vektorově a tak uživatel není nucen ruku přikládat stále do téže polohy. Postup verifikace je pak stejný jako u předchozí metody. Stejně lze bezkontaktně snímat i krevní řečiště dlaně ruky. Metoda je neinvazivní, bezkontaktní a sociálně přijatelná.

Obr. 7. Snímání krevního řečiště dlaně [6].

3.4.4 Metoda založená na snímání tváře

Podoba tváře a výrazu slouží odedávna k rozpoznávání jedinců. V policejní praxi jde o pořizování fotografií zadržených osob a o vykreslování dle popisu svědků, tedy o sestavování portrétu. V bezpečnostních aplikacích se jedná o strojové rozpoznávání.

Identifikace osoby na základě její tváře má ve srovnání s metodou otisku prstů nebo oční duhovky nižší identifikační jednoznačnost. Umožňuje však bezkontaktní snímání na

velkou vzdálenost. Počítačově podporovaná identifikace podle její tváře má dvě základní etapy.

První je detekce a lokalizace tváře ze scény, tedy z fotografie či nasnímaného záznamu, jako rozpoznání tváře od ostatních objektů. V druhé etapě jde o samotnou identifikaci, o automatické nalezení základních identifikačních charakteristik a porovnání s databází. Proces rozpoznávání lidské tváře se liší dle typu aplikace dle požadavků, které jsou na ni kladeny. Může jít o klasické verifikační úlohy nebo o vyhledávání nežádoucí osoby či osob na snímané scéně.

Metody rozpoznávání lidského obličeje můžeme dělit dle různých kritérií. Je možné je rozpoznávat jako 2D nebo 3D obraz. Dále dle spektra jako černobílé nebo barevné, případně infračervené. Dle pohledu jako čelní či z profilu. Dle dynamiky jako statické či dynamické (sekvence dílčích statických obrazů). Dle nástrojů zpracování a užití algoritmů znalostních, statistických, neuronových sítí a genetických algoritmů.

Strojové rozpoznávání prošlo dynamickým vývojem a v současné době jsou technologie vyhledávání zcela automatizované. Detekce a lokalizace tváře se dělí na dva základní typy; statisticky orientované metody a znalostní metody.

Statisticky orientovaná metody detekce a lokalizace jsou:

- metoda podprostoru - je založená na hledání charakteristik lidské tváře (oči, nos, ústa) v obraze. Jestliže všechny charakteristiky tváře leží v témže podprostoru vícerozměrného prostoru, je tento podprostor reprezentací tváře. Detekce tváře je pak detekcí podprostoru, v níž se tvář nalézá. Pro porovnávání je obraz normalizován na stejnou orientaci, velikost a stupeň šedi.
- metoda neuronových sítí - jedná se o aplikace, jejichž úkolem je bezchybně rozpoznat co tváří je a co ne. Na základě vzorů (knihovny).

Znalostní metody detekce a lokalizace jsou:

- metoda založená na rozložení odstínů šedi v obraze - je založená na obecných pravidlech odstínů v obrazech tváří za normálních světelných podmínek (oči jsou vždy tmavší než čelo). Užívá se metody mozaiky, zpracovávaná oblast se dělí do obrazových bloků v čtvercové síti, jestliže se v zpracovávaném obraze nachází tvář, nachází se v obrazových blocích markanty tváře. Postupně se vybírají jednotlivé

bloky a hledají se markanty. Bloky, které nesplňují pravidla, jsou vyřazeny, bloky, které zůstanou, se dále dělí. Zohledňuje se vztah mezi jednotlivými částmi obličeje.

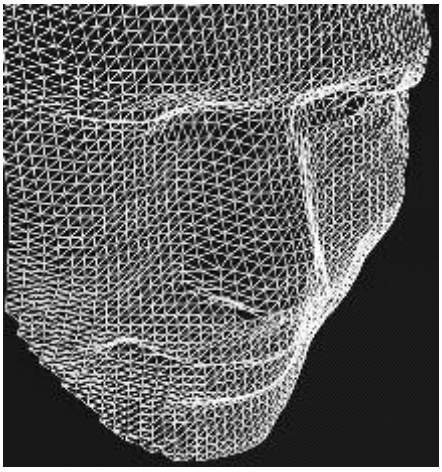
- metoda založená na rozpoznávání obličejových obrysů - obrys (kontura) je důležitou charakteristikou tváře. Metody se užívá k detekci nalezení jednotlivých objektů v tváři. Je doplňkem jiných metod.
- metoda založená na informaci o barvách - definuje zásady odlišnosti obličeje od barevně diferencovaného prostředí a podobnost rozložení barev v obličeji lidí téže rasy.
- metoda založená na informaci o pohybu na scéně - využívá časovou sekvenci snímků, pohybujících se osob vzhledem k pozadí. Problémem je přítomnost více osob na scéně, jejich pohyb různými směry a různou rychlostí, překrývající se tváře, nebo tváře zakryté jinými předměty.
- metoda založená na symetrii - je založená na nalezení symetrického obrazce odpovídajícího charakteristikám lidské tváře. Jde o zkoumání kruhových obrazců na scéně a následné zkoumání symetrických charakteristik, nebo o zobecněnou symetrickou transformaci, detekující symetrické body, jimiž jsou části obličeje. Užívá se i přímá symetrie, ta zohledňuje symetrii v různých směrech a krom detekce tváře určuje i její lokalizaci na scéně.

Detekce lidské tváře na komplexním pozadí je složitou úlohou a proto se užívá kombinace více metod detekce a lokalizace, která odstraňuje nedostatky jednotlivých metod samotných. V některých případech je možno ovlivnit pozadí či světelnost snímané scény a tím zvýšit efektivnost detekce a lokalizace a tím i celkovou produktivitu biometrické aplikace.

Obr. 8. Program rozpoznávání obličeje [7].

Zpracování obrazu tváře pro potřeby identifikace je druhou fází rozpoznávání. Pro nalezení identifikačních charakteristik je propracována řada metod:

- metoda dle rozložení odstínů šedi - je již popsanou metodou mozaiky. Známý záznam tváře je tedy rozložen do bloků mozaiky a zkoumá se podobnost jednotlivých segmentů pomocí n-rozměrných vektorů do doby nalezení shody. Mimo segmentů se porovnává i jejich okolí.
- metoda založená na geometrických tvarech a identifikačních markantech - je založená na dílčích charakteristikách geometrických rysů obličeje, na poměru vzdáleností a úhlů mezi jednotlivými identifikačními body (markanty), jako jsou vnitřní a vnější koutky oka, vnější horizontální body rtů, bod přechodu nosu v čelo atd. Metoda je závislá na světelných podmínkách, slouží jako filtr jiným metodám.
- metoda optických toků - je založená na analyzování dynamických změn pohybu ze sekvence časově po sobě jdoucích snímků jedné a téže osoby. Každý bod má svůj směr a pohyb a lze ho vyjádřit vektorově. Změny jsou texturální a strukturální, tedy změny intenzity a změny v prostoru. Slouží pro rozpoznávání emocí.
- metoda deformačních modelů - je architekturou dynamického propojování. Dá se přirovnat k přiložení sítě na tvář. Z hustoty čar a deformace lze sestavit prostorový obraz (otisk) a rozpoznat rysy tváře. Rozpoznávání tváře přechází do úlohy ztotožňování elastických grafů.



Obr. 9. Architektura dynamického propojování [7].

