# Využití biometrických prvků v zabezpečení motorových vozidel

The Use of Biometrics in Security of Motor Vehicles

Lukáš Marszalek

Bakalářská práce
2013



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

| | |
|---|---|
| Jméno a příjmení: | **Lukáš MARSZALEK** |
| Osobní číslo: | **A10566** |
| Studijní program: | **B3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **prezenční** |
| Téma práce: | **Využití biometrických prvků v zabezpečení motorových vozidel** |

Zásady pro vypracování:

1. **Seznamte se s problematikou biometrických systémů v oblasti zabezpečení motorových vozidel.**
2. **V teoretické části proveďte literární rešerši související s daným tématem (druhy a typy biometrických systémů využívaných v zabezpečení motorových vozidel, princip činnosti a jejich technická charakteristika).**
3. **V praktické části se zaměřte na využití biometrických systémů v zabezpečení motorových vozidel, interakci s ostatními technickými systémy.**
4. **Uveďte nové trendy v dané oblasti.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **RAK, Roman. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.**
2. **LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. London: World Scientific, c2012, xv, 500 p. ISBN 98-142-8784-9.**
3. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**
4. **BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.**
5. **ASHBOURN, Julian. Practical biometrics: from aspiration to implementation. London: Springer-Verlag, 2004, xiv, 159 s. ISBN 18-523-3774-5.**
6. **BOLLE, Ruud M. Guide to biometrics. New York: Springer Science Business Media, 2004, xxix, 364 s. ISBN 03-874-0089-3.**
7. **CHIRILLO, John. Implementing biometric security. Vyd. 1. Indianapolis: Wiley Publishing, 2003, 414 s. ISBN 07-645-2502-6.**


Vedoucí bakalářské práce: **Ing. Petr Navrátil, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

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

## ABSTRAKT

V této práci jsou prozkoumány technologie biometrických prvků s možností využití do zabezpečení vozidel. Jsou zde popsány jednotlivé metody ověřování identity a technologické principy. Dále jsou zde zmíněny metody klasického zabezpečení vozidel. V praktické části se nachází vlastní návrh na řešení zabezpečení vozidel pomocí biometrických prvků.


Klíčová slova: biometrické prvky, zabezpečení vozidel, biometrie, bezklíčový přístup


## ABSTRACT

In these work are defined principles of biometrics technology in a look of usage to vehicle security. There is a description of individual metods of authentification and technological metods. Also there is a mention of classical metods of vehicle security. In a practical part there is myself compilation for solution of usage biometrics technologies in vehicle security.


Keywords: biometrics technology, vehicle security, biometry, keyless system

Ve své práci bych chtěl poděkovat svému vedoucímu Ing. Petru Navrátilovi PhD. za trpělivost, kterou věnoval mému úsilí, odborné vedení a rady, které mi věnoval při zpracovávání bakalářské práce. Zároveň bych chtěl poděkovat svému spolubydlícímu za ohleduplnost zejména v závěru samotného psaní, kdy mi uvolnil prostory a zajistil tak potřebný klid.

**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 …….

podpis diplomanta

# OBSAH

# ÚVOD

Zabezpečení motorových vozidel je velmi obsáhlým a diskutovaným tématem. Každý rok se snaží výrobci v automobilovém průmyslu zajistit stále dokonalejší prvky zabezpečení, které by mohli nabídnout svým zákazníkům. Z těchto i jiných důvodu jsou do vývoje nových technologií směřovány nemalé částky. Výsledkem této snahy se na počátku tohoto tisíciletí objevili na trhu technologie biometrického ověřování identity.

Biometrické ověřování identity je samo o sobě velmi obsáhlým tématem a proto jsem se rozhodl zasvětit čtenáře této práce alespoň do základních poznatků jednotlivých využívaných metod. Postupným odhalováním kapitol by se čtenář v této oblasti měl seznámit se základními pojmy užívaným v kontextu s biometrií člověka a zároveň i definicí využívaných terminologií.

Obsáhlejším tématem jsou právě metodiky biometrického snímání charakteristických rysu zkoumaného objektu zájmu. Hlavním cílem je stanovit teoreticky využitelné metody pro aplikaci v zabezpečení vozidel. I když je nutno dodat, že některé z metod jsou představou blízké či vzdálené budoucnosti a to především s ohledem na vývoj soudobých technologií a hardwarových prvků. Tyto aspekty značně limituji samotný postup zavádění inteligentního systému ovládání a zabezpečení vozidel, ale i v jiných oblastech lidského života.

V nemalé části této práce jsem se zaměřil na technologie, které jsou v současné době využívané k ochraně motorových vozidel i majetku, který je v nich přechováván. Při definici běžných měřítek je primárním požadavkem mechanické zabezpečení. Toto řešení je rozebráno v různých aspektech, které jsou využívány samotnými výrobci vozidel i společností specializovaných do oblasti zabezpečení. Dále jsou představeny pokrokovější metody v oblasti elektronického zabezpečení a moderní technologie v souladu s požadavky na zvyšování komfortu koncového zákazníka.

Z praktického pohledu této práce jsem se zaměřil především na zpracování vlastní představy o směru vývoje biometrických prvku a jejích aplikace do zabezpečení motorových vozidel. To vše především s ohledem na parametry současně využívaných systémů.

# I. TEORETICKÁ ČÁST

# 1 POJMY SPOJENÉ S IDENTIFIKACÍ OSOB

## 1.1 Identita

Identitu též můžeme nahradit českým slovem totožnost. Tento pojem používáme za účelem srovnání s jiným objektem nebo s tím samým objektem na základě známých údajů. Identitu lze tedy pojmout jako soubor údajů, který slouží k jednoznačnému určení.

Identitu osoby definujeme jako soubor specifických biologických a psychických vlastností.

**Biologickou identitu** můžeme stanovit jako kombinaci vrozených a získaných charakteristik z hlediska fyziologických znaků a anatomických parametrů, které jsou však nezávislé na myšlení zkoumaného jedince. Mezi vrozené charakteristiky můžeme zařadit například DNA nebo otisky prstů, které se po celý život nemění.[1]

**Psychologickou identitu** chápeme jako uvědomělé vlastnosti v lidském chování a charakteristické rysy jeho projevů. Psychologická identita se mění nejsnáze a nejčastěji v závislosti na vývoji člověka při přechodu mezi jednotlivými životními fázemi, kterými chápeme například pubertu. Dalšími faktory, které přispívají ke změně, mohou být mimořádné události a životní zkušenosti.[1]

Identitu mnohdy spojujeme s pojmem osobnosti, tedy souborem vnitřních psychologických pochodů, které určují základní znaky chování jedince. Osobnost jedince se vyvíjí v závislosti na okolnostech, ve kterých se vyskytuje. Mezi tyto okolnosti můžeme řadit i sociální prostředí. V každém sociálním prostředí se projevují jisté zvyklosti a charakteristické kulturní znaky.

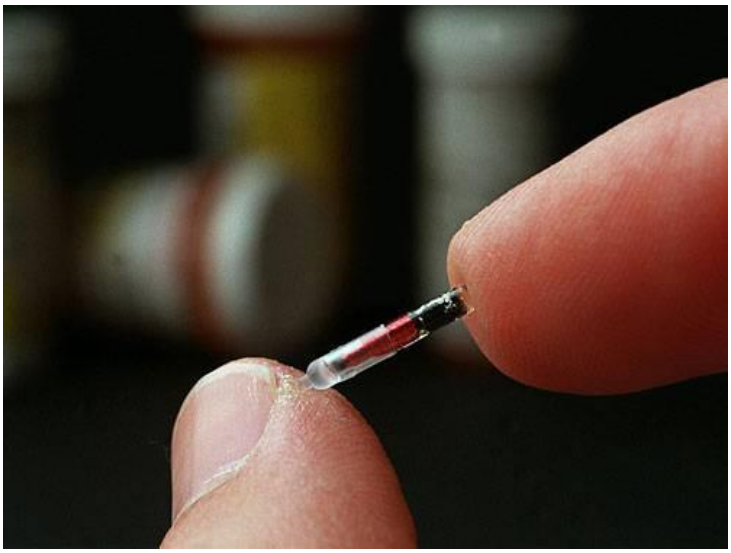
Pro účely kriminalistiky a bezpečnostně-komerčních aplikací je nutno vyčlenit takové znaky identity, které jsou snadno rozpoznatelné a v čase se relativně nemění.[1]

## 1.2 Vlastnictví

Jednou z možností identifikace osob, je pomocí vlastnictví specifických identifikátorů určujících totožnost, jako takové můžeme chápat například doklady totožnosti. Tyto identifikační charakteristiky musí splňovat podmínku jednoznačného určení identity držitele, avšak je zde vysoká míra nebezpečí zcizení, falsifikování a v některých případech přenositelnosti. [1]

Jako identifikační charakteristiku (identifikátor) můžeme považovat:

- Jméno
- Doklady totožnosti
- Jiné doklady (např. rodný list)
- Identifikační kódy nebo čísla (telefonní číslo, rodné číslo,…)
- Karty a čipy
- Klíče (např. bezpečnostní schránky v bankách)
- Podkožní RFID čipy



Obrázek 1: Podkožní RFID čip[2]

## 1.3 Znalosti

Znalosti patří mezi nejzákladnější formu identifikace. Každý člověk vědomě i podvědomě schraňuje informace o charakteristikách známých osob a věcí, stejně tak jako informace o své minulosti. Pro bezpečnostní účely má v paměti individuální znalosti o vlastněných identifikačních údajích. Mezi ty řadíme osobní údaje a přístupové hesla (identifikační kódy).

Hesla můžeme rozdělit na statická a dynamická. Nejčastěji se v dnešní době využívají hesla statická, která vytváříme na základě specifických znalosti nebo jako náhodně generované kódy. Dynamická hesla jsou proměnná na základě stanoveného algoritmu. Mohou mít různé závislosti, např. na čase nebo místě. Mnohdy se používají speciální hardwarové prvky, které slouží ke kalkulaci požadované hodnoty.[1]

# 2 POJMY V BIOMETRII

K pochopení problematiky je zapotřebí definovat základní pojmy spojené s tímto vědním oborem. Mezi ty hlavní patří:

- **Biometrie**
  Je věda, která zkoumá živé organismy z pohledu jeho fyziologických vlastností, anatomických parametrů nebo projevů chování.
- **Biometrika**
  Je vědou o metodách rozpoznávání člověka, na základě biologických údajů nebo behaviorálních vlastností.
- **Autentizace**
  Je proces založený na zjištění a porovnání charakteristik vztažných k ověřovací metodě. Výsledkem je automatizované určení identity uživatele.
- **Identifikace**
  Je proces ověření údajů předem nedefinovaného uživatele. Způsob srovnání je tedy jedna k mnoha. To znamená, že systém porovnává získané údaje s celou databází uživatelů.
- **Verifikace**
  Je proces ověření vstupních údajů na základě definované totožnosti a očekáváného výsledku. Výsledkem je přijetí nebo zamítnutí požadavku. Způsob srovnání je jedna k jedné. To znamená, že systém porovná pouze záznamy k definované identitě.

## 2.1 Biometrický etalon

Ke správnému ověřování je zapotřebí definovat soubor charakteristik nebo vlastností, které mají byt vyhledávány, referenční vzor, který pro účely biometriky budeme nazývat biometrickým etalon. Tento vzor je zapotřebí uložit do systému a k eliminaci možného výskytu chyb je zapotřebí ho nasnímat vícekrát, aby údaje byly pořízeny jednoznačně. Výsledný vzor je tedy zprůměrovanou hodnotou těchto snímání. Referenční vzor musí mít jistou kvalitu, tedy jistý počet zaznamenaných charakteristických znaků. O správném přijeti vzoru indikuje přímo čtecí zařízení nebo software, který se čtecím zařízením komunikuje. Za použití verifikace je nutné ke vzoru připojit identifikátor, který slouží k pozdějšímu nalezení v databázi.[5]

Etalon ukládáme:

- **Ve čtecím zařízení**

  Hlavní výhodou je rychlost zpracování a nezávislost na externích zdrojích i procesech. Nevýhodou pak vysoká míra zranitelnosti, závislost na funkčnosti daného prvku a nutnost přenosu etalonů na každé čtecí zařízení samostatně nebo opětovnou tvorbou vzoru.
- **V centrální databázi**

  Výhodou je dostupnost vzoru pro kterékoliv zařízení skrze datovou komunikaci a bez nutnosti provádění změn na jednotlivých ověřovacích prvcích. Nevýhodou je nefunkčnost při výpadku datové komunikace, proto je více zapotřebí zabezpečit alternativní přístup.
- **Na přenosných jednotkách (tokeny, čipové karty)**

  Jedná se o složité a cenově nákladné systémy. Uživatel si nosí svůj biometrický etalon a sebou, tedy není potřeba žádného centrálního nebo lokálního ukládáni. Tato výhoda je zároveň nejzranitelnějším místem systému, protože identifikační prvek může být zcizen, znehodnocen nebo upraven za účelem zneužití.
- **Kombinovaně**

  Tato varianta klade důraz na eliminaci nevýhod jednotlivých samostatných řešení.

## 2.2 Biometrická autentizace

Je založena na principu jedinečných tělesných charakteristik nebo znaků v chování určitého jedince, které slouží k jednoznačné identifikaci. Důraz je kladen na relativní stálost a neměnnost těchto znaků. Hlavní výhodou je praktičnost těchto metod ověřování, protože každý své biometrické údaje „nosí“ stále sebou. Relativní výhodou je poměr bezpečnosti a ceny, v závislosti na použité metodě. Praktické využití nacházíme především u přístupových systémů, kvůli jednoznačné identifikaci a nezcizitelnosti identity. V současné době je kladen důraz na implementaci těchto metod zejména do prostor s vysokými požadavky na bezpečnost, jako jsou například prostory celní kontroly na letištích nebo ve vojenských objektech.[6]

## 2.3 Měření výkonnosti

Výkonnost biometrických systémů hodnotíme na základě údajů o schopnosti správně rozlišovat charakteristické znaky vztažné k ověřovanému vzoru. Výsledkem je pravděpodobnost přijetí nebo zamítnutí uživatele.[7]

### 2.3.1 FAR (False Acceptation Rate)

V překladu pravděpodobnost chybného přijetí, je mírou přijetí neoprávněného uživatele. Pro biometrické prvky je podstatné eliminovat možnost zkreslení a následné záměny identity. Pro účely zabezpečení je pak důležité zamezit přístupu pomocí falsifikátů biometrických údajů, jako například fotky otisku prstu nebo obličeje. Lze vyjádřit, že FAR je chybným ztotožněním jiné osoby.

FAR můžeme definovat pomocí vzorců:[1]

$$FAR = \frac{N_{FA}}{N_{IIA}} \tag{2.1}$$

$$FAR = \frac{N_{FA}}{N_{IVA}} \tag{2.2}$$

Kde:

$N_{FA}$ – Number of False Acceptation (počet chybných přijetí)

$N_{IIA}$ – Number of Impostor Identification Attemps (počet pokusů o neoprávněnou identifikaci)

$N_{IVA}$ – Number of Imposter Verification Attemps (počet pokusů o neoprávněnou verifikaci)

### 2.3.2 FRR (False Rejection Rate)

V překladu pravděpodobnost chybného zamítnutí, je mírou zamítnutí oprávněných osob při pokusu o ověření identity. U komerčního využití tato problematika snižuje míru komfortu, vzhledem ke skutečnosti, že je uživatel nucen se opětovně vystavovat pokusu o ověření identity. Tím zároveň klesá důvěryhodnost metodiky daného produktu. Ve sféře bezpečnostních složek státu je ale nutno brát v potaz, že chybné vyřazení osoby může zprostředkovat možnost úniku pachatele před spravedlností.[1]

FRR můžeme definovat pomocí vzorců:[1]

$$FRR = \frac{N_{FR}}{N_{EIA}} \tag{2.3}$$

$$FRR = \frac{N_{FR}}{N_{EVA}} \tag{2.4}$$

Kde:

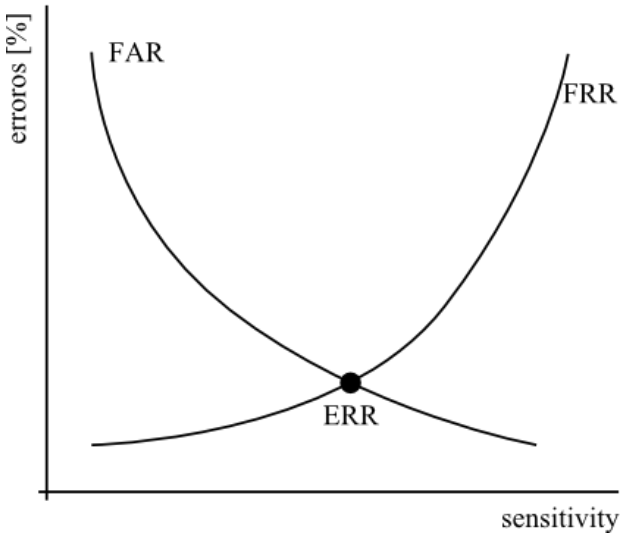
$N_{FR}$ – Number of False Rejection (počet chybných přijetí)

$N_{EIA}$ – Number of Enrolle Identification Attemps (počet pokusů oprávněnou osobou o identifikaci)

$N_{EVA}$ – Number of Enrolle Verification Attemps (počet pokusů oprávněnou osobou o verifikaci)

### 2.3.3 EER (Equal Error Rate)

Jedná se o bod, ve kterém se křivky pravděpodobnosti chybných přijetí a zamítnutí protínají. V praxi slouží pouze k porovnání vlastností jednotlivých aplikací a zároveň znázorňuje závislost počtu chyb na nastavení citlivosti. EER stanovuje pomyslnou hranici využití, kdy klesající mírou citlivosti je aplikace vhodná k užití ve forenzních vědách a naopak při stoupající citlivost roste komfort při užití v komerčních aplikacích.[1]




Obrázek 2: Vztah mezi FRR a FAR[8]

### 2.3.4 Vícenásobné ověření

Vícenásobné ověření biometrickými metodami nasazujeme tam, kde je zapotřebí zvýšení bezpečnosti a naprostá jednoznačnost oprávnění k přístupu ověřované osoby. Zpravidla se jedná o prostory s utajovanými informacemi nebo místa kde se takovéto informace mohou vyskytovat. V současné době však můžeme postřehnout i tento způsob ověřování u automatizovaných bran celní kontroly na letištích. Kvůli uživatelskému komfortu se využívá nejčastěji ověření otisku prstů a obličeje. Můžeme však naleznout i systémy, které kombinují například hlasovou analýzu nebo skenování sítnice s jinými metodami získávání údajů, zpravidla však s jinými než biometrickým ověřováním.

Pravděpodobnost FAR se dosazuje do vzorce v součinu prvku všech dílčích pravděpodobnosti jednotlivých ověřovacích metod.[9]

$$FAR_C = FAR_1 * FAR_2 * \ldots * FAR_n \tag{2.5}$$

Kde:

$FAR_c$ – Celková pravděpodobnost chybného přijetí

$FAR_n$ – Dílčí pravděpodobnost chybného přijetí

Pravděpodobnost FRR se dosazuje do vzorce v součtu prvku všech dílčích pravděpodobnosti jednotlivých ověřovacích metod.[9]

$$FRR_C = FRR_1 + FRR_2 + \cdots + FRR_n \tag{2.6}$$

Kde:

$FRR_c$ – Celková pravděpodobnost chybného zamítnutí

$FRR_n$ – Dílčí pravděpodobnost chybného zamítnutí

# 3 PRINCIPY A TECHNOLOGIE BIOMETRICKÝCH PRVKŮ

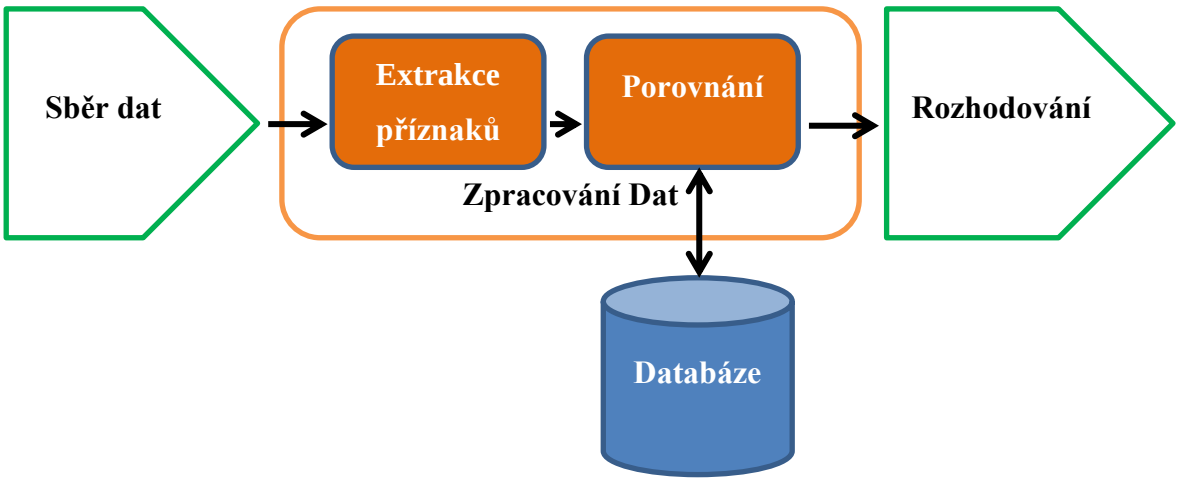
Metodiku jednotlivých biometrických prvků můžeme rozdělit do dvou základních skupin, v závislosti na druhu ověřovaných dat, na:

- **Biologické metody**
- **Behaviorální metody**

## 3.1 Obecný princip

Všechny biometrické metody používají zobecněného postupu pro ověřování nebo vkládání údajů. Nejprve vložíme vzorek ke zpracování, kterým chápeme například otisk prstu, snímek obličeje nebo zvukovou stopu. Tento vzorek následně zpracujeme tak, že v něm určíme charakteristické rysy. Z těchto charakteristických rysu se určí markanty, tedy biometrické identifikátory, které slouží k rozpoznání identity a neobsahují nepodstatné charakteristiky. Mezi těmito markanty se určí souvislosti, které jsou specifické pro danou identitu a vytvoří se z nich šablona (vzorec), který ukládáme do databáze v podobě číselné identitu a vytvoří se z nich šablona (vzorec), který ukládáme do databáze v podobě číselné matice. V závislosti na režimu daného prvku, dochází ke srovnání šablon nebo k ukládání biometrického etalonů.[1]

Biometrické systémy zpravidla pracuji ve dvou režimech. V registračním režimu dochází k získání biometrických dat za účelem vytvoření biometrického etalonů. V autentizačním režimu dochází k samotnému procesu ověřování identity v závislosti na funkčnosti a účelu zařízení.[5]




Obrázek 3: Obecný princip biometrických prvků

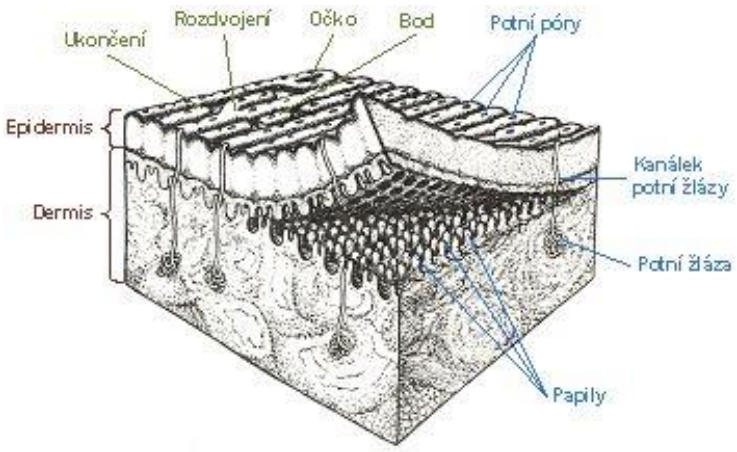
## 3.2 Biologické metody

Tato metodika je založena na principu ověřování fyziologických charakteristik nebo anatomických znaků příznačných pro identifikovaného jedince. Tyto údaje jsou zpravidla relativně neměnné.[5]

### 3.2.1 Otisky prstů

Posuzování otisků prstů (daktyloskopie) slouží jako jedna z nejstarších a nejpoužívanějších metod k biometrickému ověření identity. Základem je vrásnění pokožky, na dlaních a chodidlech, do útvarů, kterým říkáme papilární linie. Biologický účel tohoto zvrásnění, je vývojem dán, aby zabránil prokluzovaní předmětu z rukou nebo uklouznuti na kluzkém povrchu.[1]

Papilární linie tvoří celý povrch svrchní pokožky a obnovují se do původních tvarů i po jejím zbroušení. Jejich průměrná výška je mezi 0,1 až 0,4 mm a šířka mezi 0,2 a 0,7 mm.

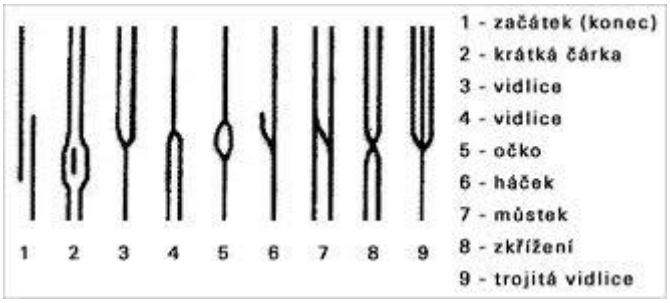



Obrázek 4: Pokožka s papilárními liniemi[10]

Pro kriminalistické a bezpečnostní účely je podstatná tvorba specifických sekvencí obrazců v papilárních linií. Obraz papilárních linií je relativně neměnný po celý život, výjimkou jsou jizvy nebo úplné odstranění svrchní pokožky, a pro každého člověka jiný. Dočasně poškodit papilární linie může taky kožní onemocnění nebo povrchové zranění.[10]

Snímání otisku prstu může probíhat kontaktním a bezkontaktním způsobem v závislosti na použité technologii. Snímání dále může rozdělit na statické a snímání šablonováním. Statické snímání vytváří obraz celého otisku najednou. Nevýhodou je, v případě kontaktního snímače, zanechání celého otisku na snímači. U šablonování dochází ke skládání obrazu z více snímků, proto je nutno po snímači prstem přejíždět, zároveň však za sebou mažeme samotný otisk zanechaný na snímači.[5]

Při ověřování otisků prstu se zaměřujeme na několik základních typů markantů (Obrázek 5).