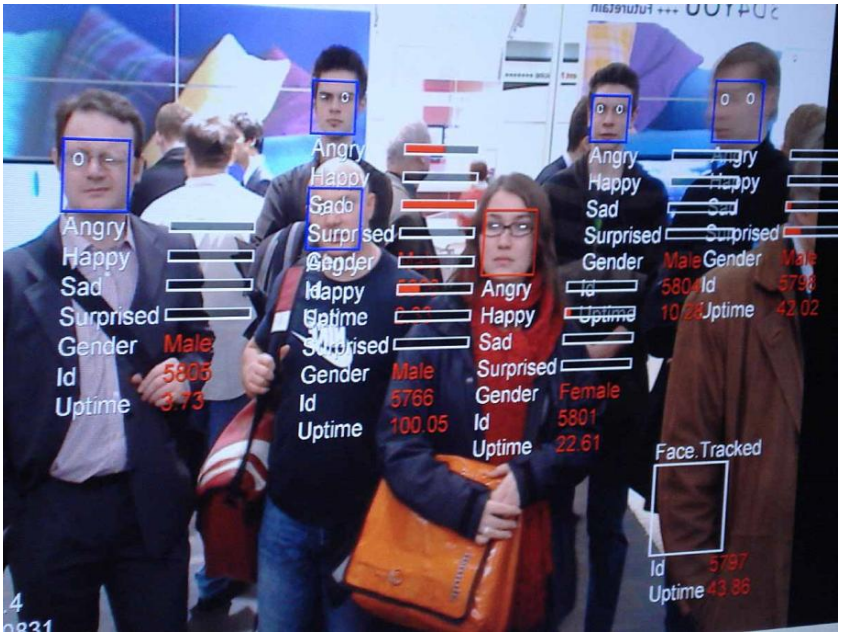
- metoda neuronových sítí - je řešení s použitím výpočetního systému, který se učí sám. Ne vždy jsou totiž snímaná data kompletní a ne vždy je jasné jaký algoritmus je výhodné použít. Neuronová síť využívá ke své práci propojených procesorů a výpočetních cest, jsou schopny se učit samy a analyzovat rozsáhlé a komplexní množiny dat. Síť vytváří spojení mezi mnoha různými procesními prvky, a vyhodnocuje váhu spojení. Známý je vstup a výstup, ale ne přesný tok dat mezi jednotlivými vrstvami. I když je tento systém pomalejší než klasický algoritmus, může paralelně zpracovávat velice rozsáhlé množiny dat. V tomto směru jsou tedy výkonnější. Využití metody neuronových sítí pro identifikaci tváře je velice adaptabilní a účinné proti všem jiným metodám.
- metoda eingenhed - vnímá celou hlavy jako třírozměrný 3D objekt. Odvozuje každou tvář z jakési standardní normalizované hlavy, kde konkrétní tvář je vyjádřením odchylek od normalizované.
- metoda infračerveného snímání - je založeno na snímání rozložení tepla v obličeji, jeho vyzařování do okolí. Porovnávají se tvary obrazců v infračerveném spektru, teplota slouží k vykreslení těchto obrazců.

Automatické rozpoznávání tváří má dnes široké uplatnění, od kontroly prostorů na veřejných prostranstvích, letištích, v nákupních centrech a sportovních areálech, až po přístupový systém. Tedy na ochranu státních veřejných i privátních prostorů. Snímání tváře je uživatelsky jednoduché, neinvazivní, mnohdy bez vědomí snímaného i na velkou

vzdálenost. Metody neuronových sítí si dokáží poradit i měnícími se účesy, brýlemi, pokrývkami hlavy a různými světelnými podmínkami.

Výhodou takovéhoto rozpoznávání je možnost použití stávajícího kamerového systému či záznamového zařízení. Slouží k pasivní identifikaci, tj. upozornění na přítomnost nežádoucí osoby v jistých prostorách a umožňuje sledovat pohyb této osoby. Podmínkou je určitá kvalita snímací technologie a softwarová vybav enost.

Na Obr.10. je vyobrazen výstup softwaru schopného vyhodnocovat nejen identitu jako takovou, ale také chování jedinců dle jejich pohybů nebo dynamiky v tváři.



Obr. 10. Systém pro analýzu tváří, identifikuje pohlaví a náladu [9].

3.4.5 Metoda založená na snímání tvaru ucha

Tvar ucha a jeho otisky poskytují velké množství jedinečných charakteristik, jeho využití v komerční sféře se však zatím samostatně nevyskytuje pouze jako doplněk ke snímání tváře. Využití nalezne tedy výhradně v kriminologii.

3.4.6 Metoda založená na snímání ručního písma a podpisu

Vzhled podpisu a jeho vznik je behaviorální vlastností člověka, je odrazem jeho osobnosti. Při snímání a rozlišování užíváme systémy on-line a off-line.

Systém on-line porovnává jednoznačné charakteristiky jako je dynamiku podpisu, provedení tahů, sílu, kterou tlačíme při psaní na podložku, rychlost psaní, změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na a nad papírem, tlak prstů na pero samotné, sklon psaní, přiložení prstů na podložku a jiné.

Charakteristiky jsou získávány v reálném čase v průběhu vzniku podpisu specifickým hardwarem pomocí speciálního tabletu či pera. Používáno je pero (téměř nerozlišitelné od standardního), které bezdrátově přenáší snímané informace do přijímače a následně do počítačové jednotky k porovnání, nebo je mono využít PDA obrazovku a pera se speciálním psacím hrotem. Podpis je těžké zfalšovat, ovšem problémem může být nutnost velkého množství referenčních vzorků a nastavení prahu citlivosti.

Obr. 11. Biometrický LCD tablet [10].

Systém off-line porovnává podpis na papíře s referenčním vzorkem, jeho podobu a tvar písmen. Podpis je nasnímán kamerou, digitálně zpracován a porovnán s následným rozhodnutím shody. Systém může rozlišovat i podvržení kopie originálu pomocí analýzy spektra. Dále zkoumá, vždy podezřelou, 100%ní shodu. Metoda nikoho neobtěžuje jak po stránce technické, tak i společenská a kulturní.

3.4.7 Metoda založená na snímání hlasu a řeči

Audioexpertíza hlasu a řeči osob (fonoskopie) má v komerční sféře uplatnění jako doplňková metoda při verifikaci. Je to dáno nízkou spolehlivostí a proměnlivosti hlasu vzhledem k psychice a zdravotním stavu mluvčího. Konečná podoba hlasu je dána fyziologickými vlastnosti tj. uspořádáním částí těla, které se podílí na vytváří zvuku, a behaviorálními vlastnostmi danými vývojem a naučením.

Aplikace je většinou založená na textové závislosti. Mluvčí je vyzván k namluvení či přečtení textu, systém pak zkoumá porovnávání stejné sekvence zvuků. Může se jednat o heslo vybrané systémem či heslo vybrané uživatelem. Systém s textovou výzvou není uživateli znám předem. Identifikuje pravost vybraných slov a následně pravost mluvčího. Je to ochrana pře předem nahraným textem. v tomto systému výzva-odpověď jde vlastně o test živosti. Při verifikace je dobré zachovat vhodné akustické podmínky tj. nebýt rušen. Existují i textově nezávislé systémy tyto modelují řečový signál z globálního pohledu. Výsledná přesnost je však nižší. Ovlivňující faktory jsou spolupráce uživatele, podmínky záznamu, množství registračních a testovacích dat, variabilita mluvčího tj. stárnutí či momentální hlasové dispozice (nemoc).

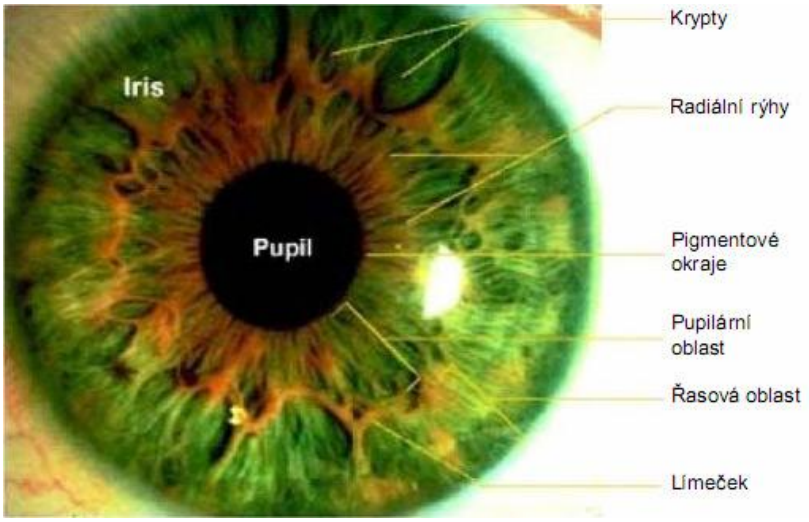
Metody se užívá v bankovnictví a telekomunikaci jako doplňkové metody a ve výkonu testu jako kontroly domácího vězení. I při nízké spolehlivosti je tato metoda považována za akceptovatelnou vzhledem k přirozenosti mluveného jednání a absenci fyzického kontaktu.

3.4.8 Metoda založená na snímání oční duhovky

Složitý vzor duhovky obsahuje mnoho charakteristických znaků; klenuté vazy, rýhy, hřbety, krypty, prstence, korány, pihy a klikaté čáry a při snímání různými částmi spektra jsou rozlišitelné ještě další znaky. Jednoduchost nalezení očí na snímku tváře a charakteristický kruhový tvar duhovky dělá tuto metodu spolehlivou a velmi přesnou.