Obrázek 5: Typy markantů otisku prstů[11]

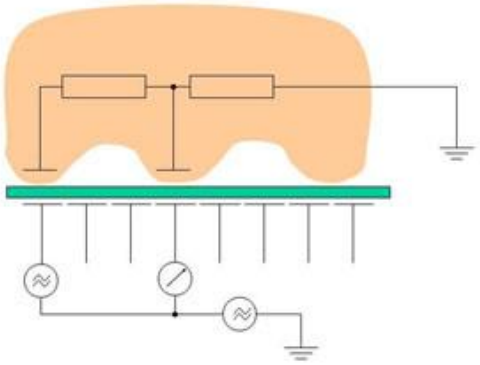
Tabulka 1: Pravděpodobnost chyb a rychlost snímání otisků prstů[5]

| | |
|---|---|
| FRR | < 1 [%] |
| FAR | 0,0001 – 0,00001 [%] |
| Rychlost verifikace | 0,2 - 1 [s] |
| Spolehlivost | vysoká |

#### *3.2.1.1 Kapacitní snímač*

Tyto snímače pracují na principu rozdílů kapacity mezi pokožkou a deskou snímače. Papilární linie, které jsou v kontaktu s tenkou vodivou plochou, zvyšují kapacitu na elektrodách, schovaných pod ní. Každá elektroda pak vyšle signál ke zpracování na sběrnici, skrze kterou se generuje digitální obraz. Kapacitní snímače pracují výhradně jako kontaktní prvky.[12]

Kapacitní snímače jsou malých rozměrů, mají jednoduchý princip funkčnosti a dosahují vysokých kvalit za nízkou pořizovací cenu. Mezí hlavní patří krátká životnost, citlivost na znečištění pokožky a možnost znehodnocení vlivem statické elektřiny.[12]



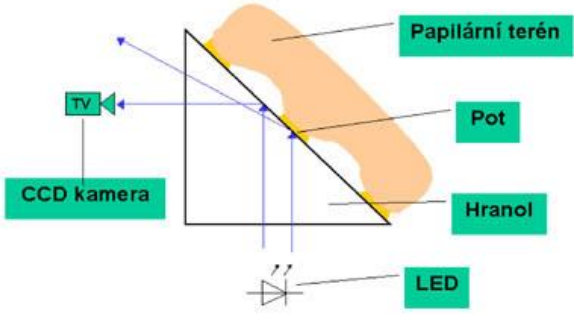
Obrázek 6: Schéma kapacitního snímače[13]

#### *3.2.1.2 Optický snímač*

Optické snímače pracují na principu odrazu světla na papilárních liniích, který zaznamenáváme na CCD čip, podobně jako u fotoaparátů. CCD čip se skládá z mikroskopických fotodiod a tranzistorů. Světlo odražené od papilárních linií vyvolá na čipu excitovaný stav elektronů a ty přenesou výboj na výstup. Rýhy světlo neodráží.

Tyto snímače jsou zpravidla nejpoužívanější, kvůli vysoké životnosti a spolehlivosti. Mezi další přednosti patři možnost snímání bezkontaktně, tedy stačí přiložit prst dostatečně blízko povrchu snímače bez nutnosti doteku, což zvyšuje bezpečnost, protože nikde nenecháváme své otisky. Snímače jsou vysoce odolné proti elektrostatickému rušení.

Nevýhodou této technologie je citlivost na znečištění pokožky, které způsobuje zkreslení a následně špatné vyhodnocení. Dalším limitujícím faktorem bývají větší rozměry, které nás limituji při použití v přenosných zařízeních.[12]

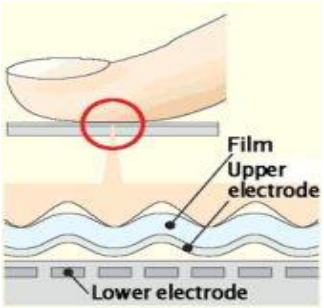



Obrázek 7: Schéma optického snímače[13]

#### *3.2.1.3 Tlakový snímač*

Snímač se skládá ze tří vrstev. První vrstva je krycí a deformovatelná. Pod ní je schovaná piezoelektrická vrstva, která se deformuje společně s vrstvou krycí a vyvolá statický náboj. Statický náboj zachycuje poslední vrstva elektrod, které slouží jako jednotlivé pixely obrazu.[14]

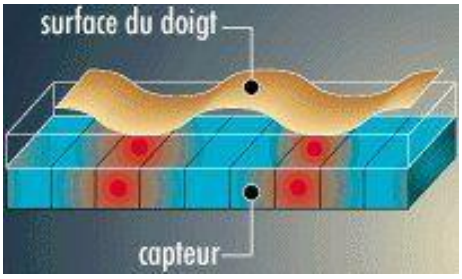
Druhou variantou tlakových snímačů je využití mikrospínačů o velikosti 50 µm. tato technologie je však velmi nákladná a nespolehlivá vlivem častého poškození a opotřebení spínačů, které zastupuji jednotlivé pixely ve výsledném digitálním obrazu.[14]




Obrázek 8: Princip tlakového snímače[14]

#### *3.2.1.4 Teplotní snímač*

Teplotní snímače se skládají z miniaturních teplotně citlivých detektorů, které snímají rozdílné teploty mezi papilárními liniemi a prázdným prostorem mezi nimi. Zpravidla bývá nutnost po detektoru prstem pohybovat, aby třením vznikalo dostatečné teplo. Proto tyto snímače pracují sekvenčně a obraz dopočítávají z jednotlivých snímků plochy. Na tomto faktu je stanovena nízká kvalita a častá chybovost těchto prvků. Další problematickou části je nutnost nasazovat komplikované algoritmy. Výhodou je relativní cenová nenáročnost a malé rozměry.[12]




Obrázek 9: Princip teplotního snímače[14]

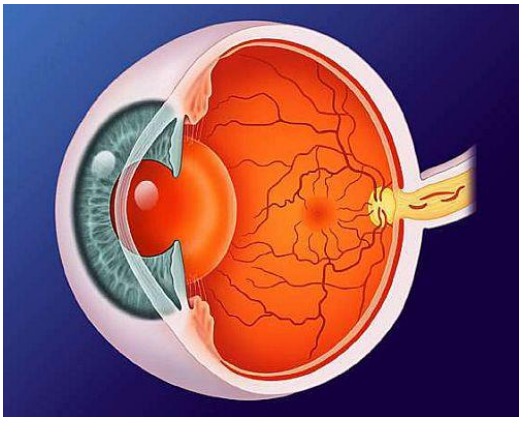
### 3.2.2 Očí

#### *3.2.2.1 Sítnice oka*

Sítnice je na vnitřní straně zadní stěny oční bulvy. Obsahuje tyčinky, čípky, nervová zakončení a cévy. Na oční sítnici lze pozorovat jedinečné rozložení očních cév u každého jedince. Rozložení cév se však v průběhu života mění. Tato technologie vychází původně z lékařských přístrojů, které byly prostorově náročné.[15]

Ke snímání je využíváno infračerveného koherentního paprsku světla. Je zapotřebí, aby testovaný subjekt setrval ve stabilní pozici blízko snímače, což snižuje komfort, a nesmí nosit brýle. Kontaktní čočky u kvalitních systému nezpůsobují potíže. Paprsek nasnímá obraz, který je následně přečištěn pomocí filtrů k odstranění šumu a zvýšení kontrastu.

Mezi hlavní výhody tohoto systému patří rychlost ověření a vysoká přesnost určení. Tyto vlastnosti zajišťují užití pro stupeň nejvyššího zabezpečení. Nevýhody systému představuje délka snímání vzorku, uživatelský komfort a relativně stálé okolní prostředí, což vylučuje možnost využití ve venkovních podmínkách.[7]



Obrázek 10: Znázornění cév na oční sítnici[16]

Tabulka 2: Pravděpodobnost chyb a rychlost biometrie sítnice[5]

| | |
|---|---|
| FRR | < 1 [%] |
| FAR | 0,0001 – 0,00001 [%] |
| Rychlost verifikace | 0,2 - 1 [s] |
| Spolehlivost | vysoká |

#### *3.2.2.2 Duhovka*

Oční duhovka se u člověka formuje v posledním trimestru těhotenství a drobné změny ve struktuře lze ještě sledovat v prvních měsících od narození dítěte. V dalších fázích života už zůstává neměnná. U každého člověka je uspořádáni charakteristických znaků unikátní a to i v případě jednovaječných dvojčat. Tato teorie byla i matematicky dokázána.[15]

Duhovka obsahuje charakteristické obrazce, různé nedokonalosti, jako jsou třeba rýhy, zakřivené čáry nebo pigmentové skvrny. Oko je nasnímáno kamerou s čipem CCD přes monochromatický infračervený filtr. Algoritmus rozčlení signifikantní znaky a zaznamená jejich polohu. Kulatý tvar duhovky napomáhá ke zjednodušení algoritmizace a urychluje celý proces. Snímaný obraz je zapotřebí rozložit na fázové a amplitudové informace, protože ke zpracování se používají pouze fázové údaje.

Toto ověření je rychlé a komfortní pro uživatele, bez nutnosti setrvávat ve speciální poloze, prakticky stačí pohlédnout zpříma do objektivu. Mezi hlavní nevýhody však patří náchylnost na osvětlení v prostoru. Tyto systémy jsou rovněž velmi náchylné na oklamání pomocí fotografie, protože nezaznamenávají prostorový obraz.[7]

Obrázek 11: Znázornění snímání oční duhovky[17]

Tabulka 3: Pravděpodobnost chyb a rychlost biometrie duhovky[5]

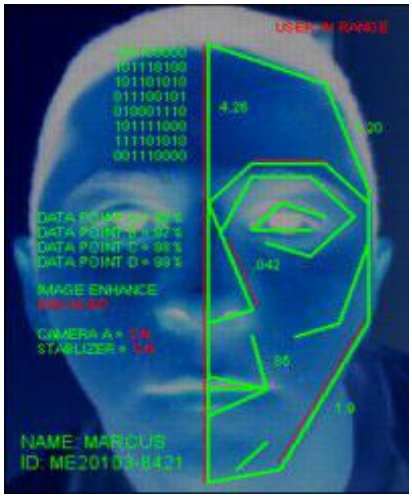
| | |
|---|---|
| FRR | < 1 [%] |
| FAR | 0,00078 [%] |
| Rychlost verifikace | 2 [s] |
| Spolehlivost | vysoká |

### 3.2.3 Geometrie obličeje

Lidský obličej obsahuje charakteristické a relativně neměnné údaje, stanovené strukturou lebky a uchycením mimických svalů. Systémy určují vzdálenosti mezi jednotlivými záměrnými body, jako jsou ústa, oči, nos a nadoční oblouk. Výchozími hodnotami jsou pak rozměry a úhel spojnic mezi těmito stanovenými body. V dvoudimenzionálním (2D) snímání jsou to dostačující charakteristiky k doplnění portrétů a zanesení markantů do biometrického etalonu. 2D technologie lze snadno obelhat například pomocí fotografie. V případech kdy se využívá prostorových (3D) technologií je zapotřebí zaznamenat pohled minimálně ze dvou kamer. Z výsledných obrazů se diferenciálně dopočítají prostorové vzdálenosti na základě algoritmu a vytvoří se prostorová síť rýsující tvary obličeje. [12]

Pro účely získávání charakteristik pohybující se osoby slouží dynamické systémy snímání obličeje. Ty se dnes používají například na letištích v některých zemích nebo ve vymezených vládních budovách. Problematickými jevy bývají špatné světelné podmínky a pozice kamery vůči rozpoznávanému objektu, které zneschopňují možnost identifikaci a to zejména pokud se osoba pohybuje v davu. Užití těchto systému je na našem území prakticky nemožné vzhledem k platné legislativě.[1]

Pro účely přístupových systému se využívají statické systémy, tedy uživatel přímo a úmyslně pohlédne do kamery za účelem ověření identity. V těchto případech odpadají rizika špatného nasvětlení scény nebo nedostatku informaci vlivem neúplného snímku. Pro vlastní realizaci pak postačí obyčejná webová kamera a rozpoznávací software. Z toho plynou hlavní výhoda užití těchto systémů a těmi je technická nenáročnost.[5]




Obrázek 12: Snímání geometrie obličeje[18]

Tabulka 4: Pravděpodobnost chyb a rychlost snímání geometrie obličeje[5]

| | |
|---|---|
| FRR | < 1 [%] |
| FAR | 0,1 [%] |
| Rychlost verifikace | 3 [s] |
| Spolehlivost | střední |

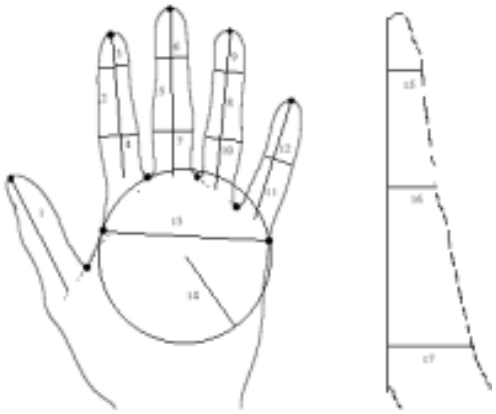
### 3.2.4 Geometrie ruky

Tvar lidské ruky a zakřivení jednotlivých prstů je z určitého hlediska jedinečnou identifikační charakteristikou každého člověka. Pro účely ověření se určuje délka, šířka a tloušťka každého prstu jedné ruky. Tyto charakteristické rysy se v průběhu stárnutí relativně nemění. Ovlivňujícím faktorem změny může být jemná změna tloušťky při změnách klimatického období nebo úraz. Při získávání charakteristik je ignorována délka nehtu. Jedná se o jednu s prvních komerčně užitých technologii vůbec.[1]

Možnosti snímání obrazů jsou dvě. První variantou, je přímí snímek pomocí kamery vybavené CCD čipem. Druhá varianta je realizována pomoci soustavy zrcadel, což umožňuje zmenšení rozměru celého zařízení i trojrozměrné zobrazení. Moderní snímače jsou schopny identifikovat až stovky identifikačních bodů během krátkého časového intervalu, zpravidla během jediné sekundy. K biometrickému etalonu je zapotřebí přidat identifikátor, protože tyto systémy nedosahují takových kvalit, aby je bylo možné použít jiným než verifikačním způsobem. Jako podkladové plochy využíváme matný materiál, aby byl zajištěn vysoký kontrast obrazu.[1]

Při skenování jsou snímány pouze obrysy jednotlivých prstů a dlaně. Rozlišení není zdaleka tak přesné, aby bylo schopno zachytit a rozeznávat otisky prstů. Ukládána data jsou ve formě pozic a délek spojnicových přímek. Tyto přímky pak slouží ke generování obrysu.[19]

V reálném komerčním prostředí se tyto systémy používají především pro rychlé přístupové systémy.[1] Z pohledu zabezpečení vozidel, rychlost ověření, může být žádanou vlastností, v případě umístění snímače do dveřní kliky u vozidla.