Snímání je prováděno monochromatickými CCD kamerami a vyžívá se blízkého infračerveného pásma 700 – 900 nm, které je neinvazivní pro uživatele. Systémy mohou užívat jednu či dvě kamery (většinou s širokoúhlou optikou). Nejprve je nalezeno oko pomocí výše popsaných metod a následně lokalizována duhovka a další kamerou je duhovka nasnímána. Může být také využito spolupráce uživatele tak, aby mu umožnila umístit své oči do dosahu kamery s úzkým záběrem. Obraz je zaostřen a sejmut. Snímky splňující kritérium minimální ostrosti jsou následně analyzovány na přítomnost duhovky, a

ta je lokalizována. Následuje kódování znaků a srovnávání. Vyhodnocuje se, do jaké míry jsou snímky odlišné či shodné.



Obr. 12. Struktura duhovky [11].

Teoretická pravděpodobnost nesprávného přijetí je 1 ku 4 milionům. Algoritmy Johna Daugmana pro kódování a rozpoznávání vzorů duhovek jsou reprezentovány srovnávacím softwarem, který byl využit v doposud všech komerčně nasazených systémech rozpoznávání duhovky. Všechny organizace provádějící testy algoritmu oznámily počet nesprávných přijetí roven 0 (nepočítaje případy záměrných pokusů o podvody např. vytvoření imitace duhovky někoho jiného)[2]. Závěr je takový že; jsou li dvě sejmutí shodná, patří tento snímek jedné a téže osobě.

Prohledávající algoritmus je schopen provádět až 100 tis. srovnání různých duhovek za sekundu, aplikace jsou vysoce spolehlivé a je možné je využít na letištích, v procesu imigrační identifikace či registrace přístup zaměstnanců do vymezených prostor, kde je vyžadována velmi vysoká bezpečnost a nízká míra chybovosti jako v bankovnictví, vězeňství, v jaderných elektrárnách nebo prostory ve zvláštním režimu utajení.

3.4.9 Metoda založená na snímání oční sítnice

Sítnice se nachází na zadní straně oční bulvy a detekuje světlo na ni dopadající a vede toto informaci dále do mozku. Je zásobená pomocí cév. Každé oko má svůj unikátní vzor očních cév.

Obr. 13. Snímek oční sítnice [11].

K získání snímku je používáno speciálních kamer a k osvětlení sítnice infračervené světlo. Snímek je vytvářen až odrazem cév ve vrstvě choroidu za nimi. Metoda je uživatelsky nepřívětivá a má vysokou cenu, není možné ji použít ve venkovním prostředí a snímání je zdlouhavé a náročné na kvalitu snímku. Vyskytuje se ojediněle často jako testovací projekt.

3.4.10 Metoda založená na snímání dynamiky stisku počítačových kláves

Dynamika psaní na klávesnici je behaviorální charakteristikou nejméně ovlivněnou momentálním fyzickým a psychickým stavem pisatele. Zkoumání může být zaměřeno na několik charakteristických rysů uživatelova psaného projevu.

- doba stisku klávesy (od počátku do doby trvání jejího stisku)
- rozdíl času mezi stiskem jednotlivých kláves (ctrl+v, ctrl+c)
- celkovou rychlost psaní (podle stisků kláves za určitý časový interval)
- frekvenci chyb (sledování chyb, tedy stisk klávesy backspase)
- styl psaní velkých písmen (sledování zvyklosti uvolňování při psaní velkých písmen, nejprve klávesu Shift nebo klávesu s daným znakem)
- síla použitá pro stisk klávesy (s použitím speciální klávesnice, schopné měřit sílu úderu)

Registrace uživatele je prováděna během jeho práce a uživatel je vícekrát vyzván k zadání předem zvolené frázi a z těchto vstupů je následně vypočítán reprezentativní vzorek. Rozhodnutí o verifikaci může být rozhodnuto s pomocí neuronových sítí, nebo na algoritmech porovnávajících vzory.

Lepších výsledků je dosahováno u zkušených písařů, nezkušení písaři se mohou časem zlepšovat a oddalovat se tak od zaznamenaného vzoru. Mimo přístupu, může systém kontrolovat identitu uživatele průběžně či následně, při dočasném přerušení práce na počítači.

Tato metoda je čistě softwarovou implementací a je jednoduchá a hardwarově nenáročná a klávesnice je přirozeným komunikačním prostředkem interakce. Na podobném principu pracuje:

Metoda založená na dynamice pohybu myší je srovnatelná s předchozí. Identifikující osoba je vyzvána, aby za pomoci myši nakreslila nějaký předem určený vzor, verifikační proces připomíná počítačové kreslení. Z nakresleného vzoru se extrahují důležité znaky, jako jsou pozice, rychlost tahu, úhly a zaoblení, jež může následně porovnávat s referenčním vzorkem. Tato technologie je zatím stále ve vývoji.

Není vyloučeno, že vzniknou programy, které se učí samy a budou v podstatě pozorovat a zkoumat uživatele, jeho stěžejní chování při práci s PC (práce s okny, způsob kopírování, rychlost clicku a dvojclicku, vyhledání pozice na obrazovce u zavírání oken, četnost používaných slov při on-line komunikaci a podobně). Metoda je vyloženě softwarová a pro uživatele nepozorovatelná.

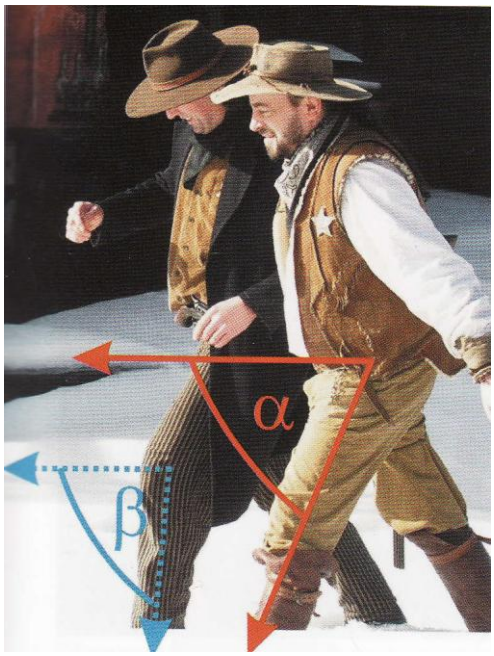
3.4.11 Metoda založená na snímání lokomoce

Lokomoce člověka je vyjádření jeho pohybu v prostoru vlastní silou. Zachycují se funkční a dynamické vlastnosti pohybu, respektive pohybový návyk v rámci dynamického stereotypu. Člověk může chůzi vědomě ovlivnit, ale v případě rychlých změn či reakcí se chová přirozeně. Při analýze je nutné, aby byl sledován souhrn všech znaků a jejich konkrétní souvislosti. Lze vymezit: geometrické, kinematické a dynamické znaky.

V praxi jsou využívány metody počítačového vidění k získání požadovaných pohybových charakteristik, které mohou a nemusí zohledňovat změnu chůze člověka vlivem oblečení, změny stavu či vnějšího vzhledu (opilost, těhotenství, podpatky).

Pohyb je možné rozpoznávat **podle trajektorie člověka**, sledováním těžiště. Těžiště opisuje při pohybu vlnící se křivku, přidáním dalších aspektů (ohybu v klubech, rotace pánve a hrudníku) se křivka zjemňuje a dosahuje sinusoidální průběh. Těžiště těla není viditelné, nahrazuje se sledováním pohybu temene hlavy.

Další metodou je **sagitální kinematika** (měření základních charakteristik), jde o charakteristiku chůze. Sledují se jednotlivé částí pohybového aparátu (kyčle, kolena, kotník) a měří se úhel odklonu určité části končetiny od kloubu, směrem níže od předozadní osy procházející daným kloubem, po dobu jednoho cyklu chůze. Pohyb je znázorňován do grafů. Metoda je náročná na kapacitu počítačové paměti, a rychlost zpracování obrovského množství dat z obrazových sekvencí.



Obr. 14. *Ukázka měření úhlu pohybu kyčle (α) a kolena (β) v sagitálním směru. [2].*

V rozpoznávání osoby na základě její chůze se běžně využívají poznatky, metody a způsoby jejich aplikace i z ostatních biometrických oblastí. Dnes rozlišujeme směr rozpoznávání dle analytických metod:

- zpracování siluety pohybujícího se objektu (zaměření na tvar, vyčleňují z pozadí pohybující se siluetu, sledují a vyhodnocují průměrováním)
- modelování pohybu (zaměření na dynamiku pohybu, tělesné rozměry, a úhly při chůzi, nezohledňuje vliv oblečení na chůzi)

Referenční záznamy jsou pořizovány především v civilních, případně vojenských institucích (letiště). Výhodou je aplikovatelnost na velkou vzdálenost, metody se využívá při automatizovaném vyhledávání osoby v zájmovém prostoru.