Obrázek 13: Znázornění snímaných charakteristik geometrie ruky[19]

Tabulka 5: Pravděpodobnost chyb a rychlost snímání geometrie ruky[5]

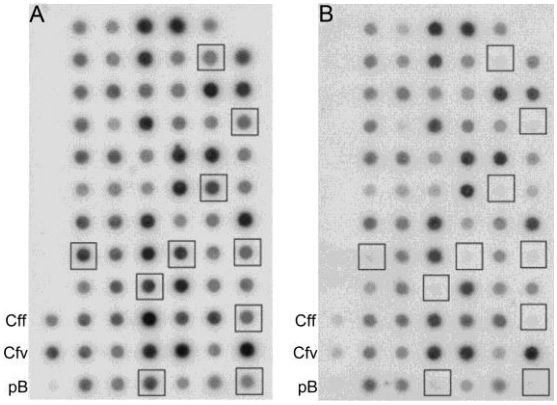
| | |
|---|---|
| FRR | < 0,1 [%] |
| FAR | 0,1 [%] |
| Rychlost verifikace | 1-2 [s] |
| Spolehlivost | střední |

### 3.2.5 DNA

Základem metodiky je skutečnost, že dva lidé nemohou mít totožné genetické informace a to ani v případě, že se jedná o rodinného příslušníka, v takovém případě dochází pouze k částečné shodě i v případě jednovaječných dvojčat. Existují specifické znaky ve struktuře DNA, které můžeme definovat jako určující charakteristiky, markanty. Na základě těchto signifikantních znaků jedince, lze s naprostou spolehlivostí ověřovat identitu, pro účely forenzní kriminalistiky a komerčních aplikací. [1]

DNA obsahuje řetězce 4 základních nukleotidů, které tvoří různě poskládané páry. Na základě uspořádáni do páru a orientace ve vzorci uspořádání do šroubovice, lze charakterizovat jedinečnost genomu. Tyto jedinečné znaky jsou však obsaženy pouze v 5% z celého genomu, v takzvaných variabilních pozicích. Tyto pozice určují charakteristické rysy jedince, jako jsou například barva očí, vlasu, pleti a taky náchylnost k onemocněním. Úprava genetického kódu není technologický možná, a proto je tato metoda naprosto bezpečná. [1]

Z důvodů urychlení procesu se v komerčních aplikacích používá pouze verifikačního procesu ověřování DNA. Tato metodika je velmi přesná, ale velmi nepohodlná vzhledem ke skutečnosti, že vyžaduje odběr biologického vzorku ověřované osoby. Dalším problémem je soudobá časová náročnost při ověřování. Dnešní technologie umožňují zpracování vzorku v řádech minut. Pro tuto skutečnost je tato metoda nepoužitelná pro přístupové systémy. Do budoucna je však nutné s touto metodou počítat kvůli vysoké míře spolehlivosti.[12]




Obrázek 14: Znázornění charakteristických rysů v DNA[20]

## 3.3 Behaviorální metody

Tato metodika je založena na principu rozpoznávání charakteristických znaků v chování, které určují fyziologické parametry nebo návyky vytvořené na základě životních zkušenosti a taky začlenění ve společnosti. Tyto vlastnosti musí být vybírány tak, aby nebyly napodobitelné. Velkou nevýhodou může být relativně častá změna v závislostech na prostředí, ve kterém se jedinec pohybuje. [5]

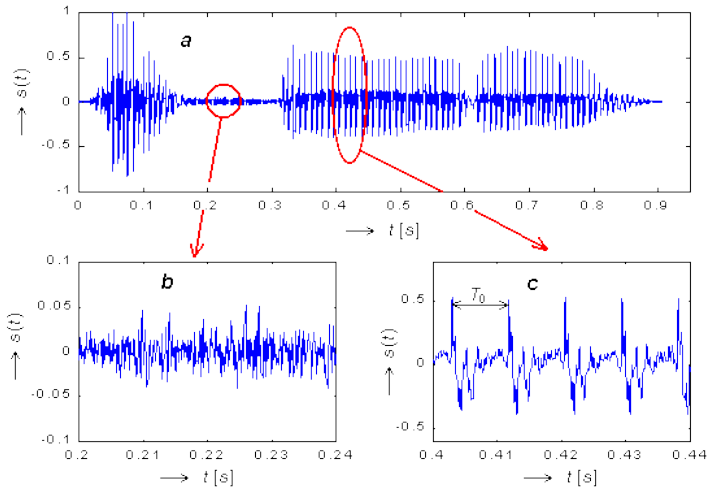
### 3.3.1 Hlasová analýza

Hlasový projev vzniká prouděním vzduchu z plic skrze ústní trakt. Rozdílnost ústního traktu zaručuje, dostatečně individuální charakteristiky k identifikaci osoby. Fyziologické vlastnosti, jako jsou uspořádání zubu, velikost jazyka, rozměry dutina ústní a nosní, zaručuji ovlivňují zvukový projev. Proto jsou tyto systémy velmi náchylné na projevy nemoci a zranění v oblasti úst. Naopak rysy v chování jsou relativně neměnné pro člověka, který se vyskytuje pouze v jednom charakteristickém prostředí. Jsou ovlivněny kulturou, sociálním prostředím a vlivem příbuzných. [1]

Podstatou metody je vymezení malého množství hlasových dat, vzorku. Na základě frekvenčního rozboru jednotlivých slov nebo frázi lze určit signifikantní znaky při výslovnosti.

Systémy rozdělujeme na textově závislé a textově nezávislé. U textově závislých systému je zapotřebí vyslovit specifický soubor znaku, heslo, uložené jako biometrický etalon v databázi. Na základě srovnání vzorku pak dochází k určení shodnosti a identifikaci uživatele. U textově nezávislých systémů je zapotřebí většího počtu vzorku, v nichž se vytyčí srovnávací charakteristiky, které následně srovnáváme s databází známých uživatelů. Zvuková stopa se rozděluje na jednotlivá slova nebo slovní spojení.[1]

Důležitou součásti, systémů na hlasovou analýzu, jsou šumové filtry, které redukují citlivost na projevy okolního prostředí. Vliv okolního prostředí a aktuálního stavu mluvčího jsou největší nevýhodou. Naopak velkými výhodami jsou cena, technologická nenáročnost a uživatelský komfort.[5]




Obrázek 15: Vizualizace frekvenčního rozsahu hlasového projevu[22]

Tabulka 6: Pravděpodobnost chyb a rychlost analýzy hlasu[5]

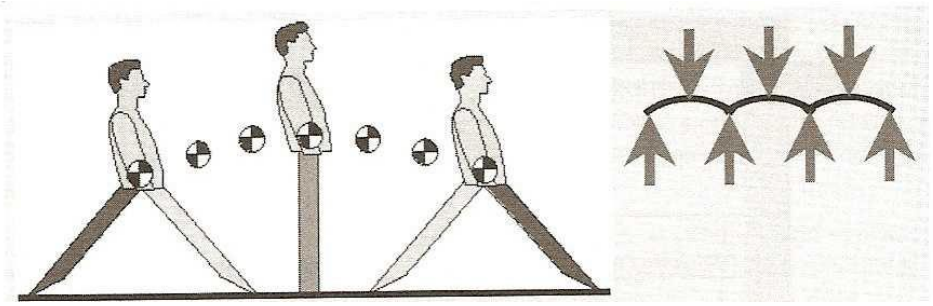
| | |
|---|---|
| FRR | 0,01 [%] |
| FAR | 0,28 [%] |
| Rychlost verifikace | 0,2 - 1 [s] |
| Spolehlivost | nízká |

### 3.3.2 Chůze

Lidskou chůzi nebo běh ovlivňuje spousta okolních faktoru jako jsou anatomické rysy a psychologické aspekty. Tyto faktory zapříčiňují jedinečnost funkčních a dynamických vlastností pohybu. V případě, že se zkoumaný objekt záměrně nevěnuje účelové změně stylu chůze, jeho pohyb je jednotvárný a charakteristický. Na základě těchto poznatku je možno identifikovat osobu. Vedlejšími faktory, které ovlivňují motoriku chůze, jsou zatížení, možná zranění nebo třeba únava a stres. Pří snímaní jsou problematické jevy nasvětlení prostor a úhel snímání. [7]

Metodika rozpoznávání chůze je založena na pohybu těžiště. Dalšími složkami, které jsou zaznamenávány u komplexnějších systémů, jsou ohyby klubových aparátu v kyčlích a kolenech nebo rotace v oblasti ramen a pánve. Výstupní údaje jsou určeny jako uhly mezi křivkami stanovenými mezi jednotlivými body výše uvedených částí těla.[23]

Jedná se o bezkontaktní metodu, kterou lze využít i se stávajícím kamerovým systémem za přítomnosti speciálního rozpoznávacího softwaru. Primárně se tato metodika zaměřuje na identifikaci jedinců prostředí s vysokým pohybem osob, kde očekáváme vysokou míru nepříznivých faktorů znemožňujících identifikaci obličeje. Doposud se tyto metody využívají především pro bezpečností zájmy státu v objektech s vysokou mírou nebezpečí, jako jsou například letiště. Pro komerční využití je však nutno brát v potaz hlavní výhody systému. Za použití této technologie, jsme schopni identifikovat jedince z relativní vzdálenosti, což snižuje časovou náročnost na identifikaci a komfort přístupových systémů.[7]



Obrázek 16: Grafické znázornění dynamiky pohybu těžiště[1]

# 4 PRVKY ZABEZPEČENÍ MOTOROVÝCH VOZIDEL

## 4.1 Mechanické zabezpečení vozidla

Prvotním zabezpečením veškerých automobilu jsou dveře a zámkové mechanismy v nich. V dnešní době se využívá moderních prvku kombinujících klasické prvky cylindrické vložky a elektronické identifikace klíče. Princip této technologie je založen na kódování klíče a mechanismu elektronického ověření na základě imobilizačního čipu obsaženého v klíči. K ověření dochází na základě vzájemné komunikace mezi čipem a řídící jednotkou. Imobilizační čipy můžeme rozdělit na několik typů:

- S pevným kódem
- S plovoucím kódem
- S krypto kódem

U pevného kódu je nastavení čipu prefabrikováno a není zapotřebí přítomnosti vozidla k synchronizaci. U plovoucích a krypto kódů je zapotřebí vložit klíč do zapalování kvůli synchronizaci s řídící jednotkou vozidla. U krypto kódů je navíc zapotřebí speciálního klíče k nastavení řídící jednotky pro přenos.[24]

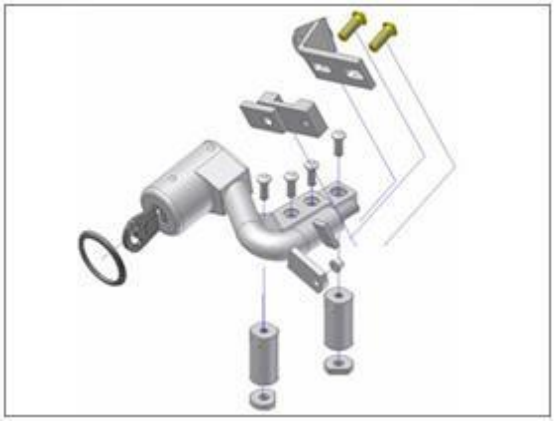
Obrázek 17: Klíče s identifikačním čipem[25]

Spínací skříňka ve vozidle zpravidla osahuje, u klasického vozidla, cylindrickou vložku a mechanismus ověření imobilizačního čipu v klíči. Mechanizmy zabránění nastartování vozidla se různí v principu přerušení elektrického signálu ke startérů.[24]

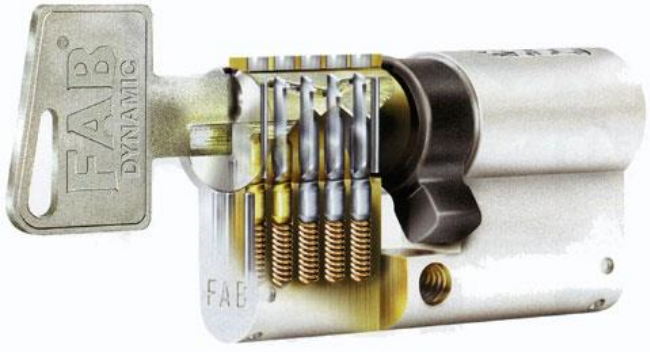
Dalším mechanismem zabezpečení vozidla je zámek řízeni. Jedná se o automatický uzamykací systém, který zabraňuje otáčení volantu v případě nepřítomnosti klíče v zapalování.[24]

Dveřní zámky u vozidel dnes zpravidla fungují na principu centrálního zamykání. Kdy odemčením jednoho zámku vyšleme signál řídící jednotce k otevření veškerých dveří ve vozidle. Systémy centrálního zamykání je možné montovat i dostavbou servo-motorických prvků k dveřním mechanizmům a instalací samostatné řídící jednotky.