3.4.12 Metody založené na jiných charakteristikách

Metoda snímání DNA – identifikace člověka prostřednictvím DNA je složitým technologickým postupem, trvajícím řadu hodin.

Živá buňka obsahuje biopolymery nukleové kyselina proteiny. Nukleové kyseliny nesou informace a proteiny jsou stavení polymer. Soubor proteinů je každého jedince jiný. Kyselina tedy deoxyribonukleová kyselina DNA je tedy nositelem informace a je obsažena ve všech tkáních. Kód DNA je rozvětvený řetězec tvořený střídáním čtyř možných prvků.

Identifikace na základě DNA je metodou nejpřesnější, ale drahou a využití v bezpečnostních aplikacích nenalezne dříve, nežli se zkrátí doba vyhodnocení na několik minut, zatím tedy nalézá využití v kriminologii a kriminalistice.

Metoda snímání tvaru a lůžka nehtu - lidský nehet je přirozeně nerovný. Při svém růstu kopíruje tvar lůžka, které se nachází pod ním a získává tím svůj jedinečný vlnitý tvar. Každý nehet u každého jedince na každém prstu je jiný. Mezi nehtem a lůžkem pod ním se nachází přírodní polymer keratin, jenž dokáže měnit orientaci polarizovaného světla. Když se tedy osvítí pod správným úhlem, lze analyzovat fázové změny paprsku po odrazu. Reprezentativní vzorek lůžka nehtu připomíná čárový kód. Metoda je málo odolná proti podvrhům.

Objevilo se také řešení pomocí RFID čipu který je přilepen na vrchní části nehtu Je schopný vyzařováním pod sebe detekovat kapacitní odpor nehtu, jenž je závislý na individualitě jedince.

Snímání absorpčního spektra lidské kůže - lidská kůže je odlišná vzhledem i vnitřní strukturou. Jednotlivé vrstvy kůže mají různou tloušťku, rozhraní mezi nimi se odlišně vlní a také tvar a hustota buněk uvnitř těchto vrstev je rozdílná. Čtecí zařízení je složeno z několika LED diod o různých vlnových délkách, jež ozařují kůži, a analyzuje rozptýlený odraz zachycený foto-diodami. Poměr diod na snímači může být například 32 ku 5. Technologie je do jisté míry podobná ultrazvukovému snímání otisku prstů.

3.5 Technická úskalí

Použití konkrétní metody je vždy závislé na hranicích snímané metody v závislosti na fyzikálním principu snímače, použitém algoritmu, případně na kombinaci těchto veličin. Kritériem použití je i ve velikosti, ceně a rozlišovací schopnosti zařízení s ohledem na potřeby uživatele.

Nároky kladené na snímače jsou především:

- Vyhovující celkové rozměry, což není problém přístupových systémů, ale konkrétní implementace do malých zařízení (notebooky, čipové karty), tam se využívají zejména kapacitní snímače.
- Dostatečně velká snímací plocha, pro účely rozeznání a nasnímání dostatečného počtu markant.
- Dostatečné rozlišení, které je dáno především použitým algoritmem. Čím vyšší rozlišení, tím kvalitnější snímač z hlediska kvality získaného obrazu otisku pro další zpracování.
- Dobrá kvalita obrazu bez zkreslení, ta je omezena použitým fyzikálním principem (dostatečný kontrast, široká škála stupně šedi, podmínky při snímání vlhko, suchý prst, prach apod.). Snímač má být opatřen korekcemi tohoto zkreslení.
- Opakovatelnost dosažené kvality, což znamená zamezení rozdílné kvality z rozdílných míst nasnímání, vzniklé posunutím či natočením snímané části těla, při snaze neobtěžovat uživatele.
- Ochrana proti napodobeninám (test živosti).
- Odolnost vůči elektrostatickému výboji; elektronické součástky a zařízení a integrované obvody pracují s nepatrnými proudy a vysokými pracovními odpory (např. obvody CMOS), elektrostatický náboj vznikající na osobách při jejich chůzi je pro tato zařízení a součástky velmi nebezpečný zvláště pro snímače teplotní a kapacitní.
- Uživatelská přívětivost odráží příjemnost či nepříjemnost metody při snímání pro uživatele. Cílem je neobtěžovat.
- Nároky na implementaci do zvoleného systému, (interface, knihovny) konkrétní technické připojení a zabezpečení.
- Odolnost vůči mechanickému poškození, jako odolnosti v provozu za zhoršených klimatických podmínek, pro zvláštní provozy či armádní využití.

- Spolehlivost snímačů, což bývá často klamný údaj výrobce.
- Životnost snímačů, tu ovlivňuje míra poškozením jednotlivých částí, doba životnosti použitých materiálů, zastarání principu a vliv konkrétního prostředí.
- Cena snímače, je poměrem ceny a kvality v kontextu potřeb konkrétního využití.

Potřeby uživatele se vždy odvozují od jeho cílů, tedy co a do jaké míry chce chránit, případně na jak dlouho. Uživatel také řeší otázku komunikace systému identifikace s ostatním systémy firmy.

4 MOŽNOSTI NASAZENÍ NOVÝCH TECHNOLOGIÍ V PRAXI

Ne všechny charakteristiky jsou vhodné pro použití k identifikaci v rámci bezpečnostních systémů ať už z důvodů nízké přesnosti nebo nepříliš vysoké uživatelské přívětivosti. Existuje několik dalších parametrů, které přímo ovlivňují míru vhodnosti konkrétní technologie pro praktické nasazení. Takovými parametry jsou bezpečnost jako přesnost vyhodnocení, nákladnost, míra subjektivní přijatelnosti procesu čtení charakteristiky pro uživatele, jednoduchost nebo složitost provádění snímání charakteristiky a její vyhodnocení.

4.1 Kritéria biometrických metod

Přestože biometrické údaje jsou jedinečné, biometrická identifikace není bezchybná. Jsou však popsána kritéria důležitá pro funkčnost biometrických identifikačních a verifikačních technologií, tak i pro jejich praktické efektivní nasazení. Tedy celkovou úspěšnost. Kritéria se dotýkají základní teorie a praxe identifikačních a verifikačních systémů, ochrany osobních údajů, ekonomičnosti, praktičnosti, společenské a finanční přijatelnosti.

4.1.1 Kritéria operační

Charakteristiky: jedinečnost, neměnnost, měřitelnost, uchovatelnost, spolehlivost, exkluzivita, praktičnost, přijatelnost, uživatelská přívětivost.

Jedinečnost – nebo také unikátnost je charakteristika, která umožňuje odlišit jednu osobu od druhé s vysokou spolehlivostí a přesností.

Neměnnost – stálost identifikačních znaků člověka po dobu jeho života.

Měřitelnost – charakteristiky musí být měřitelné a symbolicky vyjádřitelné, se znalostí chybovosti měření.

Uchovatelnost – možnost uchovávání neměřených charakteristik bez ztráty jejich kvality a za přijatelných nákladů.

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

Exkluzivita – bez nutnosti zavedení další metody identifikace.

Praktičnost – nenáročnost na čas, kontakt uživatele se zařízením, počet vykonaných úkonů, či nácviku snímání.

Přijatelnost – vyloučení takových technologických postupů a metod, které vyžadují část lidského těla, jako provedení zásahu do lidské integrity a jakýmkoli způsobem lidský organismus poškozují nebo oslabují a bez známek diskriminace. Musí být zajištěna ochrana všech získaných údajů před neoprávněným přístupem nebo zneužitím.

Uživatelská přívětivost – nerušivý proces snímání a vyhodnocování bez pocitu diskriminace uživatele, v závislosti na hodnotě chráněné informace, či míře rizika.

4.1.2 Kritéria matematická algoritmická a bezpečnostní

Biometrické metody využívají různé matematické algoritmy, komprese, kódy a protokoly. Biometrické algoritmy jsou podobné a liší se v technologiích jednotlivých metod, kde jsou požity.

Matematický pohled na biometrické algoritmy:

- statistické metody modelování
- dynamické programování
- neuronové sítě

Bezpečnost biometrické identifikace závisí na v podstatě na kvalitě algoritmu, který musí být ohodnocen, otestován a certifikován (a také na kódování, protokolech, na bezpečném uložení databáze, a na bezpečnosti síťového prostředí při přenosu a využití dat). Chybný algoritmus má za následek nespolehlivost metody. Požadavek na kryptografické algoritmy a techniky, které musí odolávat intenzivním útokům, je tedy vysoká (a je vztažen na hodnotu chránění informace).

Z hlediska metody, algoritmu a bezpečnosti se posuzuje:

- správnost teorie
- správnost algoritmu
- bezpečnost algoritmu
- správnost výběru markantů
- efektivita a zabezpečení kódování biometrických dat
- zabezpečení databáze s biometrickými daty
- bezpečnost protokolů

- bezpečnost síťového a distribuovaného prostředí

V procesu identifikace dochází ke snímání, kódování, kompresi, přenášení, dekompresi biometrických dat a i zde záleží na spolehlivosti a bezpečnosti algoritmu. Zabezpečená biodata musí pro neoprávněnou osobu zůstat skryta a zabránit poznání skutečného obsahu a spojitosti s prověřovanou nebo existující osobou.

4.1.3 Kritéria technická

Technické zařízení se musí vypořádat s mnoha faktory, jako jsou vlivy okolního prostředí, zejména hluk, otřesy, prach, vlhko, světlo, navíc jsou na něj kladeny i další technické požadavky, jimiž jsou:

- minimální čas zpracování či vyhodnocování identifikačních charakteristik
- přijatelná chybovost
- flexibilita
- odolnost
- efektivnost
- výkonnost
- standardizace (kompatibilita, schopnost užívat části jiných systémů)
- skladovatelnost identifikačních charakteristik
- požadovaný prostor na uložení a zpracování identifikačních charakteristik, velikost šablony
- přesnost
- jednoduchost
- rychlost
- nezávislost na vnější prostředí

U časové analýzy se hodnotí čas příprav uživatele a zařízení na proces snímání, čas snímání, čas na zpracování a uložení sejmutých charakteristik, doba identifikace či verifikace. Testuje se i chybovost technologie (FRR a FAR). Vše v kontextu s jinými užívanými technologiemi identifikace.

4.1.4 Kritéria finanční

Finanční náročnost je hodnocena z pohledu:

- pořizovací ceny technologie

- ceny instalace
- nákladů spojených s uvedením do provozu (školení, trénink)
- ceny následujících upgradů, nových modifikací
- ceny návazných systémů (počítačových, fyzické ostrahy aj.)
- ceny logistické podpory a provozu
- ceny dalších zamýšlených zařízení, budoucího rozvoje systému
- ceny obsluhy zařízení apod.

4.1.5 Kritéria výrobní a uživatelská

Kvalita, dostupnost a reference na dodavatele má nemalý vliv na jeho výběr i z pohledu možného následného servisu, rozšíření zařízení a propojenost s dalšími systémy.

Uživatel může být spolupracující či nespolupracující. Nespolupracující osoby skrývající svou identitu a mají úmysl identifikační systém oklamat.

Aplikace se dále dělí na aktivní a pasivní, podle toho zda dochází k přímému fyzickému kontaktu a to platí i o skenování duhovky. Pokud jde o snímání z velké vzdálenosti nebo uživatel nemusí vykonávat specifickou činnost vzhledem ke snímacím procesům, jde o metody pasivní.

Pro uživatele mohou být aplikace obvyklá či neobvyklé dle toho jak často se s nimi setkávají, aplikace dále mohou vyžadovat obsluh či ne dle kontroly či řízení snímání.

4.2 Šifrování a biometrika

Vzhledem ke skutečnosti, že biometrický údaj není tajným údajem a k našemu otisku prstu se může dostat prakticky kdokoli, je vhodné při práci s šablonami a komunikaci na přenosových cestách systému biometrická data chránit určitým klíčem – šifrou. Šifry prošly zajímanou historií a v informační technologii se staly, zejména po propojení internetových sítí nepostradatelnými. Šifry neboli kryptografie slouží k utajování zpráv. Z celé škály zmíníme pouze metodu soukromého a veřejného klíče a hašovací funkce.

Soukromý a veřejný klíč je asymetrickou kryptografií (ta která užívá veřejného klíče). Soukromý klíč slouží k dešifrování zpráv a má být uchován v naprosté tajnosti. Veřejný klíč je všem známý klíč konkrétního příjemce, tímto klíčem šifrují odesílatelé zprávy pro tohoto konkrétního příjemce. Pokud Bob bude chtít Alici poslat šifrovanou zprávu, nalezne si její veřejný klíč a s jeho pomocí tak učiní. Jediná Alice, která vlastní odpovídající

soukromý klíč, může zprávu správně dešifrovat [1]. Tento systém způsobil revoluci ve světě kryptografie. Tajným ekvivalentem pro šifrování se stal algoritmus RSA využívající prvočísel a faktorizace. Rozložení složitého čísla na součin prvočísel je z hlediska odhalení neřešitelný problém. Soukromým klíčem mhou být biodata.

Hašovací funkce slouží k podepisování dokumentů o velkém objemu. Při velkém objemu dat by byl kryptografickým systém pomalý a je šifrován pouze otisk dat haš. Hašovací funkce pro vstup libovolné délky vytvoří otisk pevné délky, takže z desetimegabytového souboru získáte například 128bitový haš. Malá velikost výsledného otisku patří mezi charakteristické vlastnosti hašovacích funkcí [1]. Funkce je jednosměrná a tak ten, kdo zachytí cizí haš, není schopen díky jednosměrnosti odvodit původní data.

4.2.1 Biometrie v cestovních dokladech

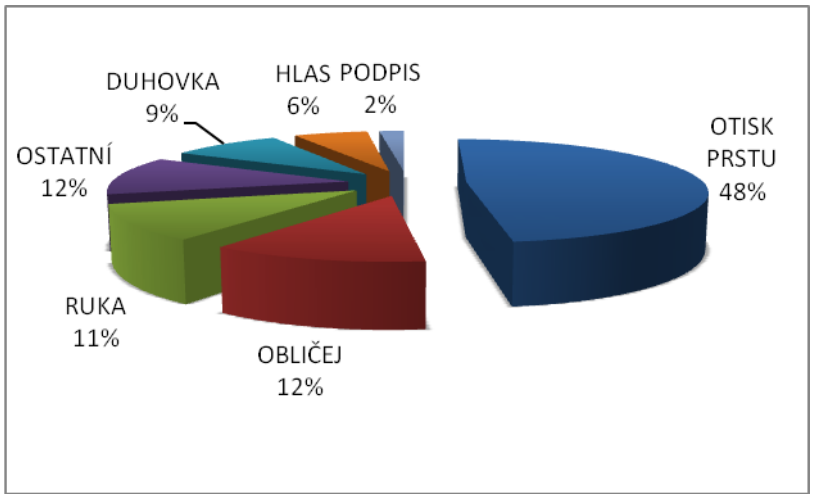
Podle nařízení Rady EU č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy, schváleného dne 13.12.2004, jsou všechny členské státy EU povinny zavést první biometrické prvky (obličej) do nově vydávaných cestovních dokladů do konce srpna 2006 a další biometrické prvky (otisky prstů) do konce února 2008. Tyto biometrické charakteristiky budou používány pro ověřování autenticity pasů a víz a také pro ověřování identity držitele pasu [12]. Biometrické pasy jsou vydávány od září 2006, jsou opatřeny mezinárodní značkou pro biometrický pas tj. logem čipu na předních deskách a údaje o držiteli jsou z velmi tvrdého plastu. Uživatel absolvuje autentizací proces, kdy jsou biometrická data sejmuta, zašifrována a zaznamenána v digitální podobě. V pase jsou data uložena v FRID čipu, zabudovaného do fyzické struktury dokladu.

Obr. 15. Biometrický pas [14].

4.3 Použití biometrik na trhu

Výběr konkrétní biometrické metody je závislý na potřebách uživatele a správné definici požadavků na zabezpečení. Úroveň kontrolních mechanismů vstupu (přesnost, rychlost) vychází z úrovně zavedené bezpečnostní politiky firmy, ta chrání firemní aktiva i zaměstnance. Zavádění nových technologií zvyšují stupeň zabezpečení majetku, osob i firemního know how a snižují provozní nálady.