Doplňkovými prvky v zabezpečení vozidel jsou uzamykací mechanizmy na volant a řadící páku. Jejich provedení se různí a neobsahují systémy elektronického ověření klíče. Tyto mechanismy jsou složeny z klasické cylindrické vložky a mechanické blokační jednotky. Nejjednodušším příkladem mechanizmu zabezpečení volantu jsou páky na volant. Jejich výhodou je jednoduchost konstrukce a nízké pořizovací náklady. U řadící páky se pak aplikují integrované mechanizmy, které se instalují zpravidla přestavbou.[24]



Obrázek 18: Paka na volant[29] a mechanizmus blokace řadící páky[30]




Obrázek 19: Cylindrická vložka[31]

## 4.2 Elektronické prvky v zabezpečení vozidla

### 4.2.1 Imobilizér

Imobilizér je prvek v zabezpečení motorových vozidel, který funkčně zabraňuje odcizení vozidla. Jedná se o elektronické zařízení, které zabraňuje nastartování vozidla pomoci přerušení elektrických obvodu, zpravidla na řídící jednotce motoru.

Hlavní součástkou imobilizéru je přijímací jednotka, která komunikuje s transpondérem čipu umístěného v přímo klíči nebo jako klíčenka. Komunikace probíhá pomoci zašifrovaného pevného kódu.[32]

### 4.2.2 Autoalarm

Podobně jako u běžných poplachových zabezpečovacích systémů, slouží auto alarm k detekci pachatele nebo nekalé činnosti spojené s vozidlem (např. odtažení). Účelem těchto systémů je informovat majitele vozu o této nežádané aktivitě a to prostřednictvím textových zpráv nebo sirény a jiných výstupních zařízení. [32]

Autoalarmy mají zpravidla samostatnou řídící jednotku („ústřednu“), která má možnost komunikace po sběrnici s řídící jednotkou ve vozidle. Komunikační sběrnice je zde především z důvodů integrace ke stávajícím systémům ve vozidle, jako je například centrální zamykání.[32]

Běžnými detektory jsou dveřní spínače, které spolehlivě detekují otevření dveří do kabiny nebo zavazadlového víka. Nástavbovými prvky jsou detektory tříštění skla, které slouží k indikaci vykrádání vozidla a případnému odstavení zámkových mechanizmů. K vnitřní ochraně vozidla slouží mikrovlnné detektory, které lze využít i u vozidel bez pevné střechy. Tyto detektory slouží k rozpoznání narušení vnitřního prostoru vozidla.[32]

Mezi další detektory můžeme řadit nárazové snímače, které střeží vozidlo především proti vandalismu. U těchto prvku je vysoká míra falešných poplachů. Dalším prvkem detekujícím vnější vlivy je náklonový snímač. Ten snímá charakteristiku změny náklonu vozidla i ve více osách.[32]

Mezi signalizační zařízení se řadí akustické sirény, které informují okolí hlasitým zvukovým signálem. K těmto prvkům doplňuje řídicí jednotka světelnou signalizaci pomocí blinkru vozidla.[32]

## 4.3 Key-less systémy

Mezi moderní prvky ve výbavě vozidla patří systémy bezklíčového přístupu. Tuto technologii můžeme rozdělit do dvou základních kategorií:

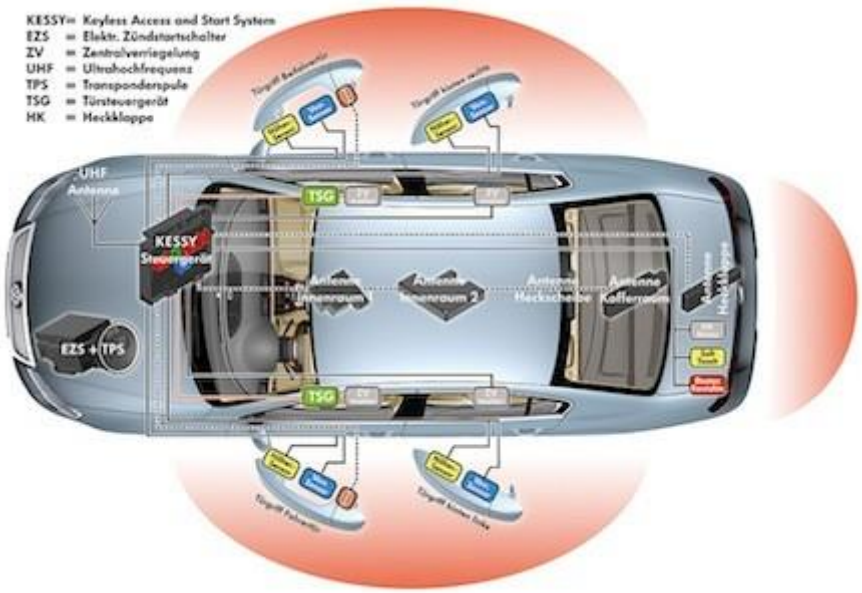
- Systémy pro bezklíčové startování vozidla
- Systémy pro bezklíčový přístup a startování vozidla

U technologie bezklíčového startování vozidla využíváme standartních ovládacích prvků centrálního zamykání, obsažených v kódovaném klíči. Klíč však zpravidla již není osazen planžetou ani jiným prvkem přímého vstupu do zapalovacího mechanismu. Pro startování vozidla se využívá tlačítka umístěného na palubní desce uvnitř automobilu. K nastartování je zapotřebí aby se klíč nacházel v kabině vozu, kde je snímán na principu radiofrekvenční detekce.[33]

U technologie bezklíčového přístupu a startování vozidla je využíváno podobného principu jako u metodiky bezklíčového startování. Rozdílným faktem je rozsah snímané plochy, tedy interakce s klíčem. Klíče jsou detekovány v okolí vozu do vzdálenosti několika metrů. Samotný uzamykací mechanismus má integrovány ochranné prvky před zneužitím. V případě že opouštíte vozidlo, stisknete tlačítko na klice a vozidlo se uzamkne. K znovu otevření je zapotřebí opustit detekovanou zónu nebo vyčkat po stanovený interval. Klíč je v tomto případě detekován i mimo prostory kabiny a tedy pro účel nastartování vozidla stačí mít klíč například v kufru vozidla. U některých značek výrobců vozidel je zapotřebí k přístupu do vozidla navíc stisknout tlačítko na libovolné klice.[34]

Klíč samotný obsahuje identifikační údaje potřebné k ověření autorizovaného přístupu do vozidla. Data jsou na klíči šifrována pomocí bezpečnostních algoritmů. Zvyšování komfortu v této oblasti dnes zachází do míry natolik vzdálené, že například pro přístup do kufru již nepotřebujete stisknout kliku nebo tlačítko ovladače, postačí pouze „nakopnout“ nárazník, kdy je detekován pohyb pod nárazníkem a přítomnost klíče v zadní snímané zóně.[35]

Dnes již prakticky každá světová firma, působící ve výrobě vozidel, využívá adaptované principy těchto technologií. Zpravidla se však jedná o nadstandartní prvky ve výbavě vozidla.




Obrázek 20: Systém KESSY automobilky VW[34]

## 4.4 Další a speciální technologie

V automobilovém průmyslu nachází využití velká řada speciálních technologií. Pro komerční využití je nutno zdůraznit především identifikační technologie vozidel, které nachází uplatnění zejména v systémech elektronického mýtného, ale taky v aplikacích bezpečnostních složek státu. Pro komerčně-bezpečností aplikace je důležitým odvětvím rozvoj identifikačních metod osob a to zejména pomocí technologií RFID a biometrických metod. Tyto doplňky zpravidla představují prémiové prvky ve výbavě vozidel.

### 4.4.1 Lokační systémy

Lokalizační moduly vozidel dnes patří mezi běžně montované doplňky, které však nabízejí specializované firmy. Samotné automobilky nabízejí pouze instalaci komunikačního rozhraní pro připojení modulu, v ceníku označovaných jako takzvaná příprava na zabudování vyhledávacího systému. Principiálně lze rozdělit technologii lokalizace vozidel do dvou základních kategorií a to GSM a GPS lokalizace.

GPS lokalizace, jak už z názvu vyplívá, využívá technologie globálního pozičního systému, tedy zaměření pozice pomocí družic na oběžné dráze Země. Tento typ lokalizace umožňuje zaznamenávat údaje o poloze a rychlosti objektu v reálném čase. Odchylka v zaměření polohy se počítá pro komerční účely v řádech metrů. Přesnější zaměření je možné, ale pouze pro vojenské a akademické účely. V takových případech je tento systém natolik přesný, že je schopen zaměřit objekt s přesností na milimetry.[36]

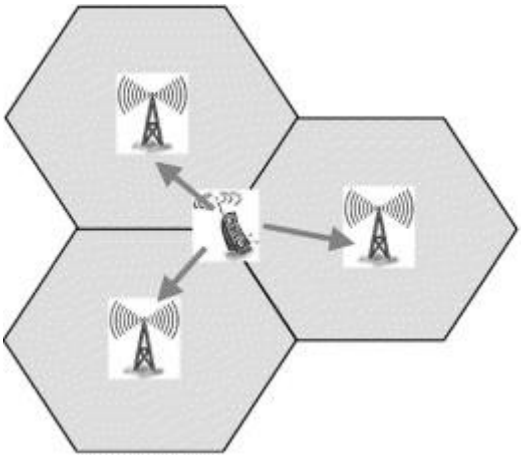
GPS je pouze zobecněným názvem satelitního určení polohy. Ve skutečnosti se však jedná o technologii, která byla původně vytvořena pro účely armády Spojených států amerických. GPS se řadí jako technologie satelitního zaměření první generace společně s ruským systémem GLONASS. Evropský satelitní systém je v současnosti ve fázi zkoušení a na oběžné dráze ještě nejsou vyneseny všechny satelity, které byly pro tyto účely vytvořený. Ústředí evropského systému Galileo se nachází v Praze.[36]

Principiálně je tato technologie založena na Dopplerově jevu frekvenčního posunu. Poloha se určuje pomocí měření vzdálenosti mezi anténou přijímače umístěného na družici a vysílače ve vozidle. K zaměření polohy je zapotřebí signál alespoň ze tří družic. Ke komunikaci se vzdálenými zařízeními se poté používá GSM modulu a mobilní komunikační sítě.[36]


Obrázek 21: GPS lokalizace[37]

GSM lokalizace se zakládá na principu lokalizace pasivního prvku, tedy komunikačního modulu. Tento prvek je stále sledován, jak prochází jednotlivými buňkami mobilního pokrytí retranslačních stanic. Určení polohy umožňuje přesná znalost zeměpisné polohy Těchto retranslačních stanic a znalost principu šíření rádiových vln. Metodika je založena na dvou základních principech, na porovnávání aktivní odezvy k jednotlivým stanicím nebo pasivního diferenčního měření odezvy na vstupu do jednotlivých sektorů pokrytí. Pasivním principem je myšleno přihlášení přístroje v dané buňce, bez vzájemné komunikace se stanicí, tedy přístroj nemusí být v aktivním komunikačním režimu. Oba principy jsou však založeny na měření rozdílu časové odezvy oproti stanovenému času retranslační stanice.

Přesnost těchto metod dosahuje v řádech desítek metrů a to pouze v lepším pohledu. Zpravidla Se můžeme dostat i k odchylce přes sto metrů.[36]



Obrázek 22: Princip GSM lokalizace[38]

V dnešních dobách se používá zaměřování pozice pomocí kombinace předešlých dvou technologií. Tento princip je označován jako A-GPS (Assisted GPS), kdy k určení polohy uživatel potřebuje dosah družic a ke zpřesnění polohy a jednoznačnému určení je využit princip GSM lokalizace. Tato technologie dosahuje přesnosti na několik metrů, ale plně funkční infrastruktuře moderních datových sítí jsme schopni zaměřit pozici s přesností na centimetry. Hlavní výhodou je stálé zaměření na území pokrytém síti mobilní komunikace i v případě nedostačujících signálů z družic. Nevýhodou je stálé datové připojení nutné k přesnému určení. Odchylky v případech nedostupnosti mobilní sítě jsou v řádech desítek metrů.[36]

# II. PRAKTICKÁ ČÁST

# 5 TECHNICKÉ POŽADAVKY

Při návrhu biometrických systému je nutné považovat technické požadavky na instalaci elektronických prvků do výbavy vozidla. Zároveň je však důležité nahlížet na technologické standardizace při tvorbě biometrických prvků.

## 5.1 Normy stanovené v automobilovém průmyslu

Pro schválení elektronických systémů ve vozidle je nutno brát ohled na oblast elektromagnetické (EM) kompatibility dle EHK 10.03 na klasifikaci EM rušení, ČSN 30 4011 s požadavky na odolnost vůči EM a příslušných norem ISO. Dalšími požadavky jsou integrace imobilizačních jednotek dle EHS 95/56. Pro účely startování vozidla je stanovená klasifikace řídící elektroniky dle normy ČSN 30 4208 pro spalovací motory. Zároveň je nutno stanovit normy ochrany krytím dle ČSN EN 60 529, známé pod zkratkou IP. Kde stanovujeme požadavky na krytí IP 53 pro klasifikaci odolnosti vůči prachu a voděodolnost krápěním.

## 5.2 Normy stanovené pro biometrické prvky

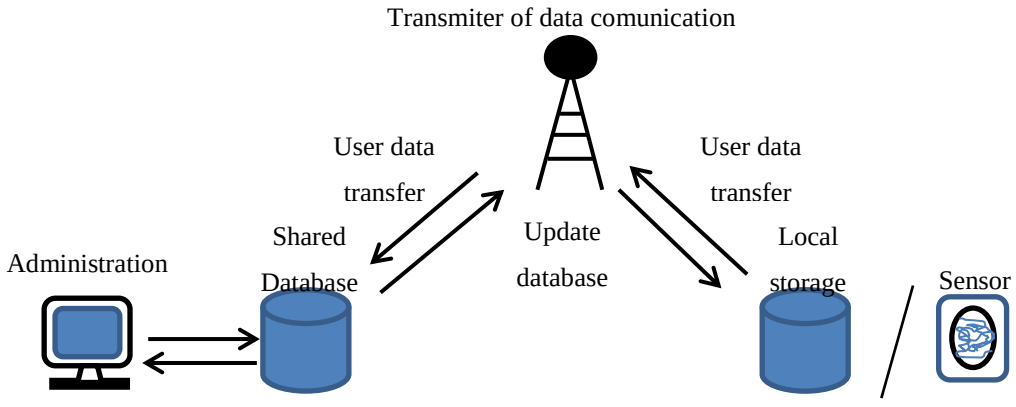
Při tvorbě biometrických prvku je kladen důraz především na životnost a standardizace formátů dat. Mezinárodně platné normy formátů pro kategorizaci dat jsou stanovené normou ISO/IEC 19785 v oblasti specifikace a registrace biometrických údajů. Pro účely jednotlivých metod snímání byla vytvořena norma ISO/IEC 19794. Pro využití aplikačního rozhraní využíváme standardizace ISO/IEC 19784, která slouží především k synchronizovanému vývoji koncových aplikaci pro uživatele. Při testování výkonosti systému je využívána norma ISO/IEC 19795, kde jsou definovány požadavky na rychlost odezvy a hodnoty pravděpodobnosti vzniku chybné reakce na požadavek uživatele. Biometrické systémy samozřejmě podléhají normalizaci při klasifikaci odolnosti jednotlivých prvku z pohledu elektromagnetické kompatibility a odolnosti vůči vnějším jevům podle normy ČSN EN 60 529.

# 6 NÁVRH BIOMETRICKÝCH PRVKŮ PRO AUTOMOBIL

## 6.1 Obecná hlediska využití biometrických prvků v zabezpečení vozidel

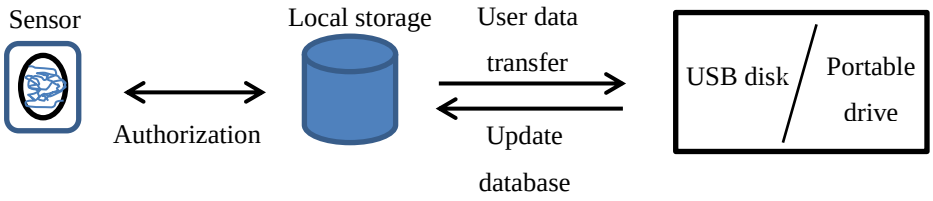
Pro využití biometrických prvku v zabezpečení vozidel je zapotřebí brát v potaz účel dopravního prostředku, vozidla. Je zapotřebí rozlišovat zdali máme v úmyslu systém využívat soukromě, tedy je předpokladem, že dané vozidlo bude využívat minimální počet uživatelů, a využitím v provozu běžného podniku, tedy vozidlo bude využívat, pro naše účely, blíže nespecifikovaný počet osob. V těchto závislostech je potřeba rozlišit implementace databázových prvků do samotných snímacích zařízení, popřípadě využití stávajících datových uložišť komunikačního rozhraní, nebo využití externího, samostatného, uložiště, které bude schopno pojmout více biometrických etalonů a současně bude možno tyto data přenášet a sdílet. V tomto kontextu je potřeba definovat sdílení informaci v systému vozidla i mimo něj.

Pro účely firemního vozidla je vhodnějším řešením samostatně založený systém s možností přenositelnosti a distribucí dat. Zároveň je nutné implementovat prvky zabezpečení datové komunikace, šifrování, a to zejména při komunikaci z vnější sítí. Jednou z možností je začlenit datový modul komunikace do systému. Toto řešení nabízí řadu výhod, a to zejména do oblasti informovanosti zaměstnavatele o pohybu svých vozidel a oprávněnosti osob, které je užívají. Zároveň se zde nabízí možnost sdílené databáze uživatelů, tedy nižší požadavky na datová uložiště ve vozidle samotném. Problematickým jevem však může být zajištění dostatečně rychlého připojení k datovému serveru a stálost pokrytí signálem o dostačující intenzitě. Mezi hlavní výhody takovéhoto systému pak můžeme řadit jednoduchou správu dat a možnost okamžitého zjištění stavu užití vozidla.



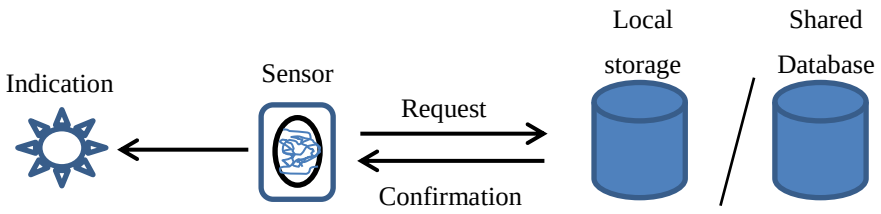

Obrázek 23: Obecné znázornění vzdálené komunikace

Systémy nezávislé na datové komunikaci je zapotřebí zabezpečit v rámci kvalifikované obsluhy a pravidelné správy systému. Bez datové komunikace se serverem je zapotřebí zajistit aktuálnost dat a alternativní přístup do vozidla. Pro tyto účely je zapotřebí zajistit rozhraní ke komunikaci s funkční jednotkou a přístup ke komunikačnímu portu. Výhodou této aplikace je však právě zmiňovaná nezávislost na intenzitě signálu v dané lokalitě a relativně vyšší bezpečnost, způsobená samostatnou funkčností systému. Tuto vlastnost uživatel ocení především v případě poruchy na zařízení, kdy disfunkce jednoho systému vozidla nenaruší funkčnost vozidel zbylých.



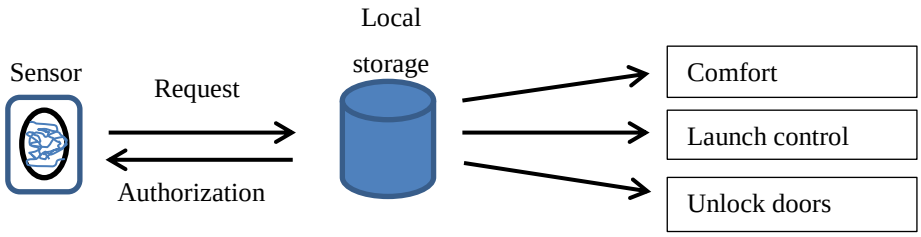

Obrázek 24: Obecné pojetí implementace dat do lokálního uložiště

Pro účely soukromého užití je výhodnější a snáze aplikovatelnou variantou využití samostatně zapojeného systému ověřování biometrických charakteristik za využití stávajících komunikačních systému osobního vozidla. Instalace těchto prvku probíhá ve dvou variantách provedení. První variantou je nástavba vlastního systému ověření identity. Kdy do stávajícího systému lze začlení komunikační a ovládací moduly biometrických prvků. Tyto moduly následně propojíme skrze standardizované komunikační rozhraní s řídící jednotkou automobilu. Druhou variantou je začlenění systému do základní struktury komunikačního rozhraní ve vozidle. V takovémto případě je zaručená jednoznačná kompatibilita stávajících systémů a designové začlenění těchto prvků v základním rozvržení vozidla. V těchto systémech je zapotřebí ukládat biometrické etalony samostatně pro každé jednotlivé vozidlo. Data lze ukládat pomocí komunikačního rozhraní zprostředkovanou formou nebo přímo ze snímače umístěného ve vozidle.




Obrázek 25: Obecné pojetí zpracování zadávaných vzorů

V případě využití implementovaného bezpečnostního systému, do základního komunikačního rozhraní vozidla, je možné využít i vymezení komfortních prvků v přístupovém systému a ovládání základního nastavení. Pomocí vymezení identity uživatele lze předdefinovat parametrické nastavení například polohy sedadel nebo zrcátek. Rovněž lze charakterizovat možnosti využití přístupových práv a tak definovat uživatele, kteří jsou oprávněni k pouze přístupu nebo současně i k řízení vozidla.




Obrázek 26: Obecný princip zpracování vstupu

## 6.2 Otisky prstů

V této oblasti ověřování identity je zapotřebí členit systémy implementované do struktury vozidla v továrním provedení a takzvaných nástavbových systémů doplňujících stávající bezpečnosti prvky v již provozovaném vozidle. Vlivem požadavků na odolnost snímačů je reálné užití pouze u technologií optických a kapacitních prvků.

### 6.2.1 Technologie zpracování biometrických vzorů

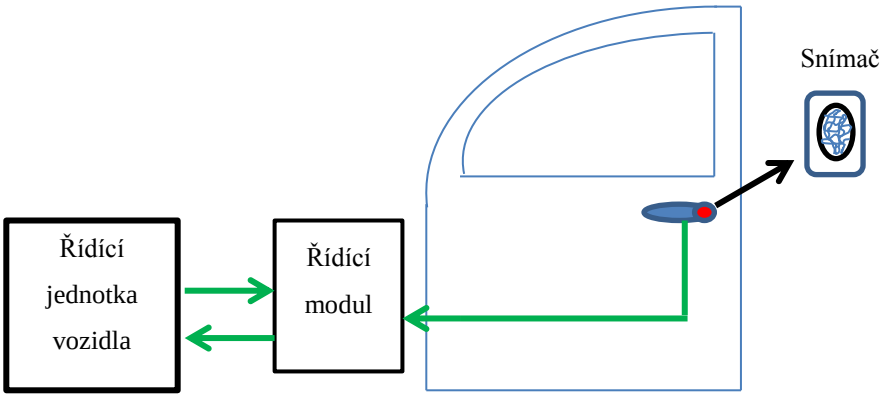
Při rozvoji mobilních aplikací vznikají softwarová řešení algoritmů využitelných v mobilních zařízeních. Pro účely zabezpečení vozidel jsou právě tyto komprimované aplikace, s nízkými požadavky na výkon samotného systému, vhodným řešením, vzhledem k hardwarovému základu celého systému. Při využití systému nabízeného společností IBM je definován rozsah posuzování shody v rozmezí 12 až 36 porovnávaných charakteristických znaků při stanovení variací uspořádání překračujících hodnotu $6.10^{-8}$. Jednotlivé údaje o vyhodnocovaných charakteristikách jsou ukládány do matice znázorňující jednotlivé pixely snímače. Standardizovaný rozsah snímané scény na jednotlivých pixelech se u kapacitních i optických snímačů stanovuje na 0,5 µm.

### 6.2.2 Využití pro přístupové systémy

Při využití biometrických prvků pro přístup do vozidla je možné charakterizovat dvě varianty užití. V prvním případě je možné začlenit snímač do klíče vozidla. V takovém případě je užití možné k ověření identity pro účely keyless systému. Takováto instalace dostává smysl v případě kombinace se systémy startování vozidla, kdy běžné ověření imobilizačního kódu doplňujeme o identifikaci specifické uživatele, a vymezení prav užití vozidla. Tedy i v případě zcizení klíče je možné zabránit přístupu do vozidla. V tomto provedení je možno využít kapacitních i optických snímačů, které nejsou vystavovány přílišným změnám v klimatu. Pro tyto účely je možno využít i nástavbových systémů za předpokladu instalace komunikačních modulů.

V druhé variantě se jedná o instalace snímacích prvků do vnější konstrukce vozidla, do oblasti kliky dveří u řidiče. V tomto provedení je zapotřebí klást důraz na odolnost jednotlivých prvků vůči klimatickým změnám, zejména voděodolnost a odolnost vůči nízkým teplotám stanovené třídou prostředí. Pro účely venkovního všeobecného prostředí je zapotřebí přizpůsobit prvky na funkčnost při teplotách od -25 °C do 60 °C. tyto rozsahy teplot jsou definovány českou normou pro využití přístupových systému.

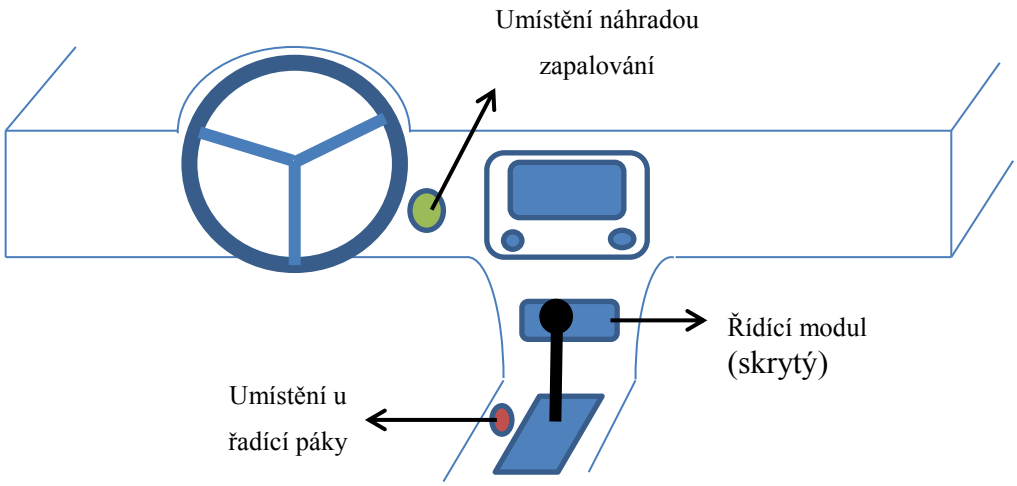
Z těchto důvodů je možné využít pouze optických snímačů. V tomto provedení je možné využití nástavbových prvků, ale instalace je problematická vzhledem k nutnému zásahu do struktury karoserie vozidla.




Obrázek 27: Návrh rozmístění přístupových prvků biometrie otisků prstů

### 6.2.3 Využití pro systémy startování vozidla

Pro účely identifikace osob při startování vozidla je možné využít stávajících systémů nabízených výrobcem vozidla nebo nástavbovým systémem a instalací komunikačního rozhraní. Důležitým faktem je přehledné umístění prvků a systém indikace stavu zařízení. Pro tyto čely lze využít statických snímačů, které snímají otisk prstu v jednom celku. Umístění prvků je možné začlenit jako náhradu skříňky zapalování vozidla, v centrálním tunelu u řadící páky nebo do řadící páky samotné. U poslední varianty je zapotřebí brát ohled na pohyblivost kabeláže. Možnost využití ověření identity můžeme kombinovat s prvky startovacího tlačítka, tedy při ověření dochází k inicializaci řídící jednotky motoru, nastartování, nebo v kombinaci se samostatnou inicializací startování pomocí doplňujících prvků spínání.




Obrázek 28: Návrh rozmístění prvků systému STOP/START biometrie otisků prstu

## 6.3 Obličejová rekognice

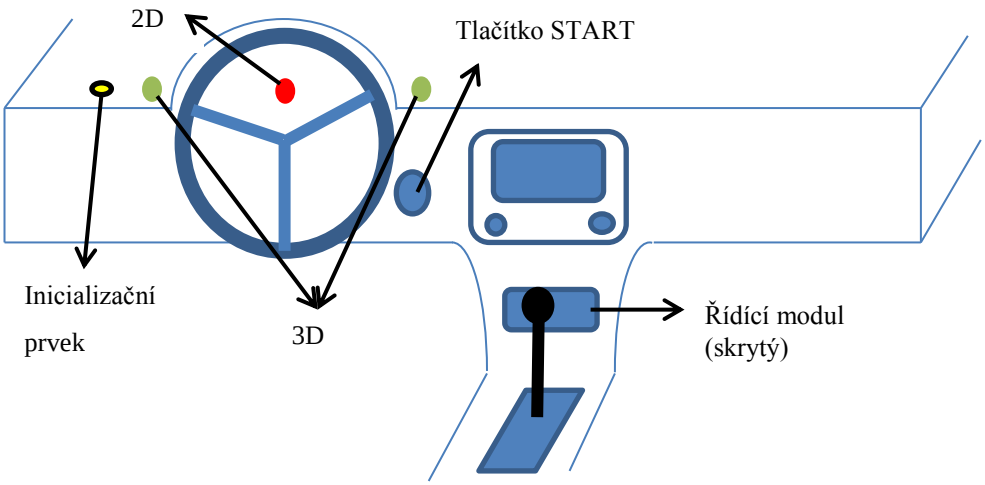
Vzhledem k možnostem umístění biometrických prvků je vyloučena možnost využití pro účely přístupových systémů. Problematikou je vysoký sklon obrazu a omezující vlivy prostředí dané světelnými podmínkami v denním cyklu, kdy nelze zaručit stabilní podmínky nasvětlení snímané scény. Na základě těchto předpokladů lze stanovit nemožnost získání dostačujících identifikačních charakteristik při běžném využívání vozidla.

### 6.3.1 Technologie zpracování biometrických vzorů

Při minimalizaci rozměrů je považován jako technologický zaklad snímání obličeje, v monochromatickém spektru, o rozlišení 640 x 480 pixelu. Úhel sklonu zobrazované scény je doporučován na hodnoty přibližně 15 stupňů pro jednoznačnou identifikaci. V případě snímané scény v 2D zobrazení je požadovaná délka snímání pod 3 sekundy a rozměry výsledného vzoru zpravidla obsahují údaje o velikosti 4 kB. Při znázornění 3D snímané scény je zapotřebí připočítat časovou prodlevu při komunikaci systémů s jednotlivými prvky a skládání výsledného obrazu. Stanovený objem dat jednoho vzoru je pak 10-ti násobný při minimalizovaných požadavcích na rozlišení a kvalitu obrazu.

### 6.3.2 Využití pro systémy startování vozidla

Instalace prvků k rozpoznání obličeje lze charakterizovat do dvou základních skupin, 2D a 3D systémy. Pro využití 2D snímání je zapotřebí instalace jednoho prvku do roviny snímané scény, kdy je zapotřebí volný prostor v trajektorii pořizovaného obrazu. Tyto systémy jsou však vysoce náchylné na rozpoznávání živého objektu od fotografie. Při instalaci systému pro pořizování 3D obrazu je zapotřebí dvou prvků umístěných v jedné rovině. Pro inicializaci snímání lze využít klasických elektronických spínacích systému nebo automatizovaného procesu při aktivaci řídící jednotky ve vymezeném časovém úseku.




Obrázek 29: Návrh rozmístění prvků obličejové rekognice

## 6.4 Analýza hlasu

Pro účely hlasové analýzy, při řízení přístupu do vozidla, je důležitým faktorem okolní ruch, který tuto možnost využití vylučuje. Za těchto podmínek je nutné instalovat filtry zvukového šumu i v kabině vozidla, kde je míra okolního ruchu na přijatelné hranici.

### 6.4.1 Technologie zpracování biometrických vzorů

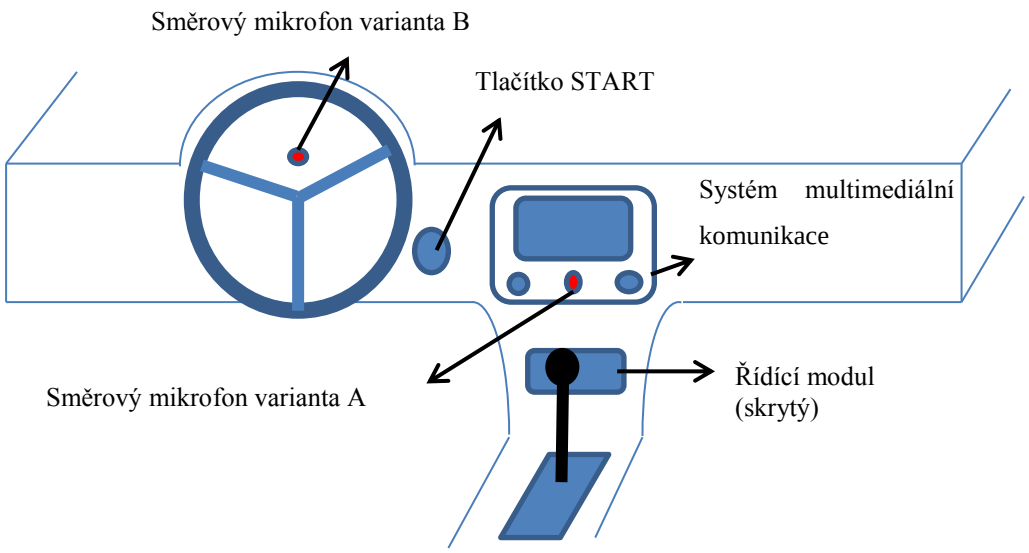
Při použití technologie určené pro mobilní zařízení je nutné brát v potaz rozsah frekvencí snímaných mikrofonem a to zejména u již instalovaných komunikačních rozhraní ve vozidle. Pravidlem je stanovení minimální frekvence hlasu na 11 kHz při hloubce rozsahu analyzátoru na 16 bitech. Pro zpracování vzorku při využití dostupných technologií mikročipů, je stanovená délka porovnání shody menší než 1 sekunda. Na extrahovaný vzorek je stanovena minimální délka záznamu 2 sekundy. Tyto systémy mají zpravidla omezení na počet uživatelů, ten se pohybuje okolo 10 osob.

### 6.4.2 Využití pro systémy startování vozidla

Technologii startování vozidla pomocí hlasové analýzy lze realizovat implementací samostatného vyhodnocovacího systému nebo integrací specializovaného softwaru do stávajících komunikačních systémů vozidla za předpokladu využití ovládacích prvku a nástavbových modulů. Při využití stávajícího komunikačního rozhraní je zapotřebí definovat systém ukládání dat, na uložiště multimediálních komunikačních prvků, a systém oživení elektroniky vozidla při vstupu. Je možné definovat textově závislé příkazy k ovládání inicializace ovládací jednotky motoru, za pomoci definice specifického vzoru příkazu.

Druhou variantou je využití stávajících systému inicializace pomoci spínacích prvku, tlačítek STOP/START, při schválené identifikaci uživatele. Pro tyto účely je nutno specifikovat širší spektrum hlasových vzorků.

U nástavbových systémů je předpoklad samostatně umístěného směrového mikrofonu do pozice prostoru řidiče, vlastní vyhodnocovací jednotky, lokálního uložiště a ovládacího a komunikačního modulu, případně inicializačních prvků. Opět je možné implementovat systémy textově závislé a textově nezávislé.




Obrázek 30: Návrh rozmístění prvků systému STOP/START pro analýzu hlasu

## 6.5 Geometrie ruky

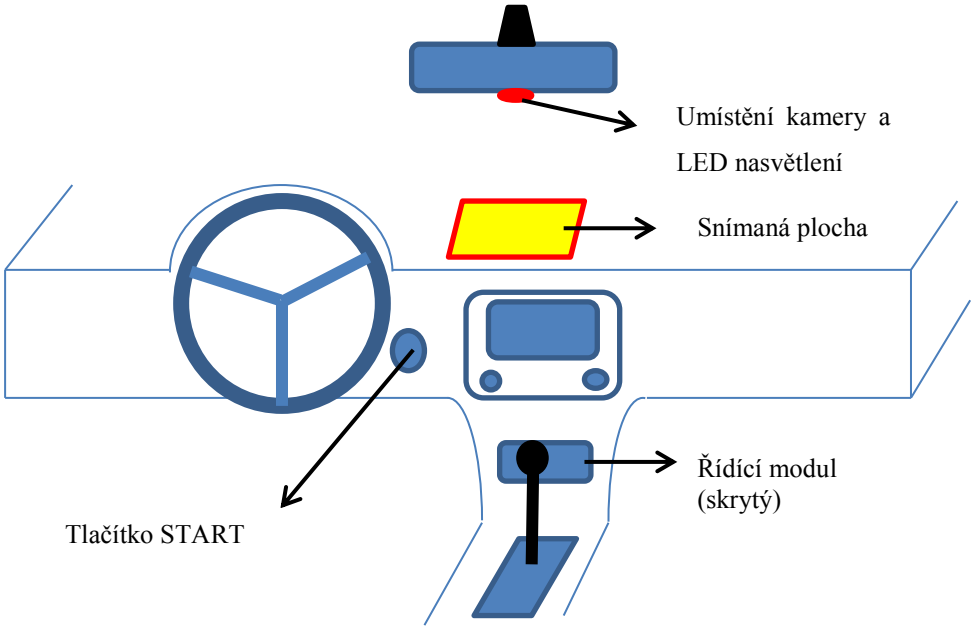
Ve velmi okrajovém pojetí, při implementaci stávajících technologií, je možné využít systému rozpoznávání biometrických charakteristik tvaru ruky. Tato metodika je zpravidla náročná na prostor a pro účely přístupových systému je proto nutné zvolit algoritmy postupného snímání. V takovém to případě je však vysoká pravděpodobnost chybného zamítnutí, vlivem zkreslení výsledného obrazu.

### 6.5.1 Využití pro přístupové systémy

V této fázi ověřování identity je možné využít dvou variant instalace. V první variantě je možné instalovat kameru systém nasvícení plochy do prostor samotné kliky kdy je zapotřebí definovat algoritmus postupného snímání scény. Tento postup vyžaduje plynule umístění ruky do prostor snímání. V druhé variantě lze definovat zónu snímaní do prosklené plochy za předpokladu využití vhodným snímacích prvku. Hlavním problémem z hlediska nežádoucích vlivů je možnost zanesení kamery snímače nebo okenního prostoru a tím znehodnocení snímaného vzoru.

### 6.5.2 Využití pro systémy startování vozidla

Při prostorové náročnosti systémů je jediným možným umístěním snímané scény do prostor horní části palubní desky. Snímané charakteristiky lze v takovém případě z pozice umístění kamery s CCD čipem do vnitřního zpětného zrcátka, kdy je zapotřebí eliminovat rozdílné světelné podmínky nasvícením scény. Inicializaci systému je možné realizovat pomocí tlakového snímače na desce definující snímanou plochu. V takovémto využití je nutnost rozplánování integrace prvků už v samotném návrhu konstrukce vozidla. Za předpokladu samostatné inicializace snímání je možno definovat snímanou scénu na libovolné rovné ploše palubní desky za předpokladu dodržení horního snímání.




Obrázek 31: Návrh rozmístění prvků systému STOP/START geometrie ruky

# 7 NOVÉ TRENDY

Na přelomu milénia se začaly instalovat systémy biometrického určení identity pro přístup a ovládání startování vozidla. Především se jedná o iniciativu automobilových koncernů, ale také existují samostatné společnosti nabízející nástavby k již osazeným funkčním bezpečnostním prvkům. V současnosti na komerčním trhu existuje úzké využití biometrického rozpoznávání otisků prstů. Zpravidla se jedná o prémiové doplňky zabezpečení vozidel.

Současný trend uvádí rozvoj především komunikačních a multimediálních prvku ve vozidle. Jednoduché systémy analýzy hlasu pro účelné zvýšení komfortu uživatele, jsou již dnes ve vývojích automobilových koncernů. Do budoucna lze tedy počítat s širším spektrem využití při rozvoji technických prostředků těchto zařízení. Při využití bezklíčového přístupu do vozidla se přímo nabízí možnost doplňujících bezpečnostních prvků založených na biometrickém ověření. Existuje řada studií dokazujících právě neefektivitu zabezpečení těchto systémů proti neoprávněnému zneužití.

Biometrické systémy nabízí zvýšení úrovně komfortu uživatele při maximalizace bezpečnostních aspektů. Zároveň, pro účely podnikových vozidel, jsou schopny zprostředkovat jednoduchou správu a informovanost o uživatelích. S rozvojem komunikačních technologií jsem přesvědčen, že je otázkou času než se v tomto odvětví začnou biometrické systémy hojně využívat.

# ZÁVĚR

Po celém světě je majetková kriminalita, do oblastí motorových vozidel, velmi citlivým tématem. Nezávisle na poloze vozidla z hlediska odstavení, je nutno zajistit jeho dostatečné zajištění proti zcizení i samotnému vloupání a páchání následné škody. Existuje hned několik pohledu na tuto otázku. Zejména se ohlížíme na dnes již zastaralé pojetí čistě mechanických zábranných systému. V moderním pojetí pak na vzrůstající požadavky v oblasti elektronického zabezpečení proti krádeži a vniknutí.

Účelem této práce bylo seznámit veřejnost s alternativními a moderními postupy v chápání zajištění vozidla. To především do oblasti biometrického ověřování. Z těchto důvodu jsem vyhodnotil reálně využitelné technologie z pohledu současných možností i budoucího využití a předpokládaného vývoje.

Základem této práce bylo seznámit čtenáře s pojmy v této oblasti a představit jednotlivé využívané metody v oblasti biometrického ověření. Zároveň pak seznámení s prvky využívanými v zabezpečení vozidel a pro účely zvýšení komfortu uživatele.

V praktické části jsem vyhodnotil možnosti současných technologií a zpracoval návrh na řešení zabezpečení motorových vozidel za použití biometrických systémů. Tato část je zejména vlastním zhodnocením a aplikací jednotlivých metod, nezávisle na soudobém užití. Tento návrh je brán s ohledem na současné technologie a již vytvořené projekty a to i ve smyslu vnímání oblastí jiného užití než v zabezpečení vozidel.

Dnes se jsou na trhu různá řešení využití biometrických prvků a to i v oblasti automobilového průmyslu. S krátkým ohlédnutím do blízké minulosti i budoucnosti mohu říct, že mým předpokladem je brzké rozšíření biometrických metod v tomto odvětví a to zejména s ohledem na zabezpečení i komfort ve vozidlech.

# ZÁVĚR V ANGLIČTINĚ

In a whole world, is problematice of crime against property, especially in meaning of motor vehicles, very sensitive part of discussion. In a meaning of independence to the vehicle location, there is a reasonable request for secure against theft them self and theft of property located inside as same as after damage on a vehicle. There are several meanings into those problematics. Today, we are especially look at the old stuff solution by mechanical security systems. In a mean time of modern conslusion to look at the aspects from the side of electronical alarm systems against theft.

Purpose of these work is to apprise public with alternative and modern aspects of vehicle security, especially to the part of biometrics authentification. Becouse of those reasons, I´ve evaluated real usability from nowadays and future technological state for usage and future development.

Basic part of these work was to apprise reader with terminology of these sphere and get knowledge about individaul parts of usage biometrics authentification. Withal, get knowledge of technology for usage into vehicle security and for increase of comfort level for user.

In a practical part, I´ve evaluated possibilities of nowadays technology and compile suggestion for solution of vehicle security with usage of biometrics systems. These part is in a mean time myself valorization and aplication of individual metods in a independent look to nowadays uasage. These composition is take with aspects of nowadays technology and projects in move and therefore in meaning of purpose to usage in vehicle security.

Today there are some solutions of using biometrics technology and therefore in the sphere of vehicle security usage. In the look to the near history and the future, I may tell, that I´ve gat an idea of close usage of biometrics technology in these branch and in the mainly in the meaning of security and increasing comfort level in vehicles.

# SEZNAM POUŽITÉ LITERATURY

[1] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5

[2] *Bude mít každý člověk v těle čip?*. In: [online]. 2004 [cit. 2013-05-09]. WordPress & BuddyPress. Dostupné z: http://21stoleti.cz/blog/2004/08/21/bude-mit-kazdy-clovek-v-tele-cip/

[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] LI, Haizhou, Liyuan LI a Kar-Ann TOH. *Advanced topics in biometrics*. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5

[5] FLÍDR, Jakub. *Biometrické autentizační metody* [online]. Brno, 2009 [cit. 2013-05-03]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=17183. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Ing. Jiří Sobotka.

[6] *Biometrika* [online]. 2010 [cit. 2013-05-04]. Biometrika. Dostupné z: http://www.nula.wz.cz/biometrika/.

[7] HRAZDIRA, Petr. *Biometrické identifikační metody* [online]. Zlín, 2010 [cit. 2013-05-04]. Dostupné z: http://dspace.k.utb.cz/bitstream/handle/10563/14192/hrazdira_2010_dp.pdf?sequence=1. Diplomová práce. UTB ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce JUDr. Vladislav Štefka.

[8] *Autentizační metody založené na biometrických informacích* [online]. 2010 [cit. 2013-05-09]. ISSN 1214-9675. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2010110002

[9] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava, 2008 [cit. 2013-02-05]. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-

root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf. Skripta. VŠB TU.

[10] *Dermatologické faktory ovlivňující snímání otisků prstů* [online]. 2010 [cit. 2013-05-09]. Dostupné z: http://www.mvcr.cz/clanek/dermatologicke-faktory-ovlivnujici-snimani-otisku-prstu.aspx

[11] *Obrazce a znaky kůže* [online]. [cit. 2013-05-09]. Dostupné z: http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

[12] VYORAL, Pavel. *Identifikační biometrické systémy* [online]. Zlín, 2011 [cit. 2013-05-10]. Dostupné z: http://dspace.k.utb.cz/handle/10563/16746?show=full. Bakalářská práce. Univerzita Tomáš Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Milan Navrátil, Ph.D.

[13] *Krize daktyloskopie* [online]. 2002 [cit. 2013-05-09]. Dostupné z: http://akademon.cz/article.asp?source=biom

[14] MAINGUET, Jean-François. *Fingerprint sensing techniques* [online]. 2004, 2012-04-13 [cit. 2013-05-09]. Dostupné z: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.htm#optic_TFT

[15] *Měření biometrických údajů* [online]. [cit. 2013-05-10]. Dostupné z: http://www.uamt.feec.vutbr.cz/vision/TEACHING/MAPV/10%20-%20Biometrie%20a%20medicina.pdf

[16] CHOLEVA. *Sněžná slepota* [online]. 2011 [cit. 2013-05-09]. Dostupné z: http://www.lezec.cz/clanky.php?xtem=&key=9177

[17] SANCHEZ. *Otros factores (externos) que influyen en el color de ojos* [online]. 2012 [cit. 2013-05-09]. Dostupné z: http://enroquedeciencia.blogspot.cz/2012/04/otros-factores-externos-que-influyen-en.html

[18] Biometric Recognition. In: *Detection, Inspection, and Enforcement* [online]. 2010 [cit. 2013-05-09]. Dostupné z: http://www.nist.gov/mml/mmsd/security_technologies/dietbiom.cfm

[19] Biometric system laboratory. In: *Hand* [online]. 2012 [cit. 2013-05-09]. Dostupné z:

http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=222&pathSubj=222&Req=&

[20] BACTERIOL. *A Genomic Island Defines Subspecies-Specific Virulence Features of the Host-Adapted Pathogen* [online]. 2009 [cit. 2013-05-09]. DOI: 10.1128/JB.00803-09. Dostupné z: http://jb.asm.org/content/192/2/502/F1.expansion.html

[21] CHIRILLO, John. Implementing biometric security. Vyd. 1. Indianapolis: Wiley Publishing, 2003, 414 s. ISBN 07-645-2502-6

[22] VONDRA, Martin. *Kepstrální analýza řečového signálu* [online]. 2001 [cit. 2013-05-09]. Dostupné z: http://www.elektrorevue.cz/clanky/01048/index.html

[23] TALANDOVÁ, Hana. *Studie využití biometrických systémů v průmyslu komerční bezpečnosti* [online]. Zlín, 2010 [cit. 2013-05-10]. Dostupné z: http://dspace.k.utb.cz/handle/10563/13364. Bakalářská práce. Univerzita Tomáš Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Petr Navrátil, Ph.D.

[24] KURIL, Jiří. *Konstrukční návrh mechanického zabezpečení vozidla proti krádeži* [online]. Pardubice, 2008 [cit. 2013-02-05]. Dostupné z: http://dspace.upce.cz/bitstream/10195/29285/1/text.pdf. Diplomová práce. Univerzita Pardubice, Dopravní fakulta Jana Pernera. Vedoucí práce Dufek, Jiří.

[25] JOB, Ann. MSN Autos. *Driving Without Car Keys* [online]. 2011 [cit. 2013-05-09]. Dostupné z: http://editorial.autos.msn.com/article.aspx?cp-documentid=435298

[26] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6

[27] ASHBOURN, Julian. Practical biometrics: from aspiration to implementation. London: Springer-Verlag, 2004, xiv, 159 s. ISBN 18-523-3774-5

[28] BOLLE, Ruud M. Guide to biometrics. New York: Springer Science Business Media, 2004, xxix, 364 s. ISBN 03-874-0089-3

[29] *Kde se nejvíc kradou auta?* [online]. 2010 [cit. 2013-05-09]. Dostupné z: http://www.autembezpecne.cz/cz/s40/c1437-Zpravy/n2083-Kde-se-nejvic-kradou-auta-V-Praze-a-strednich-Cechach

[30] *Zabezpečení automobilu* [online]. 2009 [cit. 2013-05-09]. Dostupné z: http://www.mototipy.com/zabezpeceni-automobilu-cast-3/

[31] Klíče a zámky. In: *Klíče a autoklíče* [online]. 2002 [cit. 2013-05-09]. Dostupné z: http://www.klice-autoklice.cz/?page=klice_a_zamky

[32] RAŠKA, Martin. *Identifikace a zabezpečení motorových vozidel* [online]. Zlín, 2009 [cit. 2013-05-10]. Dostupné z: http://dspace.k.utb.cz/handle/10563/9170. Bakalářská práce. Univerzita Tomáš Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce JUDr. Vladislav Štefka.

[33] Gasta & Čoupek. *Autoklíče* [online]. 2002 [cit. 2013-05-09]. Dostupné z: http://editorial.autos.msn.com/article.aspx?cp-documentid=435298

[34] SAJDL, Jan. Autolexikon. *KESSY* [online]. [cit. 2013-05-09]. Dostupné z: http://cs.autolexicon.net/articles/system-kessy-keyless-access/

[35] *Keyless GO* [online]. 2013 [cit. 2013-05-09]. Dostupné z: http://techcenter.mercedes-benz.com/cs_CZ/keylessgo/detail.html#intro-section

[36] WAGNER, Michal. *APLIKACE ELEKTRONICKÉ IDENTIFIKACE V AUTOMOBILU* [online]. Praha, 2009 [cit. 2013-05-10]. Dostupné z: http://www.general-files.com/download/gs44f0eef2h32i0/BP_Wagner_Aplikace%20elektronick%C3%A9%20identifikace%20v%20automobilu.pdf.html. Bakalářská práce. ČVUT v Praze, Fakulta dopravní. Vedoucí práce prof. Dr. Ing. Miroslav Svítek.

[37] Lokalizace vozidla. In: *O lokalizátoru* [online]. [cit. 2013-05-09]. Dostupné z: http://autopatrol.cz/lokalizace-vozidla.php

[38] DODGSON. *Mobile terminal security and tracking* [online]. 2004 [cit. 2013-05-09]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1363412705700418

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| 2D | zkratka dvoudimenzionálního prostoru (plochy) |
| 3D | zkratka třídimenzionálního prostoru |
| A-GPS | technologie pro určení polohy (assisted GPS) |
| CCD | Elektronická součástka (charge-coupled device) |
| ČSN | česká státní norma |
| DNA | deoxyribonukleová kyselina (deoxyribonucleic acid) |
| EER | průsečík mezi FAR a FRR (equal error rate) |
| EHK | norma (externí hodnocení kvality) |
| EHS | evropská norma |
| EM | elektromagnetický jev |
| FAR | pravděpodobnost chybného přijetí (false acceptation rate) |
| FRR | pravděpodobnost chybného odmítnutí (false rejection rate) |
| GPS | systém pro určení pozice (global positioning system) |
| GSM | telekomunikační technologie (global system for mobile communications) |
| IP | označení normované odolnosti |
| ISO | mezinárodní norma |
| KESSY | elektronický zamykací a startovací systém (keyless entry start and exit system) |
| LED | technologie svítivé diody (Light Emitting Diod) |
| RFID | radiofrekvenční identifikační technologie (radio-frequency identification) |
| VW | zkratka automobilového výrobce a koncernu (Volkswagen) |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH

# PŘÍLOHA 1: OBRAZOVÁ PŘÍLOHA FUNKČNÍCH PRVKŮ


Obrázek 34 : Integrovaná čtečka otisků prstů v Audi A8[14]

Obrázek 33: Nástavbová čtečka otisků prstů Siemens[14]

Obrázek 32: Čtečka otisků prstu integrovaná v klíči[14]