Firmy využívají SBS k projektování, instalaci bezpečnostního zařízení, nebo jako kompletní službu zabezpečení objektu. Určí tedy priority a stupeň ochrany a vše ostatní zajistí bezpečnostní firma (vč. strážní, úklidová a klíčové služby). Pokud by měla být hlavním kritériem bezpečnost, zvítězila by technologie vyhodnocení duhovky oka, spolehlivostí je daleko před ostatními metodami. Nejčastěji se stále bude užívat technologie snímání otisků prstů i do budoucna, a to s ohledem na stále klesající ceny těchto zařízení, zvyšující se přesnost a uživatelská nenáročnost a snadnou implementaci do jiných zařízení. Četnost výskytu biometrik na trhu znázorňuje následující obrázek (zdroj IBG 2004). Biometrie časem vytlačí starší metody autentizace, případně se stane součástí již užívaných (tokenu).



Obr. 16. Podíl biometrik na trhu

II. PRAKTICKÁ ČÁST

5 SWOT ANALÝZA

Na biometrické systémy není snadné nahlížet jako na jeden kompletní celek jednotlivých podsystémů či prvků. Vzhledem k široké variabilitě a množství faktorů, podílejících se na jejich konečné podobě a funkci, a zařazení do oblasti bezpečnostního průmyslu, mohou být některé hodnoty výhodou, stejně jako nevýhodou. Záleží tedy na konkrétní situaci a použité kvalitě biometrických prvků příp. celého systému.

SWOT analýza hodnotí klady a zápory, respektive silné a slabé stránky biometrických systémů ve vztahu k příležitostem a hrozbám, hrozícím z vnějšího prostředí.

	silné stránky	slabé stránky
vlivy vnitřní	jedinečnost je součástí uživatele přesnost plná automatizace široká nabídka systémů kombinace s jinými autentizacemi návaznost na další systémy nastavení citlivosti šablona jako bitová informace soukromý klíč	chybovost nesprávně zvolený systém nutnost další metody u verifikace kvalita je drahá nutnost nácviku nutnost souhlasu osoby u FRR nespokojenost poničení snímače absence sekundární autentizace oklamání systému
vlivy vnější	možnost implementace variabilní stupeň zabezpečení variabilita dle prostředí využití stávající techniky oblíbené metoda nepozorovaná identifikace dostupnost stále se vyvíjí volně ke stažení samoučící systémy	zabezpečení přenosových cest pro velké společnosti ztráta soukromí nedůvěra uživatelů rychle stárne vysoké pořizovací náklady nekompatibilita pro některé uživatele nevhodné složitost použití pro vzdálený přístup nevhodné k podepisování dokumentů
	příležitosti	hrozby

5.1 Rozbor analýzy vnitřních vlivů

Za vnitřní prostředí je považováno prostředí systému jako soubor podsystémů či jednotlivých samostatných nebo provázaných prvků vyskytující se uceleně v rámci jedné organizace. Velkou výhodou biometrických systémů je jejich jednoznačnost a fakt, že biometrický údaj je součástí uživatele. Po dosažení dospělosti se již neměnní a nehrozí jeho ztráta či odcizení. Kombinací s dalšími metodami se značně zvyšuje stupeň zabezpečení, v kombinaci s tokenem se na něj neukládá soukromý klíč ale zašifrované biometrická informace jako bitová informace, což zase značně zvyšuje stupeň zabezpečení. Systém může být plně automatizovaný a pracovat zcela bezobslužně, dle nastaveného zadání. Jednotlivé parametry lze pozměňovat a to i ve vztahu pouze ke konkrétním uživatelům, existuje totiž procento lidí, kteří mají problém se snímáním, a je vhodné pro tyto jedince nastavit nižší citlivost tedy procento shody. Zákazník si z vyskytující se nabídky na trhu může zvolit variantu levnou i cenově náročnou, podle svých potřeb s ohledem na účel, jaký má biometrie plnit. Cenově náročnější systémy biometrické identifikace jsou velice přesné, jsou vybaveny softwarovými aplikacemi spolupracujícími s jinými již existujícími systémy firmy, jsou opatřeny kvalitní kryptografickou ochranou, často jsou založeny na bázi stavebnicového systému, kdy předpokládají další rozšiřování, růst a inovaci systému. Naproti tomu levná zařízení jsou lehce dostupná, mají spíše odstrašující charakter, jejich životnost je znatelně kratší, často jsou implementována v jiných zařízeních a předpokládá se u nich skončení funkce s funkcí zařízení, nebo uživatel kalkuluje s rychlým vývojem, neboť dnešní technologie mohou být v horizontu cca 5ti let již zastaralé.

Slabou stránkou těchto systémů je jejich chybovost, biometrické rozpoznávání je vždy mírou shody a vždy existuje pravděpodobnost nesprávného přijetí či odmítnutí, byť je toto číslo uváděno v mizivém procentu. Správné nasnímání totiž ovlivňuje více faktorů, jako je třeba vhodně zvolený systém vzhledem k prostředí, například zvolení snímače s kapacitním čidlem do prostředí s elektromagnetickým rušením, nebo teplotního do prostředí s vysokými teplotami nebude správným řešením. Také zvolení levnější varianty, nebo neověřeného dodavatele systémů pro ochranu strategických informací či vyhrazeného prostoru může s sebou nést případnou rozladěnost odmítnutých oprávněných uživatelů, poruchovost systému, nekompatibilitu s návaznými systémy a podobně. Výsledkem je pak nespokojenost zákazníka a celková nedůvěra k těmto systémům. Záměrné oklamání systému a předkládání padělků či napodobenin se dá úspěšně řešit volbou kvalitnější

metody, systému opatřeného ochranou proti těmto povrchům. Kvalitní snímače jsou opatřeny testem živosti, nebo pracují v kombinaci s další identifikační metodou. Té je také potřeba při verifikaci, což může být bráno jako nevýhoda, ovšem verifikační proces je mnohem rychlejší než identifikační. Je to opět tedy otázka potřeby a požadavku uživatele.

Za nevýhodu je považován i nutný souhlas uživatele s poskytnutím citlivých údajů, jimiž biometrické údaje jsou. Zpracování citlivých údajů řeší § 9 zákona o ochraně osobních údajů (ZOOU) a zpřísňuje požadavky na zpracování těchto údajů bez souhlasu. Zaměstnavatel má však právo na kontrolu zaměstnanců při jejich pracovní činnosti a právo na ochranu majetku. Správce má povinnost shromažďovat osobní údaje, odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu (§ 5 odst. 1 písm. d) ZOOU). Záleží tedy na účelu. Pokud jde o evidenci docházky zaměstnanců, jsou otisky prstů nad rámec stanoveného účelu, pokud půjde o zabránění průmyslové špionáže, jde o souladu s tímto účelem [13].

Souhlas se zpracováním osobních údajů by měl být písemný s definicí účelu zpracování, upřesnění o jaké osobní údaje se jedná, jakému správci a na jaké období je souhlas dáván. Zaměstnavatel může tento souhlas zařadit ve svém organizačním řádu nebo vnitropodnikové směrnici. V podstatě je ale odkázán na vstřícnost svých zaměstnanců. Mnozí tento problém řeší výběrem jiné metody verifikace.

Za slabé místo sytému je považována absence sekundární autentizace, při výpadku celého systému, ovšem systém je detailně propracovaný a chráněný před těmito událostmi, pak by bylo otázkou, zda by sekundární autentizace nebyla slabým místem ochrany.

5.2 Rozbor analýzy vnějších vlivů

Za vnější prostředí je považováno okolí organizace jako daný stav ekonomický, politický a legislativní a hodnotí vztah biometrických systémů vzhledem k tomuto prostředí, a vztahy zprávy a tendence prvků, osob a jiných subjektů v tomto prostředí. Přičemž hodnoty systému vnitřního a vnějšího prostředí se mohou opakovat.

Faktem je, že v posledních létech jsou biometrické systémy častěji užívány a obava uživatelů i celkový náhled na jejich zavádění do civilních sektorů klesá. Systémy a prvky se stávají součástí běžného každodenního života jako kdysi platební karty. Využívání těchto systémů sebou nesou jistá rizika, ale jsou především pohodlným a rychlým prostředkem přístupu. Vliv na tuto skutečnost má propagace výrobků využívajících

biometriku jako jsou biometrické zámky, povolení přístupu do počítače či diáře, trezorové zámky s biometrikou atd. I legislativa využití biometriky ve vnějším prostředí nijak zvlášť neomezuje. Je to dáno poměrem možných hrozeb teroristických útoků ve vnějším prostředí a jejich možných následků. Občané a uživatelé chtějí být chráněni a systém, který je nijak neobtěžuje, využívá stávajících systémů (např. kamerových) a je v podstatě softwarovou záležitostí, je obecně dobře akceptován.

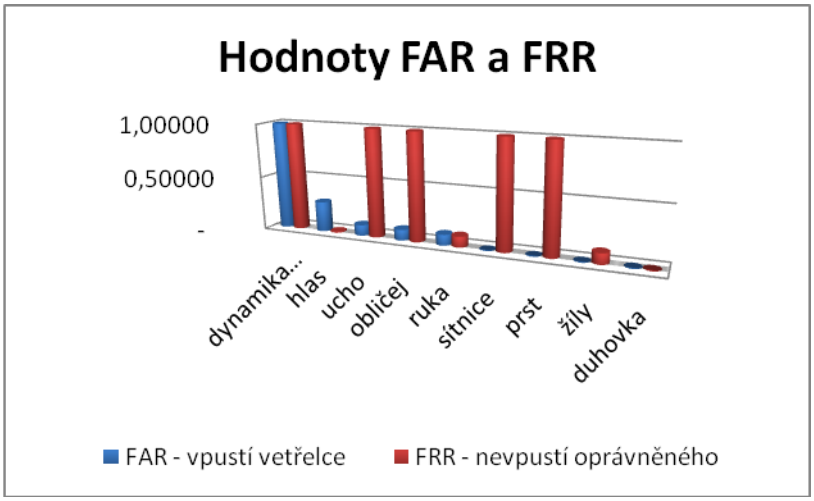
Vyskytuje se určité procento lití, pro které je tento systém nevhodný (pro konkrétní metodu) ze zdravotní, náboženských či etických důvodů, ovšem zde je možné vybrat jinou metodu identifikace. Nevhodnost metody se tedy vztahuje zejména na podepisování dokumentů a vzdálený přístup vzhledem k náročnosti zabezpečení nedůvěryhodných zařízení a přenosových cest.

5.3 Příklad použití biometrie

Biometrické systémy jsou zaváděny do systému bezpečnosti, ochrany majetku vždy na základě plánování ochrany osob a majetku jako preventivní činnost. Zásady preventivní činnosti je včasnost, rychlost, komplexnost, odbornost, permanentnost a součinnost [15]. Stěžejním údajem pro plánování zabezpečení je míra rizika jako podíl pravděpodobnosti a následku. Projektant tedy provádí analýzu rizik a navrhuje použití vhodných systémů právě na základě poměru pravděpodobnosti hrozby a výše možné následné škody v kontextu charakteristických vlastností konkrétního biometrického systému. Zohledňuje přitom hodnoty FRR a FAR, viz. tabulka a následný graf.

	FAR - vpustí vetřelce	FRR - nevpustí oprávněného
dynamika podpisu	1,00000	1,00000
hlas	0,28000	0,01000
ucho	0,10000	1,00000
obličej	0,10000	1,00000
ruka	0,10000	0,10000
sítnice	0,00100	1,00000
prst	0,00010	1,00000
žíly	0,00008	0,10000
duhovka	0,00078	0,00066

Tab. 1. Hodnoty FAR a FRR biometrických metod.



Obr. 17. Grafické znázornění tabulky 1.

Hodnoty FAR a FRR jsou výrobci uváděny spíše v ideálních hodnotách. Veřejně přístupné zdroje je uvádějí dosti rozdílně a v širokých rozptylech, nicméně i tak je z grafu patrná přesnost snímání. Uživatel se pak musí rozhodnout mezi upřednostněním FRR nebo FAR. Tedy bude-li tolerovat případného vetřelce nebo případné odmítnutí autentizacím systémem. Konkrétně u metody hlasu je zřejmé, že systém je oklamatelný, ale zamítnutí přístupu se vyskytne u jednoho z 10ti tisíce uživatelů. Na rozdíl od metody snímání krevního řečiště, která mnohem častěji nevpustí oprávněného, než že by systém vpustil vetřelce. Oprávněný uživatel může být rozladěn, ale pravděpodobnost, že do vyhrazeného prostoru vnikne vetřelec, je mizivá. Zařazení biometrický metod by pak mohlo vypadat následně.

pravděpodobnost události				
	vysoká	otisk prstu	biometrie duhovky, krevní řečiště	biometrie duhovky v kombinaci s dalšími metodami
	střední	snímání obličeje, snímání ruky	otisk prstu, snímání obličeje	otisk prstu v kombinaci s další metodou, biometrie duhovky
	nízká	dynamika podpisu, psaní na klávesnici, snímání hlasu	snímání ruky	biometrie duhovky , krevní řečiště
		nízká	střední	vysoká
		výše škody		

Tab. 2. Analýza biometrik

Tabulka je jen orientační, neboť jak již bylo uvedeno rozptyl co do kvality a ceny je značný a závisí na více faktorech.

5.4 Uplatnění biometricky v technických systémech SBS

Poplachové zabezpečovací systémy (IAS)

Slouží k detekování a indikaci přítomnosti vniknutí nebo pokusu o vniknutí do střeženého prostoru. Biometrické prvky nalezneme jako součást ovládacích zařízení zámků a spínačů, klávesnic či ovládacích nebo indikačních dílů ve formě kontaktní či bezkontaktní technologie. Dále lze na základě biometrických metod rozpoznávat obličeje, nebo jiné charakteristiky, a indikovat osoby vyskytující se v střeném prostoru.

Poplachové tísňové systémy (HAS)

Slouží k úmyslnému vyvolání poplachového stavu. Biometrii můžeme nalézt opět jako součást ovládacích zařízení, jako prvek sloužící k zpřístupnění vyvolání poplachu či jeho zrušení.

Přivolání pomoci (SAS)

Opět zpřístupnění vyvolání – odeslání zprávy o přivolání pomoci.

Uzavřené televizní okruhy (CCTV)

Slouží pro zabezpečení a dohled ve vymezeném prostoru. Kvalita dnes používaných kamerových systému; snímací, přenosové a vyhodnocovací techniky a technologie je na takové úrovně, že okruh je schopen na základě zadaných dat, požadavků či instrukcí vyhodnocovat výskyt osob, jejich pohyb, rozpoznávat nebezpečné chování osob nebo skupin osob dle výrazu či pohybu, tyto stavy signalizovat a zaznamenávat. Pokud systém vykonává akci, děje se tak na základě předem definovaných instrukcí. Proces je identifikační.

Systém kontroly vstupu (ACS)

Zde se biometrických systémů využívá nejčastěji. Jedná se převážně o systém verifikační autentizace, a to buď jednorázově k zpřístupnění vymezeného prostoru, nebo v návaznosti na další systémy docházkové a mzdové, zpřístupnění databází, odemykání dveří,

aktivování jiných technických prvků a techniky s návaznou režimovou kontrolou. Zvláštní kapitolou je vzdálený přístup, který může být výhradně softwarovou záležitostí.

Elektrická požární signalizace (EPS)

Elektrická požární signalizace je určena k trvalému střežení a stejně jako u některých předchozích bodů jsou biometrické systémy pouhou součástí ovládacích zařízení.

ZÁVĚR

Počítačově podporované technologie v oblasti SBS jsou propracovaným systémem sloužícím k přesnému, rychlému a automatickému procesu rozpoznávání identity člověka. Výstupem tohoto procesu je akce samotná, nebo jen indikace, jako upozornění na stav skutečnosti, dle předem stanovených kritérií.

Určujícím faktorem kvality technologie je jeho vhodná implementace do konkrétního prostředí při správně zvolených parametrech systému. Uživatel má na výběr celou řadu zařízení od firem nabízejících tyto technologie pro komerční využití a mimo zaměření na přístupové systémy, jsou i firmy orientující se na vývoj speciálních porovnávacích a vyhodnocovacích algoritmů, jiné na hardwarové snímače, případně samostatné čipy, další na speciální komprimační metody a podobně. Tato vyhraněnost dává možnost zkvalitňovat produkty a snižovat cenu. To vede k masovějšímu zavádění těchto technologií. Přínosem je také implementace biometrických prvků do samostatných zařízení, jako jsou počítačové jednotky, mobilní telefony a PDA, pokladny a trezorové skříně, dveřní zámky atd. Což má za následek akceptaci technologie jako takové u široké veřejnosti.

Za samostatnou kategorii můžeme považovat identifikaci ve vymezeném prostoru, jakým jsou nejen, prostory se zvláštním přístupem ve firmách a organizacích, ale také veřejné prostory nádraží, metro, letiště, obchodní centra, kde je potenciální hrozba spáchání teroristického útoku a ohrožení velkého počtu lidí. V neposlední řadě se biometrie využije i ve sportovních areálech při sportovních i kulturních akcích, e sledování chování davu, případně následné identifikace provokatérů. Střežení tohoto prostoru může být svěřeno do rukou SBS, ta pak využívá stávající kamerový a další technický systém a vyhodnocování je převážně softwarovou záležitostí.

Použití metody neuronových sítí ke zpracování nasnímaných dat je vzhledem k rostoucí rychlosti zpracování informací a rozšiřující se kapacitě paměti technologií budoucnosti. Navíc softwarové aplikace probíhají bez toho, aby si je identifikovaná osoba uvědomovala. Je pravděpodobné, že se tyto aplikace stanou běžnou součástí našeho každodenního života ve společnosti. Pak je třeba, ale jasně definovat legislativní rámec. Je zřejmé, že podnikatel či správce má povinnost a právo chránit svůj majetek a zdraví svých zaměstnanců, či zajistit bezpečnost občanům ve veřejných prostorách. Ale je na zvážení, zda permanentní sledování a zejména zaznamenávání všech údajů v daných prostorách o výskytu a chová

osob, není nad rámec daného práva. Problém není v technologii, schopné vyhodnocovat data a učit sama, ale ve zpětné vazbě. Parametry do systému zadává člověk, konečné rozhodnutí o případném zásahu vykonává také člověk, jaký člověk bude mít tedy pravomoc rozhodnout, co je v mezích standardního chování a co už ne? Které osoby budou mít přístup do takovýchto databází a jsme schopni je účinně chránit a spolehlivě likvidovat? Z těchto otázek vyplývá, že nejrizikovějším faktorem v celém systému je faktor lidský. Každopádně směr vývoje ukáže až budoucnost.

Prozatím se ukazuje, že dominantní technologií je a do blízké budoucnosti určitě stále bude snímán otisků prstů. Cenové relace snímačů se už začínají alespoň řádově blížit cenám bezkontaktních čteček, což jejich rozšiřování ještě více podpoří. Dá se tedy čekat, že se snímače otisků prstů budou díky klesajícím cenám, relativní uživatelské nenáročnosti a zvyšující se přesnosti i budoucích letech objevovat na místech, kde jsme byli zvyklí vídat jen standardní provedení kontaktních či bezkontaktních čteček [16].

Biometrické systémy jsou stále na vzestupu a i nadále můžeme očekávat jejich častější výskyt v každodenním životě, neboť jejich vývoj stále směřuje maximalizaci přesnosti, bezpečnosti a komfortu pro uživatele.

ZÁVĚR V ANGLIČTINĚ

Computer-based technology in the areas of private security services are the most elaborate system serving the accurate, rapid and automated the process of recognition of human identity. The output of this process is the action itself, or merely indications, as a warning to the status of fact, according to predetermined criteria.

The determining factor in the quality of the technology is its appropriate implementation in a particular environment when properly chosen parameters of the system. The user has the choice of a wide range of equipment from the companies offering these technologies for commercial use and out of focus to access systems, and companies dealing with the development of special comparison and evaluation of algorithms, the other on the hardware sensors, or separate chips, another special compression methods, and so on. This gives the possibility to improve products tailored nature and reduce the cost. This leads To will the introduction of these technologies. The benefit is also the implementation of biometric features into separate devices, such as computer drives, mobile phones and PDAs, the cash and safe-deposit boxes, door locks, etc. Resulting in the acceptance, of the technology as such.

A separate category can be identified within the defined area in which they are not only the premises with a special access in companies and organizations, but also the public areas of the metro station, airport, shopping malls, where is the potential threat of committing a terrorist attack and threat of a large number of people. Last but not least, the use of biometrics in the sports complexes in the sporting and cultural events, (e) monitoring of the behaviour of the crowd, where appropriate, the subsequent identification of themselves. Surveillance of this area may be entrusted to the hands of the private security services, it then uses the existing camera and other technological system and evaluation is primarily a software issue.

Application of the method of neural networks for processing of sampled data is the view of the increasing speed of information processing and the expanding memory capacity technologies of the future. In addition, the software applications are carried out without the person she is identified. It is likely that these applications will become a normal part of our daily life in society. Then it should be, but clearly define the legislative framework. It is clear that the entrepreneur or Manager has the obligation and right to protect its property and health of their employees, or to ensure the safety of citizens in the public areas. But it is to consider whether the permanent monitoring and, in particular, recording of all data in

these premises on occurrence and behavior of individuals, is not beyond the law. The problem is not technology, able to evaluate the data and the study itself, but in the feedback. Parameters of the system enters the man, the final decision about a possible intervention also carries out a man, what a man will have the power to decide what is within the limits of the standard of behaviour and what not? That person will have access to such databases, and we are able to effectively protect and reliably manage? Of these questions, be a factor in the whole system is the human factor. In any case, the direction of the development of the up.

For the time being it appears that the dominant technologies, and to the near future I will still be scanning fingerprints. The price session sensors are starting at least magnitude come contact-free readers, their spread even more support. We can therefore expect that the fingerprint will be thanks to falling prices, the relative user efficiency and increasing the accuracy and future years to appear in places where we've seen only the standard implementation of contact-free or contact smart card readers [16].

Biometric systems are still on the rise and continue to be, we can expect their more frequent occurrence in everyday life, as their development still seeks to maximize accuracy, safety and comfort for the user.

SEZNAM POUŽITÉ LITERATURY

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

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

[3] http://jorjaas.blog.cz/rubrika/kriminalistika-obory

[4] http://www.zld.cz/cinnost/vyvoj/biometrie/sni_opt.php?p=2|6|8|26|

[5] http://strade.fit.vutbr.cz/images/web/gallery/8565089430.jpg

[6] http://bio.sonixdesign.net/snimky/snimek3.html

[7] http://oreilly.com/catalog/dbnationtp/chapter/ch03.html

[8] http://www.securityinfo.cz/124/biometricke-systemy/

[9] http://newsletter.dipolnet.cz/dipol_tydenni_prehled_-_tv_a_sat_tv_cctv_wlan_inf_dipo_2009_14.htm

[10] http://www.viditelnypodpis.cz/2010/10/29/jak-se-podepisuje-digitalne-se-signosign/

[11] http://strade.fit.vutbr.cz/index.php?act=51&menu1=52&menu2=86

[12] http://www.mncr.cz/clanek/cestovní-doklady-s-biometrickymi-prvky-cdbp-aspx

[13] MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana.* 2., dopl. a aktualit. vyd. Praha: ASPI, 2008. 455 s. ISBN 978-80-7357-322-5.

[14] http://krajane.radio.cz/articleDetail.view?id=1943

[15] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* Vyd. 3 Zlín : Univerzita Tomáše Bati ve Zlíně, 2010.81 s ISBN 978-80-7318-889-4.

[16] *Perspektivní bezpečnostní technologie ochrany majetku : mezinárodní bezpečnostní konference : PYROS/ISET 2008 : Brno, 15. května 2008.* Ve Zlíně : Univerzita Tomáše Bati, 2008. 1 CD-R s. ISBN 978-80-7318-699-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D Dvojdimenzionální, zkratka označující popis prostoru dvěma rozměry.

3D Trojdimenzionální, zkratka označující popis prostoru třemi rozměry.

ACS Zkratka z anglického výrazu pro přístupové systémy.

CCD *Charge coupled device*, digitální světlocitlivý snímač.

CCTV Zkratka z anglického výrazu pro uzavřené kamerové systémy.

CMOS *Complementary metal oxide semicoductor*, digitální světlocitlivý snímač s jednoduchými obvody světlocitlivých buněk.

DNA Deoxyribonukleová kyselina.

EPS Elektrická požární signalizace.

ERR *Equal Error Rate*, míra rovné chyby.

EU Evropská unie.

FAR *False Acceptace Rate*, míra chybných přijetí.

FRR *False Reject Rate*, míra chybných odmítnutí.

FTIR *Fourier transform infrared spectroscopy*, spektroskopická metoda snímání.

HAS Zkratka z anglického výrazu pro poplachové zabezpečovací systémy.

IAS Zkratka z anglického výrazu pro poplachové tísňové systémy.

PDA *Personal digital assistant*, osobní digitální pomocník, malý kapesní počítač.

RFID *Radio Frequency Identification*, identifikace na rádiové frekvenci.

RSA Iniciály autorů Rivest, Shamir, Adleman, šifrovací algoritmus.

SAS Zkratka z anglického výrazu pro systémy přivolání pomoci.

SBS Soukromé bezpečnostní služby.

TFT *Thin-film transistor*, technologie účinku pole tranzistorů.

USB *Universal Serial Bus*, způsob připojení k PC technice.

WWW *World Wide Web*, celosvětová síť propojení počítačů.

ZOOU Zákon č. 101/2000 Sb., o ochraně osobních údajů.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK