Česká zemědělská univerzita v Praze

Technická fakulta

Biometrické identifikační systémy

Biometrics identification systems

Disertační práce

Obor: Energetika
Katedra technologických zařízení staveb

Vypracoval: **Ing. Veronika Nídlová**
Školitel: **doc. Ing. Miroslav Andrt, CSc.**

Praha 2014

Prohlášení

„Prohlašuji, že jsem tuto disertační práci vypracovala samostatně pod vedením školitele a uvedla jsem veškerou použitou literaturu. Tištěná a elektronická verze práce se doslovně shodují“.

.....

Ing. Veronika Nídlová

Poděkování

Chtěla bych tímto poděkovat svému školiteli panu doc. Ing. Miroslavu Andrtovi, CSc. za vedení a podporu v průběhu celého doktorského studia, při zpracování disertační práce a za cenné rady a věcné připomínky, které mi za dobu studia poskytl. Dále děkuji celé katedře Technologických zařízení staveb a také celé mé rodině a přátelům za psychickou podporu a věcné rady. Mé poděkování v neposlední řadě patří samozřejmě i firmám (Alarm Absolon s.r.o., Eurosat cs, Variant plus) a státním institucím (Kriminální policie ČR, Ministerstvo vnitra).

Abstrakt

Disertační práce se zabývá problematikou biometrických identifikačních systémů. První část disertační práce popisuje základní členění biometrických identifikačních systémů, jejich principy fungování a vyskytující se rizika.

Experimentální část obsahuje měření biometrických čtecích zařízení, která jsou nejčastěji používaná v České republice. Testování bylo zaměřeno na hodnoty chybného přijetí a odmítnutí uživatele. Dále byla věnována pozornost jednotlivým druhům sabotážních technik. Veškeré tyto aspekty byly zhodnoceny u čteček pro otisk prstu a u čteček pro 3D sken tváře. V neposlední řadě je také věnována pozornost vzniku nových biometrických identifikačního zařízení. Jsou zde popsány možné inovace těchto systémů v závislosti na předchozích měřeních. Byly vytvořeny prototypy systémů pro sejmutí předlohové šablony, které urychlí celý proces zadávání uživatele do systému. Také vznikla inovace 3D čteček tváře přidáním bílé LED diody. Tato inovace zvýšila spolehlivost testovaných biometrických identifikačních systémů. Další vyvinuté systémy se týkaly čteček pro užití v komerčních prostorech a také v automobilovém průmyslu.

V závěrečné části disertační práce je uvedeno shrnutí získaných výsledků. Je zde upozorněno na možné nedostatky stávajících systémů a poskytnuto doporučení pro užívání těchto systémů v praxi.

Klíčová slova: *chybovost, identifikace, otisk prstu, předlohová šablona, pyroelement, sken, tvář, verifikace.*

Abstract

The dissertation deals with the problem of biometric identification systems. The first part of the dissertation describes the basic structure of biometric identification systems, their principles of operation and the risks involved.

The experimental part includes measuring of biometric readers which are most commonly used in the Czech Republic. The experimental part consists of measurements commonly used detectors and data security alarm systems. Testing was aimed at the value of false acceptance and rejection of users. Further attention was paid to the various types of sabotage techniques. All these aspects were evaluated by readers for fingerprint and scanners for 3D face scan. Last but not least attention is also paid to the creation of new biometric identification device. There are described possible innovations these systems based on previous measurements. They were created prototype system for removing artwork templates that speed up the process of entering a user to the system. Also the innovation is the addition of white LED diod to 3D face scanners . This innovation increased the reliability of tested biometric identification systems. Other advanced systems involving readers for use in commercial areas and in the automotive industry.

In the final part of the thesis is a summary of the results. There are alerted to possible shortcomings of existing systems and providing recommendations for the use of these systems in practice.

Keywords: *the error rate, identification, template of fingerprint , pyroelement, scan, face, verification.*

OBSAH

1 Úvod

Biometrie není záležitostí novodobou. Již několik tisíc let před naším letopočtem ji lidé využívali. Důkazem jsou například otisky dlaní v jeskyních na nástěnných malbách, které vyjadřovaly podpis autora. V dávných dobách byla identifikace spojena především s osobním kontaktem a vzhledem lidí. Lidé tehdy žili v malých uzavřených společenstvech, a proto neměli problém se zapamatováním si tváře. Nevědomě tak používali základní a přirozenou vlastnost, kterou i dnes používá každý z nás – vizuální biometrickou identifikaci.

V dnešní době se stále více dostává do popředí problematika biometrických systémů. Rozvoj výpočetní techniky je velmi rychlý, dochází k tlaku na možnost použití automatizované biometrické identifikace. Výrazné snížení výrobních nákladů na komponenty pro výrobu biometrických detektorů podnítilo jejich prudký rozvoj a komerční zavádění do běžného provozu.

Moderní biometrické technologie nabízejí automatizovaný způsob zjištění nebo ověření identity žijící nebo zemřelé osoby na základě měřitelných a nezaměnitelných biometrických charakteristik. Tyto charakteristiky jsou prokazatelné, přesné a jedinečné pro každého jedince a nemohou být zaměněny. První nasazení těchto systému bylo velice úspěšné, bohužel pouze do té doby, než byl nalezen způsob jejich sabotáže. Od té doby je kladen důraz na vývoj bezpečných technologií a při jejich zavádění je potřeba realizovat opatření, která minimalizují možnosti sabotáže biometrických čidel.

V současnosti se biometrické identifikační systémy používají především pro identifikaci osob vstupujících do objektu (např. jaderné elektrárny, letiště, výzkumné ústavy, banky, státní budovy). Další obvyklé užití je pro rozpoznávání osob (např. pro vyhledání konkrétních jedinců z databáze hledaných osob).

Z pohledu budoucího možného použití biometrických identifikačních systémů, je nutné se zaměřit na kritickou infrastrukturu. Pojem kritická infrastruktura označuje důležitý zájem státu, bez kterého by nemohl fungovat a zajišťovat základní potřeby občanů. Nejzranitelnějším prvkem kritické infrastruktury je energetika, na které závisí mnoho dalších odvětví kritické infrastruktury. Narušením výroby, přenosu či distribuce elektrické energie může nastat situace nazývaná „blackout“. Jedná se o rozsáhlý výpadek dodávky elektřiny na určitém místě. Bezpečnostní strategie České republiky staví kritickou infrastrukturu na přední místo pro život a zdraví občanů a pro bezpečný chod státu. Pro stát je tedy velice důležité tuto oblast chránit.

2 Současný stav a charakteristika biometrických identifikačních systémů

Slovo autentizace vyjadřuje průběh činnosti, při které dochází k ověření identity jedince. Výslednou hodnotou je tvrzení v podobě souhlasu či nesouhlasu. Pokud jedinec splní veškeré požadavky a kritéria, je vpuštěn do daného chráněného objektu či k určitým zdrojům. Autentizaci lze rozdělit do tří základních skupin na základě znalosti určité informace (PIN, heslo, aj.), dále na vlastnictví předmětu (čip, čipová karta, aj.) a také na základě biometrické informace (otisk prstu, sken sítnice oka, chůze, aj.). Většinou se v praxi používají kombinace všech tří skupin. Biometrická autentizace se zakládá na předpokladu, že určité tělesné charakteristiky jsou pro každého člověka jedinečné, tudíž se u každého liší a současně jsou v čase minimálně proměnné. [1-6]

Dále je nutné vysvětlit jednotlivé pojmy, jelikož autentizace, verifikace a identifikace jsou častokrát zaměňovány.

Autentizace – celkový proces ověření předpokládané identity subjektu. Po tomto procesu následuje proces autorizace.

Verifikace – při verifikaci jedinec zadá své údaje (heslo, karty, aj.) a pak poskytne požadované biometrické informace. Následně dochází k porovnání s databází. Prvně se v databázi nalezne údaj poskytnutý prostřednictvím karet, pinů či hesel a poté je teprve porovnáván biometrický údaj. Jedná se tedy o porovnávání 1:1. [1-6]

Identifikace – není nutná kombinace metod, stačí pouze sejmout biometrický údaj a poté dochází k porovnávání tohoto údaje s celou databází. Mohou nastat dva případy. V prvním případě nedojde k žádné shodě a uživateli je přístup zamítnut. V druhém případě je potvrzena shoda a uživateli je vstup povolen. Jedná se o porovnání 1:N. [1-6]

Tak jako u každé jiné metody je i u biometrie třeba před jejím uvedením do praxe zvážit určité aspekty:

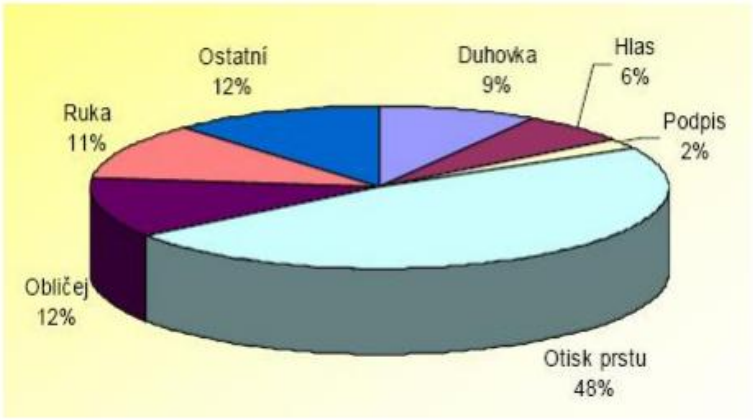
- **přesnost,**
- **rychlost odezvy,**
- **velikost předlohy,**
- **cena.**

Biometrické přístupové a zabezpečovací systémy se dají rozdělit dle nejčastějšího použití na:

- **Snímání otisků prstů**
- **Snímání otisku dlaně,**
- **Rozeznávání hlasu a řeči,**
- **Sken oční duhovky a sítnice,**
- **Rozeznávání obličeje,**
- **Identifikace dle DNA** (problém s rychlostí) – pouze u speciálních postupů,
- **Rozeznávání dle chůze,**
- **Ezoterická identifikace,**
- **Behaviometrická identifikace.** [1-6]

Jednotlivé procentuální zastoupení těchto metod je znázorněno na obr. 1. V části s názvem ostatní jsou zahrnuty metody jako rozeznávání osob dle chůze, oční sítnice a nezmíněné behaviometrické a ezoterické metody. V grafu není zahrnuta identifikace prostřednictvím rozboru DNA, jelikož tato identifikace je samostatná a velice široká vědní disciplína.

Obr. 1 ***Biometrické identifikační systémy a jejich podíl na trhu*** [7]



Mezi ezoterické metody patří sken krevního řečiště ruky, termovizní obraz tváře, otisk ušního boltce a tvar vnějšího ucha, dynamika písma a ruční podpis, otisky rtů a pórů, pleťová spektroskopie, pach lidského těla, metabolická analýza, obsah solí v těle a také rýhování a

tvar nehtu a nehtového lůžka. Tento způsob identifikace je prozatím ve stádiu testu. Zatím se ukazuje tato metoda jako poměrně levná, ale zároveň je velmi náchylná na podvrhy. [1-3]

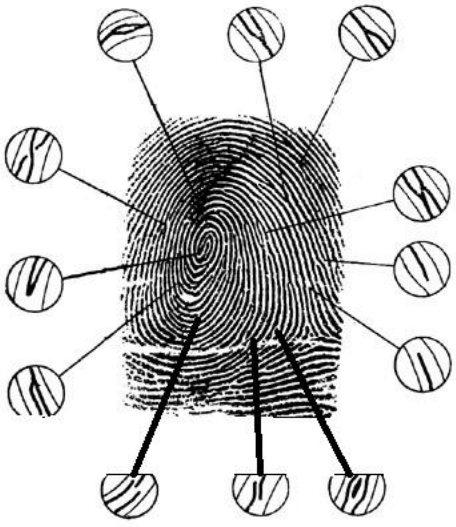
Zvláštní a v posledních letech dosti využívanou metodou je tzv. behaviometrika. Je založena na pozorování vlastností jedince. Mezi zástupce této metody patří styl a rychlost psaní na klávesnici, sledování pohybu počítačových myší. Dále také styl bipedální lokomoce, gesta, mimika i další lidské projevy se řadí do této skupiny biometrické identifikace. [1-3]

2.1 Otisky prstů

Historicky první záznamy o daktyloskopii se objevily odhadem několik tisíciletí před naším letopočtem u Indiánů na území ve státě Indiana. Byly zde objeveny kameny s vyrytými dlaněmi, jejich účel dodnes není znám. Otisky prstů využívali pro identifikaci již v Asýrii a Číně 6 – 7 tisíc let před Kristem a zhruba v letech 1792 – 1750 před Kristem tuto metodu využívala i královna Hanimurabi z Babylónu. První spis o využívání otisku prstů jakožto identifikaci člověka pochází z Číny a sepsal ho Číňan Kio Kung-yen. Číňané otisky prstů využívali při obchodování a rozvodech, kdy manžel musel uvést otisk prstu k důvodům pro onen rozvod. [4, 8, 9]

Jeden z největších přínosů bylo popsání a rozlišení devíti základních vzorů papilárních linií viz obr. 2 u posledních článků prstů J. E. Purkyněm. [4]

Obr. 2 Kresba papilárních linií [4]



Samotný rozvoj otisků prstů v České republice se pojí ke jménu Františka Protiwenského, který po dostudování začal pracovat pro policejní službu a byl pozván do Vídně na školení týkající se antropometrie a daktyloskopie. V roce 1903 byly na jeho popud

zhotoveny první daktyloskopické karty s otisky deseti prstů. [4, 8] Snímání otisků prstů jde poté rozdělit do dvou skupin:

- **klasické snímání daktyloskopických stop**
- **bezprostřední snímání otisků prstů**

Klasické snímání daktyloskopických stop představuje postupy, které využívá především policejní služba. Jedná se zejména o vyhledávání daktyloskopických stop a jejich zviditelnění, dále o zafixování a následné zanesení do daktyloskopické evidence. Bezprostřední snímání otisků prstů je charakteristické pro komerční a bezpečnostní oblasti.[4]

Metoda otisku prstu se dnes využívá ve všech odvětvích. Čtečku otisku prstu můžeme vidět zpravidla u docházkových a přístupových systémů. Dle zmíněných typů se liší jejich použití a také jejich spolehlivost.

V dnešní době máme do různých technických zařízení zakomponovány senzory pro sejmutí otisku prstu. Senzory jsou zařízení, která používají rozmanité fyzikální principy. Tyto senzory můžeme rozdělit podle způsobu kontaktu snímané tkáně se snímací plochou na kontaktní a bezkontaktní. [4, 8, 9]

2.1.1 Kontaktní senzory

Princip kontaktních senzorů spočívá v přiložení prstového lůžka přímo na snímací plochu senzoru. Dělí se na:

- **Optické senzory:** použití prvních optických senzorů je zaznamenáno v rozmezí šedesátých a sedmdesátých let minulého století. Práce těchto senzorů je založena na technologii FTIR – Frustrrated Total Internal Reflection. Jedná se o laserový paprsek nebo hustý svazek optických vláken osvětlující zespodu povrch prstového lůžka, který je přiložen na průhlednou desku senzoru. Odražený světelný tok snímá CCD (Charge Couplet Device) prvek. Papilární linie a brázdy nám určují množství odraženého světla, kde papilární linie odrážejí více světla než brázdy. CCD prvek ovšem odraz světla od brázd nepoužívá jako vyhodnocovací prostředek. [4, 8, 9]
- **Elektronické senzory:** elektronické senzory jsou založeny na elektrickém poli mezi dvěma vodivými a elektrickými deskami. Při přiložení prstu na spodní plochu se změní tvar elektrického pole. Vrchní desku elektronického senzoru tvoří prst (jeho povrch), do nějž je vysílán elektrický signál. K identifikaci slouží vysoce vodivá slaná vrstva tekutiny nacházející se pod nevodivými odumřelými buňkami. Signál je

následně zesílen a přeměněn do elektronického obrazu otisku prstu. Výhoda tohoto typu senzoru je, že při snímání nezáleží na poškození vrchní vrstvy prstového lůžka či jeho vlhkosti. [4, 8, 9]

- **Opto-elektronické senzory:** senzor je vytvořený dvěma vrstvami. Vrchní vrstva, která je vyhotovena z polymeru TFT a přichází do přímého kontaktu s prstem má vlastnost potlačit světlo, které je následně absorbováno skleněnou vrstvou se zatavenými fotodiodami, které převádějí světelný tok na tok elektrický. [4]
- **Kapacitní senzory:** tento typ senzoru je založený na měření elektrické kapacity. Skládá se z velkého počtu vodivých plošek, které jsou od sebe izolovány. Při přiložení prstu dojde skrze papilární linie k přemostění jednotlivých vodivých ploch a brázdy zde zastupují izolanty. V tu chvíli dochází k měření napětí a kapacitních úbytků mezi vodivými ploškami. [4, 8]
- **Tlakové senzory:** papilární linie vytvářejí vyšší tlak na povrch senzoru na rozdíl od brázd, kde je tlak o poznání nižší. Povrch snímací plochy je tvořen z elastických piezoelektrických krystalů. Při vyvinutí tlaku papilárních linií na piezoelektrické krystaly dojde k přeměně tohoto tlaku na elektrický signál a tím dojde k vytvoření obrazu otisku prstu. Tlakové senzory mají stále stejnou spolehlivost i s mokrými prsty. Senzor tohoto typu byl vyvíjen 10 let a na trhu se objevil v roce 2001. [4, 9]
- **Teplotní senzory:** citlivost na změny teplot jsou pro tyto senzory stěžejní. Jde o to, že při přiložení prstu na snímací plochu mají papilární linie vyšší teplotu než brázdy, které jsou od povrchu ve větší vzdálenosti. Díky teplotě můžeme určit zda otisk patří živé či mrtvé osobě, což nám zkvalitňuje celý systém. Touto formou jde určit padělané otisky a ve správnou chvíli zamítnout přístup žadateli. [4, 8, 9]

2.1.2 Bezkontaktní senzory:

Tyto senzory nevyžadují přiložení prstu na snímací plochu. Mají velké plus z hygienického hlediska. Tyto senzory a jejich technologie se stále vyvíjejí. Jejich základní rozdělení je na:

- **Optické senzory:** optické senzory fungují na podobném principu jako u kontaktních optických senzorů. Světelný paprsek je schopen snímat otisk prstu na vzdálenost 30 – 50 mm. Bezkontaktní způsob předchází znečištění snímací plochy senzoru. [4, 8, 9]

- **Ultrazvukové senzory:** opět je zde podobný princip jako u optických senzorů. U ultrazvukových senzorů dopadá krátkovlnný svazek na povrch prstu. Tento svazek se odráží různě od papilárních linií a brázd a slouží k vyhodnocení. Dalo by se říci, že se jedná o velmi citlivý sonar. Jedná se o vysílání zvukových vln s vysokou frekvencí vysílaných jejich zdrojem směrem ke snímanému prstu a vyhodnocování odražených zvukových vln přijímačem, který se nachází kolmo na vysílaný paprsek. [4, 8, 9]

2.2 Oční sítnice

V roce 1976 firma EyeDentify, založená Robertem Hillem, učinila první pokusy snímání sítnice. Vzniklé přístroje byly velice náročné na obsluhu a také velmi drahé, což znemožnilo jejich použití v praxi. Dalším již sériově vyráběným přístrojem byl Eye Dentification Systém. V tomto zařízení byla použita kamera, která za pomoci infračerveného světla byla připojena k počítači, který analyzoval odražené světlo. Při výběru vhodného algoritmu byl zvolen algoritmus jednoduché korelace. Rozpoznávání osob podle sítnice je svázáno s firmou EyeDentify. Ta si řadu principů použitých při rozpoznávání nechala patentovat. Poslední model firmy EyeDentify nazvaný ICAM 2001 byl navržen v roce 2001. Díky uživatelské nepřívětivosti a vysoké ceně byl však později stažen z trhu. Podobný snímač v současné době nabízí firma EyeKey pod modelovým číslem EyeKey 2001. [4, 10]

Identifikace osob prostřednictvím oční sítnice je metoda provádějící verifikaci snímáním a porovnáním obrazu vzoru sítnice. Pro nasnímání cév oční sítnice se používá optická kamera. Tyto snímky se porovnají s databází a následně dojde k identifikaci osoby, která vyslala požadavek o vstup. [4, 10]

Studiem oční sítnice se v třicátých letech minulého století zabývali lékaři Carleton Simon a Isidore Goldstein, kteří zjistili unikátnost vzoru očních cév. Na jejich práci navázal před šedesáti lety Paul Torer, který se domníval, že u jednovaječných dvojčat budou tyto vzory shodné. Jeho výzkum ovšem toto tvrzení vyvrátil a ukázalo se, že u jednovaječných dvojčat se vzor oční sítnice výrazně liší. [4, 10]

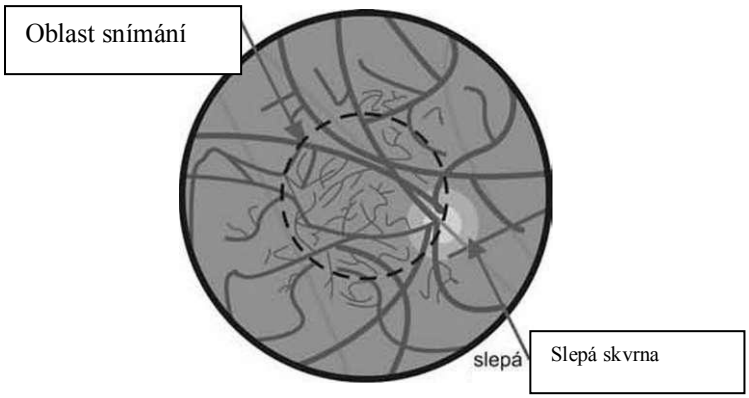
Sítnici nalezneme na zadní stěně oční bulvy a je vyživována krví pomocí cév, které do ní ústí z optického nervu. K poranění sítnice dochází zřídkakdy, a proto je vzor cév za sítnicí neměnný. Oční sítnice rozpozná dopadající světelný tok a informuje mozek o této aktivitě. Obraz, který dopadá na sítnici, se zaostří čočkou, zatímco oční duhovka koriguje velikost dopadajícího světla na sítnici. [4]

V případě onemocnění krátkozrakostí nebo dalekozrakostí se obraz zaostří před nebo až za sítnicí a dochází k dopadu neostrého obrazu. [4]

Na úvod je nutno říci, že pojmy jako snímek sítnice a rozpoznávání osob na základě sítnice, jsou nepřesné a zavádějící, jelikož pro identifikaci osob nelze použít sítnici, ale cévy, které se nacházejí v choroidu za oční sítnicí. Jelikož je zmíněná terminologie zažitá, tak u ní zůstaneme. [4]

Pro nasvícení sítnice se používá infračervené světlo. Sítnice je pro toto světlo téměř průhledná a výsledky nám zprostředkovává až vzor cév v choroidu – viz obr. 3. Ten nám vytváří obraz sítnice, který je následně použit pro identifikaci osob. [4, 10]

Obr. 3 Vzor cév v choroidu [4]



Světle šedý kruh označuje slepou skvrnu, což je místo, které nám ukazuje, kde optický nerv vniká do sítnice. Černá přerušovaná kružnice vyznačuje snímanou oblast (snímána bude jen kružnice, nikoli oblast nacházející se uvnitř této kružnice). [4, 10]

2.2.1 Systém firmy EyeDentify

Kamera sloužící k získání snímků funguje stejně jako retinoskop, který používají oční lékaři. Světelný zdroj vysílá své paprsky na oční sítnici. Světlo je vysíláno v jednotném svazku paprsků, protože je zapotřebí, aby toto záření zaostřila čočka oka na bod na sítnici. Část světla je sítnicí odražena zpět k čočce a ta znovu soustřeďuje paprsky. Dochází k tzv. retro-odrazu, což znamená, že světlo vychází a vchází do oka pod stejným úhlem. Světlo, které se odrazí, snímá kamera. Je potřeba zajistit, aby kruhový snímek sítnice byl vystředěn na kruhové jamce a také aby byl daný jedinec pod snímáním celou potřebnou dobu. Toho je dosáhnuto tím, že je uživateli ukázán cíl, na který má zaostřit. Celý proces snímání je dokončen během deseti až patnácti sekund. Uživatel nesmí během procesu hýbat hlavou a jeho oči musí být otevřené a hledět na barevný cíl zhruba ze vzdálenosti dvou centimetrů od kamery. Pro snímání se zpravidla používá dominantní oko uživatele. Snímání probíhá bez brýlí. Pokud jde o kontaktní čočky, ty se vyndávat nemusejí, ovšem někdy mohou činit

drobné problémy při identifikaci. V dalším kroku je nutné ze snímaného signálu odfiltrovat světelný šum, a to jak z okolního světla, tak i z odrazu rohovky. [4]

Ze snímku, který znázorňuje cévy v choroidu je podstatné pouze mezikruží. Pozornost je věnována nesilnějšímu i nejslabšímu odrazu (největšímu kontrastu), který se dále vyhodnocuje. Uživatel není při snímání vždy ve stejné poloze. Tuto skutečnost řeší rotační algoritmus, který posunuje získaná data o pár úhlových stupňů sklonu hlavy. [4, 10]

Testů tohoto systémů bylo provedeno velice málo, zařízení společnosti EyeDentity, viz obr. 4 bylo podrobeno testům v roce 2001 národní laboratoří Sandia s výbornými výsledky. Ovšem toto testování probíhalo pouze na samotných vědcích a ze 119 snímků byly pouze tři vyřazeny pro špatnou kvalitu a zbylých 116 mělo přesnost rozpoznání 100%. Testování neprobíhalo automatizovaně, a proto se jeví jako neobjektivní. Nevýhodou systému je, že ho nelze použít ve venkovním prostředí a také cena není přijatelná. [4]

Obr. 4 Snímací zařízení firmy EyeDentify [4]

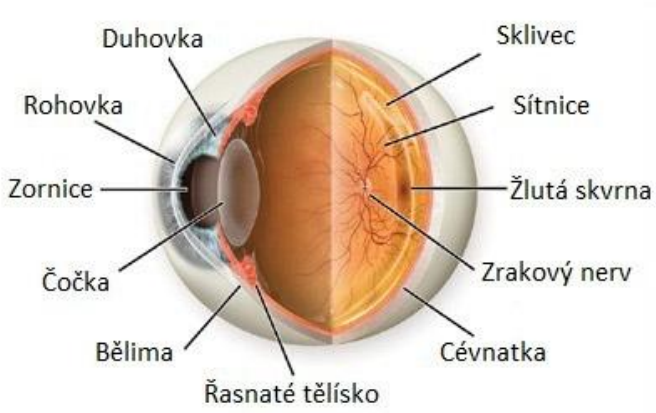
Tato metoda identifikace osob není příliš příjemná a zařízení je pro běžné uživatele poněkud cenově nedostupné. Na druhou stranu je to velmi přesný způsob identifikace. Přístroje pro identifikaci osob na základě vzoru sítnice jsou použity na místech, kde je vyžadována maximální bezpečnost (výzkumná zařízení pro vývoj a ochranu jaderných zbraní, centra, v kterých dochází k velkým transakcím, FBI, CIA, NASA, banky). Dříve byla tato metoda nejbezpečnějším a nejspolehlivějším způsobem verifikace a autentizace, ale v dnešní době je stále častěji nahrazována jinými biometrickými identifikačními zařízeními. [4, 10]

2.3 Oční duhovka

Jedním z hlavních problémů rozeznávání vzorů je i zde klíčová variabilita uvnitř jedné třídy (jedné osoby) a zároveň mezi jednotlivými třídami (osobami). V případě dodržení základního principu, kterým je tvrzení, že variabilita mezi třídami by měla být větší než variabilita v jedné třídě, se považuje vzor oční duhovky za velmi spolehlivou vizuální identifikaci osob. [4, 11]

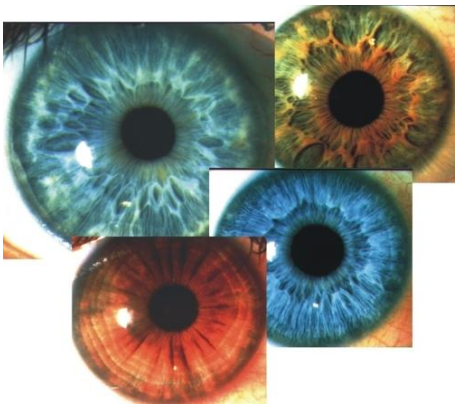
Oční duhovka viz obr. 5 je řazena mezi vnitřní orgán, přesto ji lze vidět zvnějšku. Je poměrně dobře chráněna a zároveň je tento orgán stálý v čase.

Obr. 5 Průřez lidským okem[12]



Duhovka se začíná vyvíjet koncem prvního trimestru těhotenství. Jednotlivé struktury, které tvoří vzor duhovky, viz obr. 6, jsou z velké části dotvořené koncem osmého měsíce a další usazování pigmentu může probíhat ještě v postnatálních letech. Vzor duhovky je dosti složitý a vyznačuje se velkým množstvím typických znaků (např. klenuté vazy, rýhy, hřebeny, krypty, prstence, korány, pihy a klikaté čáry znázorněné na obr. 5. Díky všem těmto znakům i přes její malou velikost (cca 11 mm) je variabilita duhovky vysoká. Je zde také patrný rozdíl ve velikosti zornice a duhovky, kde je poloměr zornice 0,1 – 0,8 násobkem poloměru duhovky. [4, 11]

Obr. 6 Vzory očních duhovek [13]



Pokud jde o geneticky identické oči, je vhodné srovnání levého a pravého oka jedné osoby. U jedince jsou oči geneticky stejné, tak jako i u všech čtyř očí jednovaječných dvojčat.

Snímání duhovky je poměrně nezávislé na úhlu osvětlení a případné niance v úhlu pohledu vyjadřují jen afinní změny. Snadnost nalezení očí na fotografii obličeje a jedinečný kruhový tvar duhovky umožňují spolehlivou a přesnou identifikaci orgánu a vytvoření modelu duhovky s neměnnou velikostí. [4, 11]

Pro zaznamenání rozsáhlých vzorů oční duhovky by měl být poskytován její snímek o minimálním poloměru 70 pixelů. U dosud používaných algoritmů je velikost získaného snímku duhovky mezi 80 a 130 pixely. Používají se monochromatické kamerové systémy (480 na 640) a infračervené pásmo o vlnových délkách 700 nm až 900 nm, které není škodlivé pro uživatele. Jsou i systémy, které pracují s širokoúhlými kamerami, jejíž funkcí je lokalizace očí ve tváři a nasměrování další kamery s výrazně lepšími vlastnostmi, která už má užší záběr a vyšší rozlišení. [4, 11]

Dnes používané algoritmy jsou vytvořené Johnem Daugmanem, jsou to algoritmy nazývané Da93, Da94, Da01. Díky těmto algoritmům mohl být vytvořen software, který je současnými systémy pro rozpoznání oční duhovky používán. Prováděné testy těchto algoritmů jsou velice úspěšné, počet nesprávné identifikace je roven nule. Do testů nebyly zahrnuty úmyslné podvody (sabotáže) např. vytvořením umělé duhovky testované osoby. [4]

Barva očí (taktéž vzhled duhovky) je výrazně geneticky ovlivněna a podrobnosti vzorů geneticky stejných duhovek se jeví jako nekorelované (jako mezi nesouvisejícíma očima). Testování bylo provedeno na 324 lidech (pravá i levá duhovka). Naměřená střední hodnota Hammingovy vzdálenosti byla 0,497 se standardní odchylkou 0,031. U jednovaječných dvojčat hodnoty vypadaly následovně. Měření se zúčastnilo 6 dvojic, HD (Hammingova vzdálenost) činila 0,507. Z toho vyplývá, že feno-typické náhodné vzory, které můžeme vidět na oční duhovce, jsou epigenetické. [4, 11]

Veškeré systémy, které identifikují osobu na základě duhovky, využívají již zmíněný algoritmus. Existuje pět možností jejich využití na letištích:

- **použití jako náhrada pasů při imigrační kontrole přijíždějících cestujících zaregistrovaných jako frequent traveller** (např. Schiphol, Frankfurt, kanadská a britská letiště)
- **pro zrychlený check-in odjíždějících cestujících** (letiště v Tokiu (Japonsko), Bostonu (USA), Los Angeles (USA) a Washingtonu (USA))
- **pohotové řízení přístupu pro piloty a členy posádek (letiště Charlotte** (USA))
- **pro personál letiště při přístupu na letištní plochu a do ostatních vyhrazených prostor** (letiště New York JFK (USA), Albany (USA) a Schiphol (Nizozemí))
- **při kontrole přijíždějících cestujících vůči databázi dříve vyhoštěných osob** (Abu Dhabi a jiná letiště ve Spojených arabských emirátech) [4]

Vesměs se systémy pro rozpoznání duhovky používají v oblasti, kde je žádána vysoká úroveň bezpečnosti (např. v bankovním sektoru, věznicích, jaderných elektrárnách, na letištích, v statutárních prostorách a v mnoha dalších). Řadí se mezi jednu z nejrozsáhlejších aplikací a to především díky velikosti její databáze. Krom důležitých objektů uvedených výše je tato metoda identifikace použita v japonském nájemním domě, kde jsou jednotliví nájemníci zavedeni do databáze duhovek pro tento dům. Když je identifikace osoby kladná, je dotyčný vpuštěn do domu a je mu i přivolán výtah, který je naprogramovaný, aby obyvatele odvezl do příslušného patra. [4, 11]

2.4 Geometrie ruky

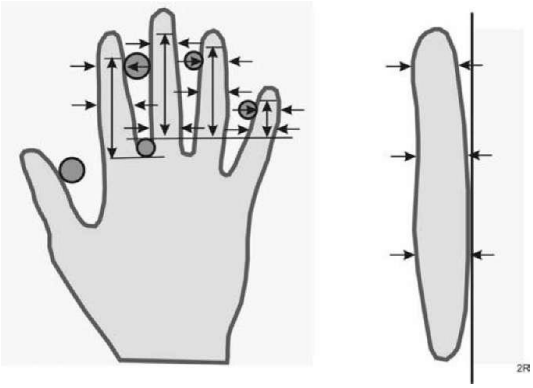
První prototyp přístroje pro měření geometrie ruky byl jednorozměrný. Měřila se pouze délka prstů. Tento systém byl vyvinut v 70. letech minulého století panem Robertem P. Milerem. Použití nalezl při kontrole vstupu do společnosti Shearson Hamill a Western Electric. Nejzásadnější použití bylo v jaderných elektrárnách. První model této technologie nebyl příliš úspěšný vzhledem k jeho jednoduchosti. Vývoj pokračoval a došlo k vyvinutí dvojrozměrně fungujícího systému. Kromě délky jednotlivých prstů se měřila i jejich šířka. Dnes máme již 3D měření, které se rozšířilo ještě o měření výšky prstů. První, kdo vyvinul elektronický skener pro zaznamenání geometrie, byl David Sidlauskas z firmy Recognition Systéme, Inc. [4, 6, 14]

Oproti skenu oční duhovky či sítnice je metoda identifikace osob prostřednictvím skenu geometrie ruky pro uživatele nejméně vtíravou a osobní. Ruka se v průběhu života (samozřejmě až po dokončení vývinu) téměř nemění. Případné změny jsou způsobeny různými aspekty jako je např. změna tělesné hmotnosti, kdy dojde k zvětšení/zmenšení tloušťky jak prstů, tak celé dlaně nebo nemocemi a v neposlední řadě také velkou roli hrají úrazy. K identifikaci slouží délka, šířka, tloušťka prstů a prakticky celý obrys ruky. Je ovšem nutné při měření zanedbat délku nehtů. Jelikož neustále se měnící délka nehtů, která by způsobovala nepřesnost měření. [4, 6, 14]

Celý proces snímání začíná přiložením ruky na horizontální plochu skeneru. Podkladová deska je vyrobena z lesklého materiálu, který disponuje velkou optickou odrazivostí, abychom získali jasný a kontrastní obraz. Tato plocha je opatřena tzv. fixačními kolíky, které zajišťují stále stejnou polohu ruky. Ruka se klouzavým pohybem dostane do fáze, kde mezi prsty jsou ony fixační kolíky viz obr. 7. Poté je vše připraveno k zřízení potřebných snímků k identifikaci. K nasvícení se používají infračervené LED diody. Následně prostřednictvím soustavy zrcadel se obraz odrazí do snímacího zařízení, v tomto případě do

kamery. Pořízené snímky jsou černobílé. Dnes používané skenery snímají desítky až stovky bodů za sekundu a samotné snímání je trojrozměrné. První snímek je proveden kolmo na plochu desky a druhý za pomoci zrcadel vytváří boční pohled. Tento způsob je v praxi nazýván ortografickým snímkováním. [4, 6, 14]

Obr. 7 Umístění fixačních kolíčků [4]



Jako u každého biometrického systému je i zde nutné pořízení vzorového obrazu, který bude sloužit pro následnou verifikaci a autentizaci osob. Tento vzorový snímek je tvořen ze tří obrazů, jako jejich aritmetický průměr. Je ukládán do stálé vnitřní paměti zařízení. Kromě vzorové šablony je uložen do paměti i PIN či nahraný kód karty. Tyto jednotlivé údaje mají přidělené své identifikační číslo, díky kterému se urychlí proces verifikace. Referenční šablona se vzhledem k možnosti změny tvaru ruky, které byly zmíněny výše, musí za určitý čas aktualizovat. Novodobé přístroje mají hodnotu EER (Equal Error Rates) = 0,01 %, což znamená, že každý deseti-tisící uživatel je buď chybně vpuštěn do objektu, či chybně odmítnut. [4, 6]

Po narození mají lidé obě své ruce symetricky shodné, stárnutím a vnějším vlivem okolí se ruce mění. Jedna ruka je vždy dominantní a ta pak určuje skutečnost, zda je člověk pravák či levák a z toho také plyne i to, že používanější (dominantní) ruka bývá častěji zraňována. [4]

Sken ruky své použití nalezne zejména v bezpečnostní oblasti jako komerční přístroj zajišťující verifikaci osob. Tento způsob rozpoznávání osob je velmi úzce zaměřen, obsahuje pro identifikaci osoby příliš málo informací. Většinou se tato zařízení používají v objektech s omezeným přístupem, kde dopředu víme, kolik lidí se zde pohybuje, např. ve věznicích, školách, lékárnách, kasáních, aj.. Na pracovištích slouží i jako docházkový systém zaznamenávající čas strávený v práci. [4, 6, 14]

Praktické uplatnění skenu ruky, viz obr. 8, můžeme z devadesáti procent vidět v amerických, ruských a japonských jaderných elektrárnách. I v České republice se tato

zařízení vyskytují v jaderné elektrárně Temelín. Největší úspěch měl projekt INSPASS (Immigration and naturalization service passanger accelerated service systém. Už z názvu je patrné, že tento systém má za úkol urychlit odbavování stálých cestujících (posádka letadla, diplomaté, obchodníci, herci). Kontrola probíhá na letištích v Miami, Los Angeles, New York, Washington, aj. Funguje to tím způsobem, že cestujícím je vytvořena referenční šablona a přidělena identifikační karta, která obsahuje nahrávku referenčního snímku. Tito lidé mají svůj vlastní vchod, kde vloží svou identifikační kartu do čtecího zařízení a následně je jim udělán sken geometrie ruky. Celý proces zabere od 11 do 20 sekund podle zkušenosti cestujících. Stejný princip je použit i v projektu BASEF, který kontroluje pohyb dělníků mezi pásmem Gazy a západním břehem řeky Jordán, také ve vládních institucích a složkách NATO. Krom takto vysoce střežených a důležitých objektů se sken ruky využívá například na univerzitách pro vstup do menzy, na koleje a do počítačových středisek. [4, 6, 14]

Obr. 8 Přístroj pro sken geometrie ruky [4]

Častěji se můžeme setkat se skenery, které nesnímají trojrozměrně celou dlaň s prsty, ale jen ukazováček s prostředníčkem, viz obr. 9. Jelikož se zmenšila snímaná plocha, tak se v souvislosti s tím zvýšila možnost chybovosti. Celý proces identifikace se však velice urychlí. Rozměry přístroje jsou menší než u zařízení přístroje pro sken celé ruky a verifikace nezabere více než jednu sekundu. Co se týká velikosti paměti, dosahuje až 1000 předlohových šablon. U síťových verzí to může být až 10 000 referenčních šablon. Přístroj je možné rozšířit o klávesnici, čtečky sekundárních identifikačních zařízení (čtečka magnetických zámků a karet) či o bezkontaktní způsob snímání. Zařízení lze používat i jako venkovní. Je ale nutné mít vyhřívanou snímací desku. Pokud tato deska není s výhřevem, může dojít v mrazivých dnech k vysoké chybovosti z důvodu přiložení teplé ruky na studenou snímací plochu. Dojde ke kondenzaci vlhkosti. Tento systém se používá u objektů s menšími požadavky na

bezpečnost, jako jsou například zábavní parky, sportovní a VIP kluby a pro určení docházky. Konkrétně je nalezneme například v americkém Disneylandu, kde se takto zajišťuje nepřenositelnost vstupenky. [4, 6, 14]

Obr. 9 Skener pro dva prsty [4]

2.5 Chůze

V České republice jsou první záznamy týkající se analýzy lidské chůze z roku 1977. Tento lidský jedinečný aspekt je v dnešní době velmi zkoumaný a odvíjí se od něj velké množství bezpečnostních opatření. [15, 16]

Tato kapitola se věnuje chůzi, která se vyvíjí postupem času. První známka pohybu je již u novorozence, který se snaží přetočit ze zad na břicho a zpět, dalším krokem je šikmý sed dítěte. Poté se z lehu a sedu postupuje pohybem po čtyřech (lezení). V následujícím časovém období dojde k verifikaci pohybů, kdy dítě chodí do stran s oporou horních končetin. Veškerý tento vývoj pohybů je brán jako lokomoce. Posledním stádiem je vzpřímená chůze po dvou dolních končetinách, čemuž se také odborně říká bipedální lokomoce. Všeobecně se pod pojmem lokomoce skrývá přesun z jednoho místa na druhé, jinými slovy u lidí se pod pojmem lokomoce rozumí pohyb lidského těla v gravitačním poli svou silou bez jakýchkoli technických prostředků a to za pomoci končetin nebo jiných částí těla. Krom již zmíněné bipedální lokomoce (chůze, běh) patří do lokomoční skupiny lezení, skákání, plavání, let popřípadě volný pád. Pro biometrické účely lze vzít v potaz pouze chůzi a běh. [4, 15-17]

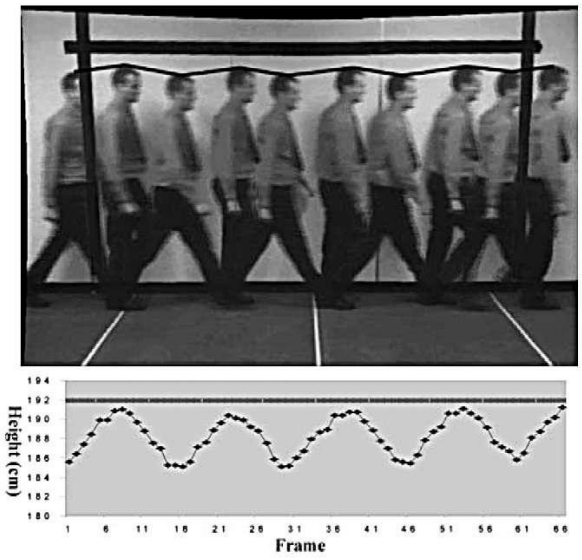
Z kriminalistického hlediska je pohybová aktivita velmi zajímavá a důležitá. Lze z ní vysledovat jak funkční tak dynamické vlastnosti, kde je rozhodující fyziologické hledisko na návyk (tělesná výška, hmotnost, sportovní návyky, zdravotní stav, anatomické vybočení od normálu – zakřivená páteř, ploché nohy, uvolněné kyčelní klouby) a psychologické hledisko na pohybový návyk. Tento způsob verifikace je ovlivňován mnoha aspekty, jako je zatěžování

se těžkým břemenem, nerovnost terénu či bolest hlavy, zad, popřípadě vyčerpání a únava. Ženy při těhotenství mají jinou chůzi z důvodu povolení kyčelních kloubů a jiné posazení kosti pánevní a také jiný vnější vzhled z důvodu zvýšení hmotnosti. Také opilost a halucinogenní a návykové látky ovlivní způsob chůze. [4, 15-19]

Údaje, které jsou analyzovány pro vytvoření závěrů verifikace, jsou stanovení rychlosti lokomoce, grafické znázornění této rychlosti, k čemuž je třeba znát frekvenci pohybu, délku kroku, časové uspořádání kroku a kombinace kinematicko-dynamografických hodnot. [4, 15]

V současné době jsou analýzy pohybu založené na kinematických parametrech. Základem jsou filmové záznamy a rozdělení lidského těla na části. Dochází k snímání stanovených bodů na lidském těle minimálně dvěma zkalibrovanými kamerami současně. Počet kamer (3, 6, 9 i více) a frekvence záznamu závisí na rychlosti a složitosti zkoumané lokomoce. Aby mohly být vysloveny závěry, je zapotřebí zjistit prostorový pohyb jednotlivých částí lidského těla, například horního bodu hlavy, viz obr. 10. Na každém segmentu lidského těla je nutné sledovat alespoň tři body ležící v jedné přímce. Sledování by mělo probíhat minimálně ze dvou míst (dvěma kamerami). To vede ke stanovení prostorové polohy. [4, 15-19]

Obr. 10 Sledování pohybu horního bodu hlavy [4]



Proto, abychom mohli určit souřadnice, je nutné kalibrovat okolní prostor a to tak, že se softwaru pošle zpráva o vzájemné prostorové pozici snímacích zařízení. Díky tomu se pak mohou vypočítat požadované prostorové souřadnice jednotlivých sledovaných bodů. Většinou je to založeno na algoritmu přímé lineární transformace (DLT metoda – algebraické vyjádření

polohy ve více dvourozměrných obrazech a současně v prostoru). První výzkumy se soustředily na pohyb těžiště těla a středu hlavy v souřadnicovém systému (x, y). Dnes se již používají 3D video-grafické metody, které se zaměřují na oblasti:

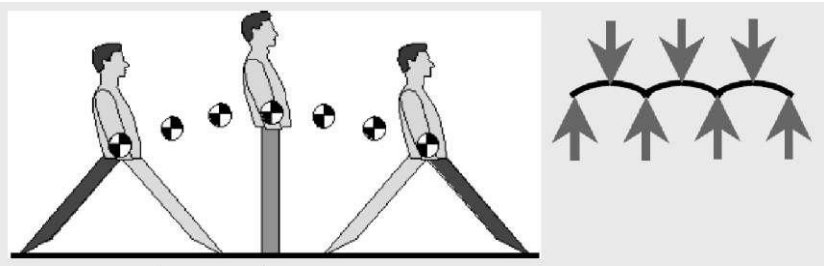
- **prostor v určitém čase,**
- **pohyb těžiště ve vertikálním směru,**
- **pohyb těžiště v horizontálním směru,**
- **pohyb kolenního kloubu,**
- **pohyb hlezenního kloubu,**
- **pohyb kyčelního kloubu,**
- **rotaci pánve a ramen v transversální rovině,**
- **pohyby dolních a horních končetin v určitém čase.** [4, 15, 17]

Metoda používající chůzi k rozeznání osob je poměrně nová, ještě nedokončená. Je zde mnoho problémových a nutno řešitelných oblastí. Velkou výhodou této biometrické metody je, že je bezkontaktní a pro snímanou osobu nikterak vtíravá a nepříjemná. Chůze propojuje mnoho oborů činností jako je medicína, psychologie, sport, modelování lidského těla, biometrie. Do metody rozeznávání osob dle jejich pohybu a také tváře se vkládají veliké naděje. S rostoucími teroristickými hrozbami a jinými trestnými činy je jejich použití stále častější. Mnoho z ostatních biometrických metod nelze použít v určitých podmínkách, například u metody rozeznávání osob na základě tváře může zakrytí tváře (kuklou, maskou) celý proces překazit. To samé platí i u verifikace na základě ušního boltce, který může být úmyslně či nechtěně zakryt vlasy. Také při nevhodném světle (šero, podzemní prostory, přímý sluneční svit, silné umělé osvětlení, aj.) nebo při barvě oblečení, která splývá s prostředím, je proces identifikace nerealizovatelný. Je pravdou, že díky neustálému vývoji si systém s řadou těchto problémů již umí poradit. [4, 15-16]

Systémy pro rozpoznávání osob podle chůze jsou používány v běžném terénu, jako je náměstí, ulice, průmyslové prostory, garážové prostory, peněžní ústavy, kde dochází k sejmutí obrazu a jeho následné poslání na centrální stanoviště k jeho dalšímu zpracování. [4]

U pohybu těžiště ve vertikálním směru (viz obr. 11) lze pouze dodat, že nohy jsou v jedné ose bez ohybu v kolenech a jiných kloubech. Postupem času se v modelování zohledňovaly další hlediska jako pohyb kloubů (kyčle, kolena), také rotace pánve a hrudního koše. Tím docházelo k zmírnění křivky, až tato křivka měla sinusoidní průběh. [4]

Obr. 11 Zjednodušený pohled na pohyb těžiště lidského těla [4]



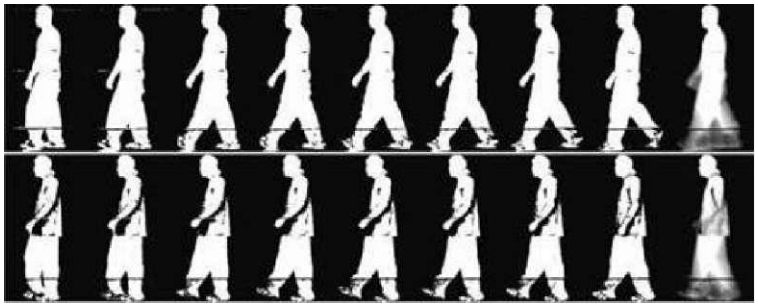
Sagitální kinematika je metoda věnující pozornost pohybu kloubů (kyčlí, kolen, kotníků aj.). U této metody je měřen měnící se úhel končetin od daného kloubu níže, viz obrázek 12, kde je znázorněn onen úhel, který se měří po čas jednoho cyklu chůze. Zprvu byla tato metoda určena a používána pouze v medicíně, ale postupem času ji začala užívat i biometrie.

Obr. 12 Svírané úhly při pohybu v signatárním směru [4]

Biometrické metody, které používají k určení identity chůzi uživatele, se dělí do dvou skupin:

- **Zpracování obrysu pohybující se osoby:** tyto metody extrahují pohybující se siluetu z pozadí, viz obr. 13. Zde je měřena například délka siluety či jiný rozměr. Poté se dané snímky opět porovnávají s databází vytvořenou v průběhu času. [4]

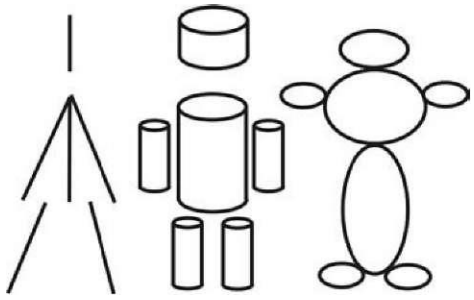
Obr. 13 Počítačově upravený pohyb [4]



- **Modelování pohybu:** tato metoda se soustředí na pohyb horní části těla nebo dolních končetin. Je zde stěžejní dynamika pohybu a ne tvar pohybujícího se objektu. Zaměřuje se na rozměry jednotlivých částí těla a na úhly, které tvoří končetiny při chůzi. Právě u této metody nastává problém s nevhodně zvoleným oblečením. [4]

Pro vytvoření požadovaného modelu se používají tři základní modely (drátěný, cylindrický a oválný), viz obr. 14. Nejpoužívanějším modelem je drátěný, který je oblíbený díky své jednoduchosti. [4]

Obr. 14 Drátěný, cylindrický, oválný model [4]



2.6 Krevní řečiště hřbetu ruky

Jednou z nejznámějších metod biometrické identifikace, při kterých jsou používány CCD kamery, je rozpoznání dle obrazu cév na hřbetu ruky. Vzhledem k nízké pořizovací ceně je v zahraničí tento systém poměrně oblíbený. [4]

Tato metoda je založena na cévách, což jsou žíly a tepny, které okysličenou krev rozvádějí ze srdce a plic k orgánům a zpět k následnému okysličení. Na hřbetu ruky jsou tyto cévy, viz obr. 18 jasně viditelné a jejich rozmístění, velikost a tvar je pro každou osobu unikátní. I tento identifikátor je v průběhu času téměř neměnný. Poloha cév se určuje již v prenatálním stádiu života. Sejmutý obraz cév pro verifikaci je odlišný pro pravou i levou ruku a ani dvojčata tento obraz nemají shodný. [4]

Obr. 15 Krevní řečiště ruky [4]

Snímání a vyhodnocení biometrického obrazu - osoba požadující povolení k vstupu do zabezpečených prostor položí ruku dlaní dospod na snímací desku skeneru. Dojde k prosvícení hřbetu ruky seskupením infračervených diod. Infračervené snímání je citlivé na teplotu. Vzhledem k tomu, že krev roznáší tepelnou energii, jsou pak na pořízeném snímku velmi dobře vidět jednotlivé cévní svazky. Snímek je pořízen černobílou CCD kamerou s šestnácti stupni šedi. [4]

U metod verifikace osob je velmi důležité potvrdit, že testovaný subjekt je živý. V tomto konkrétním případě je vše spojeno již se zmíněnou tepelnou energií, kterou tok krev zajišťuje. [4]

Pro následné zpracování se vybere vhodný algoritmus a pomocí něj se vytváří různé obrazové změny, které mají za úkol zmírnit či úplně odstranit nechtěné šumy a provést vykreslení cév (skeletizaci) s následným vytvořením binarizované biometrické šablony. Je nutno také počítat s různou vzdáleností cév od povrchu kůže a se změnou jejich tloušťky, která se mění vlivem teploty. Uživatelsky příjemné je, že ruka není nikterak fixována, jak tomu je u identifikace dle geometrie ruky, při které se používají mezi-prstové zarážky. Na obraz je pohlíženo vektorově. [4]

Použití tento systém nalezl v bankovních automatech, při odemykání a startování automobilů, také ve Velké Británii na vysokých školách pro kontrolu identity studentů. Skenery krevního řečiště bývají často vybaveny čtečkou čipových karet. Na těchto kartách je nahrána předloha držitele a data jsou nepřenosná. [4]

Pro bezkontaktní snímání lze použít i dlaň ruky, viz obr. 19. To se využívá zejména pro přístup k počítačům, kopírkám, tiskárnám a také v obytných budovách v Tokiu, kde krom skeneru je i potřeba vymačkání PINU a poté je obyvatel vpuštěn do objektu, apod. Jednou z nevětších výhod bezkontaktního skenování je zajištění vysoké hygienické bezpečnosti. [4]

Obr. 16 Bezkontaktní snímání krevního řečiště ruky [4]

2.7 Identifikace na základě tváře

Identifikace na základě tváře se vědomě používá již odpradávna. Lidský mozek automaticky při pohledu na osobu porovnává její vzhled s obrazem, který má již z dřívější doby uložen v paměti. Celý tento proces trvá mozku pouhý zlomek sekundy (20ms). Do dvacátého století sloužila tvář k bezprostřední identifikaci bez zásahu techniky. Krom tohoto důvodu byla často zachycována na portrétech a freskách. Od dvacátého století se věda začala zabývat strojovým vyhledáváním a rozpoznáváním lidských tváří. [20-22]

Procesy probíhající v mozku při identifikaci jsou rozděleny do dvou skupin a to na mozkové buňky, které ukládají tváře do paměti a na buňky sloužící k následnému rozeznání. Buňky neuronů mají horizontální i vertikální propojení, která mají specifický smysl. U lidí bylo dokázáno, že novorozenec je schopen během dvou dnů používat rozeznávací schopnosti a již po dvou dnech dokáže rozeznat svou matku. Při rozpoznávání tváří pracuje především pravý parietální mozkový lalok. Obecně je pravá mozková část spojena s obrazovými a prostorovými vjemy a levá část se zabývá abstraktním myšlením (matematické, jazykové znalosti). [22]

Strojová a vizuální identifikace osob pracuje s různými metodami. Tyto metody se od sebe velmi liší, jedná se o metody:

- **Grafická metoda identifikace na základě fotografického portrétu**
- **Metoda založená na rozpoznávání obličejových rysů**
- **Metody založené na informaci o barvách**
- **Metoda založená na geometrických tvarech a identifikačních markantech**

- **Metoda deformačních modelů**
- **Metoda neuronových sítí pro rozpoznání tváře**

2.7.1 Analyticko-statistická metoda identifikace na základě fotografického portrétu

Tato metoda je postavena na záchytných bodech a liniích, které charakterizují jednotlivé osoby.Při výzkumech bylo dokázáno, že pro identifikaci postačí 12 základních antropologických bodů, kterými jsou vnější horizontální body rtů,bod spodní hrany nosu,vnitřní a vnější koutky očí,bod, kde nos přechází v čelo, body na chrupavce ucha a body přechodu ušního lalůčku do tváře. [4]

Dojde-li ke spojení všech těchto bodů, získá se 66 úseček, které budou ve velké míře vyjadřovat prostorovou i lineární identitu lidské tváře. Prostřednictvím této metody lze porovnat a vyhodnotit shodnost dvou fotografií. Jedná se o vizuální typ identifikace stejně jako u grafické metody. [20, 21]

2.7.2 Grafická metoda identifikace na základě fotografického portrétu

Tato metoda má kořeny v deskriptivní geometrii. Každý geometrický tvar, samozřejmě i tvář, je brána jako soustava bodů, mezi kterými jsou pro identifikaci důležité body, tzv. markanty. U této metody je důležité brát v potaz natočení obličeje. Jednotlivé body jsou pak propojeny kružnicemi a přímkami. V bodech protnutí těchto kružnic vznikají spojnice a jejich postavení je následně porovnáno mezi sebou. Podle tohoto postupu se pak dá určit, zda se jedná o tutéž osobu, či nikoli. [20, 21]

2.7.3 Metoda založená na rozpoznávání obličejových rysů

Kontura obličeje je další velmi důležitou charakteristikou pro identifikaci na základě obličeje. Problémem u této metody je určit přesnou konturu, jelikož současné algoritmy mají na detekci hran omezení. Tato metoda využívá přechodu barev v obličeji (vrhání stínu). Dle těchto rozdílů lze určit umístění a tvar nosu, očí, úst aj. [20, 21]

2.7.4 Metody založené na informaci o barvách

Tato metoda je vhodná pro určení obličeje v barevně diferenciovaném prostředí. Lidé stejné rasy mají velmi podobné zbarvení jednotlivých záchytných bodů. Pro oblast očí je typická barva stínů, nos je jinak barevně výrazný a ohraničený stíny. Tato metoda není vhodná do příliš jasných či naopak tmavých prostor (osvětlení). [20, 21]

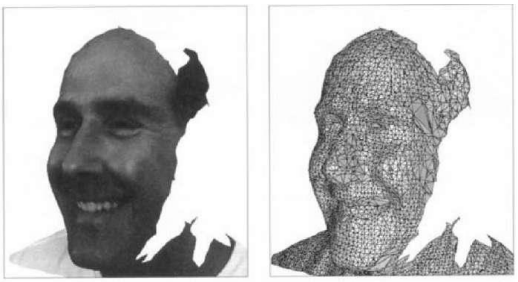
2.7.5 Metoda založená na geometrických tvarech a identifikačních markantech

Tato metoda je pro lidi běžnou a každodenní záležitostí. Tvář člověka si zapamatujeme dle jedinečných znaků a stejně tak je tomu i ve strojové identifikaci. U tohoto typu identifikace záleží na tvaru nosu (šířka, délka), úst, uší, očí, brady. Důležitými markanty jsou i tvar obočí či vzdálenost očí. Nedostatkem metody založené na geometrických tvarech je, že ne vždy dojde k zachycení těchto bodů z důvodu změny tvaru markantů, které je způsobené emocionálním vzruchem. [20, 21]

2.7.6 Metoda deformačních modelů

Pro identifikaci dle tváře lze použít i zakřivení invariantního (neměnného) objektu. Jde o využití trojrozměrného obrazu tváře a jeho pokrytí rovnoměrnou sítí horizontálních a vertikálních pravoúhlých čar, viz obr. 17. Dle hustoty čar (jako vrstevnice známe z map) lze usuzovat výšková maxima a minima, popřípadě rozeznat jedinečné linie (rysy tváře). Pokud dojde ke změně výrazu ve tváři, dojde ke změně křivek, vzdáleností nebo úhlů mezi nimi a obraz se dle toho upraví. [4]

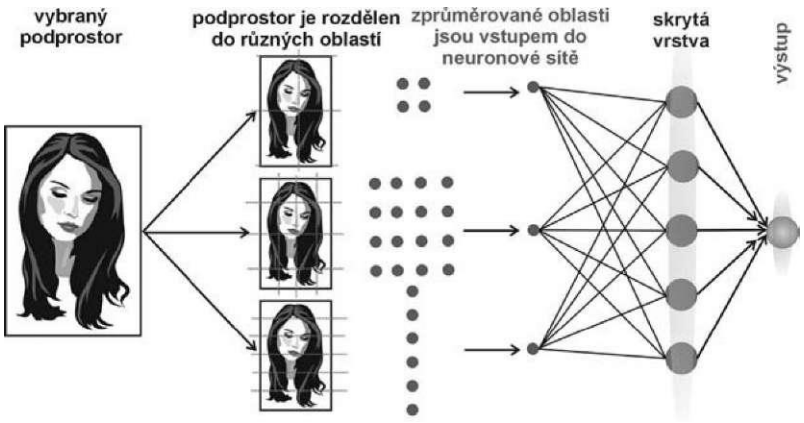
Obr. 17 Tvář vyjádřená síťovým grafem[4]



2.7.7 Metoda neuronových sítí pro rozpoznání tváře

Zde jsou dvě kategorie. První kategorie používá hlavní znaky identifikace a jejich propojení různými metodami, kde neuronové sítě slouží pouze pro klasifikaci (konečné rozpoznání) tváře. V druhé kategorii jsou neuronové sítě, které se používají jak pro identifikaci markantů, tak i pro následné konečné vyhodnocení. Na obrázku 18 je zobrazena detekce tváře pomocí komplexní metody neuronových sítí. Plocha vybraného podprostoru je třikrát jinak rozdělena. U prvního je obraz rozdělen na čtvrtiny (detekce očí a nosu), ve druhém na šestnáctiny (detekce očí a nosu)a v posledním na šest horizontálních pásem (detekce obočí a úst). Vždy je hodnota zprůměrována a slouží jako vstupní hodnota do neuronové sítě. Tento způsob vyhodnocení je poměrně rychlý díky malému počtu přítomných vazeb. [4, 20, 21]

Obr. 18 Princip komplexní neuronové sítě pro detekci obličeje[4]



2.8 Ruční písmo a podpis

Jako další do skupiny behaviorálních metod patří i ruční písmo a podpis. Každá osoba se prostřednictvím svého podpisu reprezentuje. Svým podpisem stvrzujeme různé druhy dokumentů (formuláře, šeky, cenné papíry, kupní smlouvy, právní smlouvy aj.) Dříve byl styl písma osoby zkoumán především kriminalisty, kdy šlo třeba o prokázání pravosti dopisu na rozloučenou. Podle písma se také zkoumala a dodnes zkoumá duševní a myšlenková identita. Dnes je písmo využíváno k sestavení profilu určitého jedince. Tuto metodu nepoužívají pouze psychologové, kteří hledají souvislost písma a nemocí, ale i personalisté, kteří tak určují předpoklady jedince pro výkon daných profesí. Při rozhodování o pravosti podpisu dochází k velmi subjektivnímu procesu, pokud se ovšem nejedná o posuzování za pomocí moderních technologií, které kromě statického obrazu zkoumají i proces vytváření podpisu (psaní podpisu). Jde tedy o zkoumání rychlosti psaní podpisu v čase, tlak hrotu pera, směr a návaznost jednotlivých písmen, interpunkce aj. Těmto technologiím se říká dynamická verifikace. [4, 23, 24]

Písmo je ovlivněno psychologickými a fyziologickými postupy, které vytvářejí jeho jedinečnost. Kromě již zmíněných postupů mají vliv i anatomické vlastnosti (flexibilita kloubů, stav svalstva, stavba kostí, zdravost zraku, aj.). Pojem individualizace čili jedinečnost písma vyjadřuje odchýlení od školní normy a odlišnost písma u jednotlivých jedinců. Psaní ovlivňují dva základní aspekty. Je to technický návyk (způsob psaní – držení psacího prostředku, náklon papíru, psací podklad, aj.), dále pak grafický návyk (psát jednotlivé znaky rychle a čitelně) a také pravopisný návyk (správné užití pravopisu a dodržení pravidel pro psaní určitých textů). Výjimečnost písma každého z nás vychází z šedé kůry mozkové. [4, 20, 21]

Znalci, kteří zkoumají písmo, studují na škole českých znalců. Jednou ze znalci používaných metod je grafosynkritická analýza zkoumající písemné projevy globálně.

To znamená, že se věnuje jak jazykové stránce tak i grafické, a je kombinací analytických, srovnávacích a gravimetrických metod, které jsou následující:

- **Grafická stránka psaného projevu**
    - **obecná rovina –** sklon, velikost písmen a mezer, tvar a šíře odstavců, umístění a velikost nadpisu, podpis aj..
    - **zvláštní rovina –** jednotlivé části písmene, provázanost písmen a interpunkce.
- **Jazyková stránka psaného projevu**
    - **lexikální stavby –** zařazení slov a slovních spojení do skupin dle stylu, oblasti, oboru, doby užívání
    - **gramatické stavby –** zvláštnosti jazykového projevu
    - **modální stavby –** porovnání skutečnosti v autorově koncepci a způsob projevu (autor hodnotí jev jako skutečný, možný, nutný, doporučující, aj.)
    - **aktuální členění –** srovnání projevu jako celku (věta) a částí (slova) [4, 23, 24]

Stejně jako u ostatních biometrických systémů tak i u písma je vše založeno na určení toho, co obsahuje stopa písma a také jak písemný projev vznikl. To celé je postaveno na kineziologickém rozboru. V odvětví kriminalistiky mají při rozboru písma vliv vnější a vnitřní faktory, které byly zmíněny výše. Při vyhodnocování podpisů nestačí pouze vnitřní a vnější efekty, ale je nutno brát ohled na následující metody:

- **Kvalitativní metody –** zakládají se jen na pozorování
    - **Intuitivní metoda –** zpravidla se používá jako doplňující, dříve ji využívali učitelé pro posouzení svých studentů.
    - **Grafologická metoda –** zkoumá originalitu psacího pohybu, která vychází nejen z mechanických pochodů, ale i z psychických, a také pohlíží na mravní vzdělání jedince. Tato metoda se používá spolu s intuitivní a analytickou metodou.
    - **Patografická metoda –** vychází z psychických a tělesných poruch či nemocí mající vliv na psací pohyb. Tato metoda je především diagnostická.

- **Srovnávací metoda –** je založena na odpovídajícím úsudku. Srovnávat se může buď písmo s písemným projevem nebo srovnání písma s písemným ideálem, který si vytvoří samotný posuzovatel.
- **Funkcionální metoda –** znázorňuje vztah mezi určitým počtem jevů (znak – čitelnost rukopisu).
- **Analytická metoda –** skládá se ze dvou částí, z analýzy samotného písma a z psacího pohybu (se zaměřením na: rozbor písma na základní tvarové prvky, základní vlastnosti, grafologický rozbor, rozbor pro identifikaci jedince).
- **Gravimetrická metoda –** zaměřuje svůj výzkum na přesnost popisu, který si vyžaduje stanovení měrné jednotky. Touto metodou dochází ke zkoumání velikosti písma, velikosti jednotlivých částí písmene, velikosti úhlů, přítlaku, rytmu, délky aj. To požaduje modernější technické přístroje a nástroje.
- **Kombinace posudkových metod –** je podmínkou, pokud se jedná o vědecký posudek, jedná se o doplnění a zpřesnění konečného závěru. [4, 23, 24]

- **Kvantitativní metody –** jde o převod kvalitativních údajů do určitých tříd či měřitelných záznamů. Základ tvoří zakódování písma a jeho následné porovnání s předlohou, která je uložena do pamětí vyhodnocovacího zařízení. Při použití automatického snímání se vypouštějí velmi důležité aspekty pro identifikaci osob. Patří mezi ně například směr pohybu při psaní, plynulost a návaznost tahů pera, aj. Co ovšem stroj snímá, je plošné rozvržení psaného textu, velikost pohybů při psaní písmen, sklon, velikost písmen a vzhled interpunkčních znamének, mezery mezi slovy, větami a řádky. [4, 23, 24]

Rozdíly v písmu mužů a žen - znalci uvádějí psychické rozdíly mezi muži a ženami, které se promítají i do písma. U žen se častěji vyskytuje:

- **konkrétní myšlení –** omezení tvarů písmen na hlavní tahy,
- **větší citovost –** ovlivnění citem, riziko nevěrnosti, řešení problémů s citem, subjektivní postoje (projev tohoto je větší náklon písma na levou stranu a větší délkové rozdíly,
- **sebecit –** optimální a vyrovnaný mnohem více než u mužské populace (projevem je maximálně střední velikost písma). [4, 23, 24]

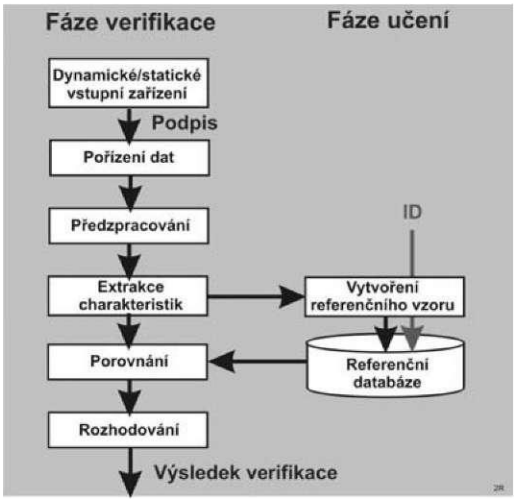
Verifikace probíhající na základě vyhodnocování podpisu má velikou výhodu v tom, že podpis jako takový se nedá ztratit, odcizit či zapomenout. Je používaný v běžném životě – podpisy smluv, finančních transakcích, bezpečnostní zajištění vstupu, či přebírání hmotných věcí. Vyskytují se dva základní typy systémů:

- **Off-line systém:** u této metody se jedinec podepíše na papír a následuje optická diagnostika skenerem nebo kamerou. Poté dojde ke shodě či neshodě s referenčním záznamem podpisu (statická metoda).
- **On-line systém:** zde je charakteristické získávání podpisu v reálném čase a to speciálním tabletem nebo přímo k tomu určeným perem či jiným snímacím hardwarem. U veškerých těchto systémů dochází k zachycení jak statických tak i dynamických znaků výsledného podpisu v průběhu celého podpisového aktu (dynamická metoda). [4]

Celý proces identifikace na základě podpisu je sestaven ze dvou částí – etapa určení a etapa testování, viz obr. 19. Při etapě určení systém využívá extrahovaných charakteristik z více předlohových vzorů pro vytvoření databáze podpisů. Osobě vytvářející referenční šablonu je přiděleno identifikační číslo (ID), které spojuje osobu se vzorem její referenční šablony podpisu. U etapy testování (ověření podpisu) identifikovaná osoba předloží své ID a následně se podepíše na vstupním zařízení. Poté identifikační systém díky ID číslu vyhledá v databázi vzorový podpis a porovná ho se sejmutým podpisem. Výsledkem pak je výrok, jestli byla osoba rozpoznána či nikoliv. U každého takového systému se objevuje hrozba padělku. Existují tři základní druhy falsifikátů:

- **„jednoduchý“ padělek** - „padělatel“ se o falšování nepokouší záměrně, ale jeho podpis se jen náhodně shoduje s podpisem jiné osoby, která má také uloženou referenční šablonu v databázi.
- **Substituční či nahodilý padělek –** osoba úmyslně zadá podpis a vyčkává, zda v databázi není někdo takový, kdo by měl stejný podpis. Pokud dojde ke shodě, je uživatel vpuštěn do systému, ale neví pod čí identitou.
- **Záměrně vytvořený padělek –** jedinec ví, za kterou osobu se chce vydávat a zcela úmyslně napodobí její podpis ve všech stránkách. [4, 23, 24]

Obr. 19 Etapy verifikace [4]



Jako u většiny metod tak i při identifikaci osob podpisem je u fáze předzpracování použita řada algoritmů (čištění signálu, zjednodušení – vznik skeletu podpisu - jen kontura, skeletizace, segmentace, vyhlazování a normalizace – odstranění nevýznamného šumu a poté normalizace buď lineární, nebo nelineární, pruhování – každý pixel v spektru šedi je srovnán s předdefinovanou hranicí podle toho, zda hranici převyšuje či nepřevyšuje a je zařazen do kategorie 0 a 1 – přeměna do binárního obrazu, aj. Například u metody off-line probíhá klasifikace dvěma způsoby:

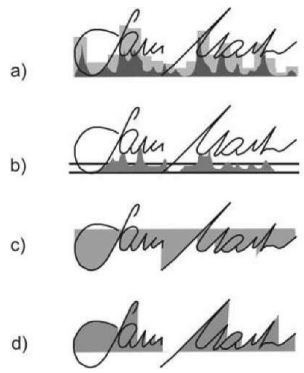
- **textové nezávislé –** u nich nezávisí na tom, co pisatel při identifikaci píše, využívá se texturové analýzy, transformačních metod a histogramů,
- **textově závislé –** v tomto případě závisí na tom co uživatelé píší. Vyskytují se zde geometrické a topologické rysy – využívají se uzavřené smyčky, hraniční překřížené body na křivce podpisu, plochy, které jsou ohraničeny body vyskytující se v podpisu, viz obr. 20. [4, 23, 24]

Obr. 20 Body na křivce podpisu [4]

Konečné vyhodnocování pak může probíhat několika způsoby, ovšem nejčastější bývají:

- **porovnání významových bodů –** linie trajektorie je ztenčena a jsou z ní vybrány speciální body (koncové body, body, ve kterých se tahy pera obrací, body, kde se tahy křižují, aj.), viz obr 21. Výsledně se porovnávají tyto body s body vyznačenými na referenční šabloně,

Obr. 21 Charakteristiky písma (a-hustota a vektor linie tahu, b-vertikální hustota linie tahu, c-horní uzavřená oblast vektorů, d-dolní uzavřená oblast vektorů) [4]



- **klasifikátor souseda –** je používaný v off-line metodě, využívá vektory vlastností. Nejčastěji se používá klasifikátor nejbližšího souseda a K-klasifikátor nejbližšího souseda. Sejmutý podpis verifikované osoby je porovnáván s celou databází podpisů a je vybrán „nejpodobnější“.),
- **neuronové sítě –** nejčastěji používaná metoda. Jde o kombinaci několika typů klasifikátorů. Každý z klasifikátorů vyhodnocuje nezávisle na ostatních a výsledek je tvořen přidělením vah těmto klasifikátorům. [4, 23, 24]

Pro použití takovéto metody k identifikaci osob je velmi důležité dodržovat legislativu. Legislativa týkající se digitalizace podpisu se na jednotlivých územích (Evropská unie, Spojené státy americké) značně liší. V Evropské unii jedinec dávající elektronický podpis tím zároveň vydává souhlas s obsahem digitálního dokumentu. Verifikace podle podpisu jedince je brána jako doplňková záležitost, stejně tak jako například PIN, písmenné a číselné heslo, aj. V USA má jakýkoli podpis, tedy ruční i elektronický podpis, tentýž právní status (=podpis na papír perem). Tento zákon, který toto upravuje, je platný od roku 2000. [4]

2.9 Dynamika stisku počítačových kláves

Dynamika stisku počítačových kláves je metoda, která se řadí mezi nejužívanější behaviorální metody. Princip rozeznávání spočívá na softwaru v počítači, který zajistí spolehlivou verifikaci osoby za pomoci počítačové klávesnice. Tato charakteristika je stejně jako ostatní behaviorální metody částečně ovlivněna aktuálním fyzickým a také psychickým stavem uživatele. U celé metody je stěžejní doba stisku jednotlivých kláves při psaném projevu. Systém může fungovat dvojím způsobem. Za prvé jako verifikace uživatele dle zapsání loginu a hesla a za druhé pak lze průběžně kontrolovat identitu uživatele a to po celý časový úsek práce s počítačem. [4, 25, 26]

Vytvoření identifikační předlohy osoby závisí na několika aspektech. Jednotlivé informace o stisknutých klávesách jsou zaznamenány operačním systémem hardwarovými přerušeními. Operační systém zaznamenává jak stisk klávesy, tak i její následné uvolnění. Z těchto hodnot lze odvodit dobu, po kterou je klávesa stisknuta. Někdy ovšem může nastat problém z důvodu klávesových zkratek, jako jsou například „Ctrl + C“, „Ctrl+V, „Alt + F4“ a další. V těchto případech uživatel stiskne obě klávesy, což zkresluje celý proces. Krom doby stisku kláves lze verifikovat dle rychlosti psaní (počet stisknutých kláves za dané časové rozpětí), dále dle četnosti chyb (kolikrát uživatel stlačí klávesu Backspace za určitou délku textu), také dle způsobu psaní velkých písmen (jakou klávesu uvolní uživatel jako první, zda Shift či daný znak) a v neposlední řadě také sílou vyvinutou na klávesu při jejím stisku. [4, 19]

Když budeme brát prvopočátky, verifikování probíhalo dle zapsání uživatelského jména a hesla, zde se sledoval interval mezi stisky jednotlivých kláves. Nejprve uživatel vytvořil jako u jiných metod referenční šablonu. U zkušeného písaře pak proběhla verifikace na první pokus, kdežto u méně zkušeného může být pokusů i více. [4, 15]

2.9.1 Kontinuální verifikace

U kontinuální verifikace je jedinou měřenou veličinou čas (milisekundy), po který je stlačená klávesa. Byly provedeny různé testy, např. na slovech authentication a theoretical. Výsledkem byly posloupnosti:

- **authentication:** 0 a 180 u 440 t 670 h 890 e 1140 n 1260 t 1480 i 1630 c 1910 a 2010 t 2320 i 2600 o 2850 n
- **theoretical:** 0 t 150 h 340 e 550 o 670 r 990 e 1230 t 1550 i 1770 c 1970 a 2100 l

Jednotlivá čísla vyjadřují čas v milisekundách, po který byla klávesa s daným znakem stisknuta. Tyto údaje slouží k výpočtu „R“ a „A“:

- **„R" hodnoty:** V „R“ hodnotách je při vyhodnocení shody brán v potaz jak psychologický tak fyziologický stav uživatele. „R“ proto, jelikož se jedná o relativní informace, protože jsou získané výsledky do jisté míry ovlivněny. [4]
- **„A" hodnoty:** „A“ hodnoty nám vyjadřují absolutní rychlost psaní na klávesnici. [4]

Výše popsané hodnoty „A“ a „R“ lze použít pro několik způsobů, které slouží k určení uživatele:

- **klasifikaci –** vzorek X náleží jednomu ze známých uživatelů (z uložené databáze) a úkolem je rozhodnout, kterému konkrétnímu uživateli patří,
- **autentizaci –** zde je opět vzorek X, ale tentokrát konkrétního uživatele U a je na systému, aby určil, zda jde o shodu/neshodu (X patří uživateli U, X patří někomu jinému z databáze nebo X patří někomu úplně cizímu),
- **identifikaci –** kde je opět vzorek X, který je předložen systému a ten odpoví, zda vzorek X je uživatele U, nebo vzorek X patří někomu cizímu. [4]

2.9.2 Statická verifikace

Téměř všechny systémy využívají statickou verifikaci, jejímž základem je dynamika stisku kláves. Při první fázi, kterou je registrace, tzv. vytvoření předlohové šablony, uživatel zadá několikrát za sebou své přihlašovací údaje (nebo jiný předem zvolený text), z čehož se následně stanoví předlohový vzor. [4, 25, 26]

2.9.2.1 BioPassword

V dnešní praxi se nejčastěji setkáváme s termínem BioPassword. Už z názvu je patrné, že jde o systém, který zabezpečuje přístup, a to nejen do samostatných stanic, ale i do PC zapojených do lokálních sítí. Je to systém, který měří čas mezi stlačením kláves a také dobu, po kterou jsou jednotlivé klávesy stisknuty. U této metody se pro vytvoření předlohy používá zapsání loginu a hesla uživatele, celkem ho musí napsat patnáctkrát (tato hodnota se odvíjí od nastavení obsluhou, doporučené je 15krát akci opakovat). [4]

Takovýto systém se používá zejména tam, kde je vyžadována vysoká bezpečnost týkající se přístupu k počítači. Většinou jej lze vidět v bankách, v organizacích jako je CIA a FBI a u tajných státních informací. [4]

3 Cíle disertační práce

Hlavním cílem této disertační práce je vytvoření návrhu řešení biometrického identifikačního systému a zpracování návrhů inovací stávajících biometrických identifikačních systémů. Hlavních cílů bylo dosaženo prostřednictvím dílčích cílů:

- **zjištění chybovosti (hodnot FAR a FRR) biometrických čteček otisků prstů**
- **zjištění chybovosti (hodnot FAR a FRR) biometrických 3D čteček obličeje**
- **zjištění rizik z pohledu sabotáže biometrických identifikačních systémů**
- **na základě vlastních testů a jejich zpracování zvolit proměnné, které ovlivňují správnou funkčnost biometrických identifikačních systémů**
- **zpracování získaných podkladů pro následné využití výsledků**

3.1 Stanovení hypotéz

Cílem práce je dále ověřit několik základních hypotéz, které přímo souvisí s biometrickými identifikačními systémy.

Hypotéza č. 1: Poranění prstových lůžek ve vysoké míře ovlivňuje hodnoty chybného odmítnutí uživatele.

Hypotéza č. 2: Schopnost identifikace a chybovost (hodnoty FAR a FRR) by měla být u obou 3D čteček obličeje (Multibio700 a IFace302) shodná v důsledku použití stejného vyhodnocovacího softwaru.

Hypotéza č. 3: Znečištění obličeje vysoce ovlivňuje hodnoty chybného odmítnutí uživatele.

Hypotéza č. 4: Přísvit pomocí bílých LED diod snižuje chybovost 3D čteček obličeje oproti použití samostatného integrovaného Infra přísvitu z výroby.

Hypotéza č. 5: Použití jiného propojení s koncovým prvkem než po sběrnici Wiegand a zároveň využití systému centrální jednotky snižuje bezpečnost ochrany vstupu.

4 Metodika disertační práce

Měření probíhalo v laboratoři zabezpečovací techniky na Technické fakultě České zemědělské univerzity v Praze. Veškerým měřením předcházely rozsáhlé přípravy a to proto, aby byly nastoleny stejné podmínky testování pro všechny subjekty. Nejprve bylo nutné zajistit všem pořízeným čtečkám stejné podmínky pro měření. Tyto podmínky vycházely z norem ČSN EN 50133, ČSN ISO/IEC 19794, ČSN ISO/IEC 19794, ČSN ISO/IEC 27006, ČSN ETSI EN 302 77 a zároveň z doporučení daných výrobcem. Všech pět čtecích zařízení bylo upevněno na dřevěnou desku a to do stejné výše. Tento panel byl vytvořen pro snadnější manipulaci a k nastavení stejných okolních podmínek při měření. Měřící panel, viz příloha 4, byl umístěn na stěně ve výšce 1,2 metru a byl uchycen na kolejnice, které zajišťují horizontální posun panelu. Na kolejnici byla vytvořena vysunovací zarážka, která zajišťuje stejnou pozici čteček při měření. Na podlaze byl nakreslen pruh, který vyznačoval vzdálenost měřeného subjektu od měřícího panelu. Tato vzdálenost byla 0,5 metrů od panelu. Dále bylo zajištěno umělé osvětlení ve vzdálenosti 2,2 metrů od biometrických čteček. Testované objekty mají být dle doporučení výrobce instalovány ve vzdálenosti minimálně 3 metrů od protějšího okna a ve vzdálenosti dvou metrů od přímého osvětlení. Intenzita osvětlení na úrovni čtecího zařízení byla průměrně 270 luxů. Hodnoty osvětlení byly získány pomocí luxmetru integrovaného v multimetru. Hodnota osvětlení doporučená výrobcem je v rozsahu 0-800 luxů. Světlo, které dopadalo na obličej (odraz od stěny), mělo v průměru intenzitu 70 luxů.

Snímanými subjekty byli dobrovolní studenti a zaměstnanci Technické fakulty a fakulty agrobiologické. Od všech zúčastněných byl získán písemný souhlas týkající se použití jejich biometrických údajů v této dizertační práci a dalších vědeckých záměrech. Celkem se na měření podílelo 80 subjektů, z toho 16 žen a 64 mužů. Věkové rozmezí testovaných subjektů bylo 21 – 62 let.

Testování biometrických identifikačních systémů, které vyžadovalo velký počet subjektů, probíhalo po dobu dvou a půl let (3 zimní a 2 letní semestry). Na dalších testech, které pojednávaly zejména o sabotážních technikách, se pracovalo i mimo období semestrů.

Měření bylo rozděleno do tří částí. V první části se na jednotlivých čtečkách zjišťovaly hodnoty chybného odmítnutí uživatele za různých podmínek. Ovlivňujícími faktory byly vlhkost, zašpinění, podchlazení a přehřátí zkoumaných prvků. V další části byly testovány možnosti sabotáže, s čímž se také částečně pojí parametr chybného přijetí uživatele. V poslední části se pojednává o sestavení a vývoji nového biometrického systému, který

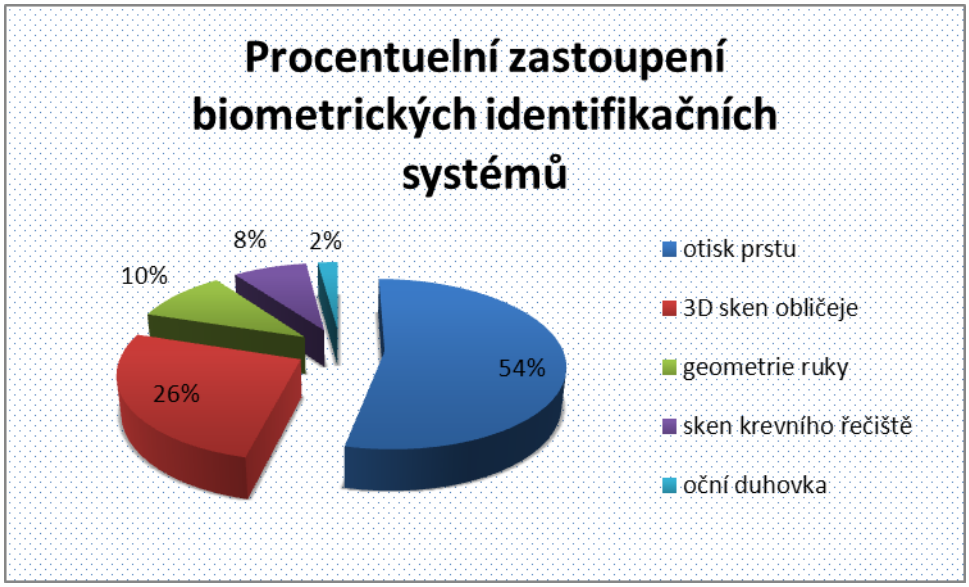
funguje na odlišném jedinečném rozpoznávacím segmentu. Dále jsou v této části řešeny inovace stávajících systémů.

Veškeré měření probíhalo na základě spolupráce s firmami Variant s.r.o., Eurosat cs a Alarm Absolon s.r.o., které dodaly biometrické systémy. Rozsáhlá spolupráce probíhala i s Ministerstvem vnitra, s vedoucím a jednotlivými členy pražské kriminální služby. Na základě této spolupráce bylo možné při zpracovávání této práce využít i jejich dosavadních poznatků, připomínek a materiálů k dané problematice.

5 Měření

Před výběrem biometrických identifikačních systémů byl proveden průzkum pomocí kterého bylo zjištěno procentuální zastoupení jednotlivých druhů biometrických identifikačních systémů, viz obr. 22. Bylo osloveno celkem 500 firem, společností a státních institucí, z toho 328 disponovalo biometrickým identifikačním zřízením. Mezi tyto subjekty patřily autoservisy, kulturní objekty, kancelářské prostory, exekutorské společnosti, letiště, policejní služebny, státní a vojenské instituce (kasárna, armádní cvičební prostory, školské prostory, ministerstva, Areál Pražského hradu, radnice aj.) a další.

Obr. 22 Grafické znázornění zastoupení biometrických identifikačních systémů



Z hlediska procentuálního zastoupení biometrických identifikačních systémů byla jako testovaná zařízení vybrána TAC-05 MFF, F7, Multibio700, IFace302. Poslední dvě z těchto jmenovaných zařízení mají zároveň i možnost identifikace na základě rysů tváře. Všechny tyto čtečky disponují optickým snímačem pro identifikaci prostřednictvím otisků prstů. Práce těchto senzorů je založena na technologii FTIR – Frustrrated Total Internal Reflection. Jedná se o laserový paprsek nebo hustý svazek optických vláken osvětlující zespodu povrch prstového lůžka, který je přiložen na průhlednou desku senzoru. Odražený světelný tok snímá CCD (Charge Couplet Device) prvek. Papilární linie a brázdy nám určují množství odraženého světla, kde papilární linie odrážejí více světla než brázdy. CCD prvek ovšem odraz světla od brázd nepoužívá jako vyhodnocovací prostředek.

Měření identifikace na základě otisků prstů se zaměřilo především na hodnoty chybného přijetí a chybného odmítnutí uživatele. Tyto dvě veličiny jsou velice důležité pro zjištění spolehlivosti čtecích zařízení. Při testování bylo třeba se zaměřit zejména na hodnotu

chybného přijetí, jelikož na rozdíl od chybného odmítnutí může chybné přijetí narušit bezpečnost hlídaného prostoru. Pokud dojde k situaci, že neoprávněná osoba bude vpuštěna do chráněného objektu, systém přestává být bezpečným.

Také byly otestovány možnosti sabotáží těchto zařízení. Testování probíhalo na čtečkách, které disponují optickým senzorem, jelikož tyto čtečky mají na českém i zahraničním trhu nejširší zastoupení.

Další měření hodnot chybného přijetí a odmítnutí probíhalo na čtečkách pro identifikaci na základě rysů obličeje. Zkoumala se také doba vytvoření předlohové šablony pro následnou identifikaci uživatele. Časové intervaly, ve kterých došlo k přijetí uživatele a také se testovala zaměnitelnost osob. V neposlední řadě byla věnována pozornost sabotážním technikám.

Pro měření byly použity různé druhy čteček, které jsou na trhu běžně dostupné, finančně a uživatelsky přijatelné a často používané. Tyto čtečky jsou:

- **TAC-05 MFF:** (viz obr. 23) je systém využívající čtyři možnosti, dle kterých dojde k identifikaci, a to jednoduchý kód, čipovou kartu, otisk prstu a otisk prstu v kombinaci s kódem. Modul pracuje na bázi docházkového systému (1:1) a také přístupového systému (1:N) vzhledem k velmi vysoké kapacitě záznamů (100000). Zařízení má dotykovou obrazovku a také Wifi připojení. [27]

Obr. 23 Čtečka TAC-05 MFF [27]

- **F7:** byla vybrána díky její kombinaci PIN (Personal Identification Number) kódu a snímači otisku prstů. Tato čtečka, viz obr. 24, by měla mít jednu z nejrychlejších odezev pod 1,5 sekundy. Zařízení se dá propojit s počítačovou jednotkou přes protokol TCP/IP nebo přes sériový port RS 232. Při propojení více čteček musí každá z nich mít svou vlastní ID. Kapacitu otisku prstů má pro 500 osob s celkovým počtem

záznamů 30 000. Slouží jako docházkový systém, kde se jeho prostřednictvím otevírají dveře. Také se vyskytuje jako terminál pro zapisování příchodů a odchodů k vyhodnocení docházky a dále jako povolení vstupu do hotelů, škol, výrobních závodů aj. Pracuje prostřednictvím jednoho z nejmodernějších algoritmů ZKF-VX10. [28]

Obr. 24 Čtečka F7 [28]

- **Multibio 700:** (viz obr. 25) verifikuje na základě otisků prstů, což je ve světě jedna z nejznámějších možností biometrické identifikace. Pro identifikaci využívá tvář a to její základní rysy (oči – vzdálenost mezi nimi, jejich velikost a umístění na obličeji, nos, ústa, lícní kosti, čelisti). Tyto rysy slouží k vytvoření předlohové šablony, díky které pak dochází k ověření či určení osoby. Také je zde možnost dle užití použít PIN či ID (Identification) kartu. To slouží pro porovnání 1:1, což znamená, že jsou uživatelovi ID karta či PIN načteny, a pak se porovnávají sejmuté biometrické údaje s předlohou uloženou na zálohovacích zařízeních. Toto zařízení využívá 3D technologie. Je možno nahrát až 400 tváří a 2000 otisků prstů. Nově použitý algoritmus VX7.0 je mnohem rychlejší (rychlost verifikace je < 2 sekundy) a má větší kapacitu. Čtečku lze použít i jako venkovní přístupový systém. Může na ni být připojeno zamykání, alarm, magnetický kontakt dveří, vstup/výstup, odchodové tlačítko, domovní zvonek. [29, 30]

Obr. 25 Čtečka Multibio 700 [29]

- **IFace 302:** (viz obr. 26) je díky jednotlivým komponentům určen do jakéhokoli prostředí (tmavé, světlé, zima, teplo, aj.). Do zařízení byl integrován vysokorychlostní procesor o velikosti 630MHz a infračervená kamera s velmi vysokým rozlišením. Stejně jako u minulého zařízení se i u tohoto může rozšiřovat o heslo. Tento systém obsahuje i funkci webserver, což je správa prostřednictvím internetového prohlížeče. Čtečku lze zapojit jako elektrický zámek, dveřní senzor, alarm, odchozí tlačítko i jako drátový dveřní zvonek. Zařízení je schopné pojmout 100000 záznamů, z toho 400 skenů obličeje a 5000 otisků prstů. Z tohoto vyplývá, že použití je především určeno pro způsob 1:N, kdy je do databáze nahráno mnoho uživatelů a identifikuje se dle nalezené shody. Algoritmus, který je zde použit, je 5.0 (starší verze než u čtečky Multibio 700). [29, 31]

Obr. 26 Čtečka IFace 302 [31]

5.1 Otisk prstů

Identifikace na základě otisku prstů je doposud nejrozšířenějším druhem identifikace osob. Je to z důvodů uživatelsky přijatelné ceny, širokého využití (docházkové systémy, zabezpečení vstupu do objektu, atd.) a uživatelsky přívětivého způsobu identifikace. Jelikož je otisk prstu jednou z nejstarších identifikačních metod, pojí se s ním i mnoho sabotážních technik. Díky tomu dochází k stálému zdokonalování těchto systémů. I z těchto důvodů byla na čtečkách provedena rozsáhlá měření, ze kterých následně byly vytvořeny závěry a doporučení.

Všechna zařízení snímají otisk prstu na základě optického senzoru. Čtečky s optickým senzorem byly vybrány z důvodů, že na českém i zahraničním trhu a také v praxi jsou nejvíce zastoupeny. Každé měření bylo složeno z dvaceti opakování. Měřeno vždy bylo 80 osob (16 žen a 64 mužů) s věkovým rozptylem 21 – 62 let.

5.1.1 Chybné odmítnutí uživatele

Tato situace znamená, že oprávněný uživatel není přes identifikační zařízení vpuštěn do objektu. Pokud k tomuto jevu dochází zřídka, uživatel zopakuje celý proces identifikace a následně je vpuštěn do objektu. Chybné odmítnutí osoby může mít mnoho příčin (nesprávně ložený prst na čtecí zařízení, vlhký prst, podchlazený prst, poraněný prst, zašpiněný prst apod.). Pravděpodobnost chybného odmítnutí uživatele lze dopočítat prostřednictvím vzorce:

$$FRR = \frac{NFR}{NEIA} . 100\ [\%] \tag{5.1}$$

FRR – chybné odmítnutí uživatele

NFR - počet chybných odmítnutí (Number of False Rejection),

NEIA - počet pokusů oprávněných osob o identifikaci (Number of Enrolle Identification Attemps) [32]

Měření bylo provedeno jak za standardních, tak i za ztížených podmínek a bylo zaměřeno na různé druhy testů, které mohou vzniknout za reálných podmínek. Testy byly rozděleny na:

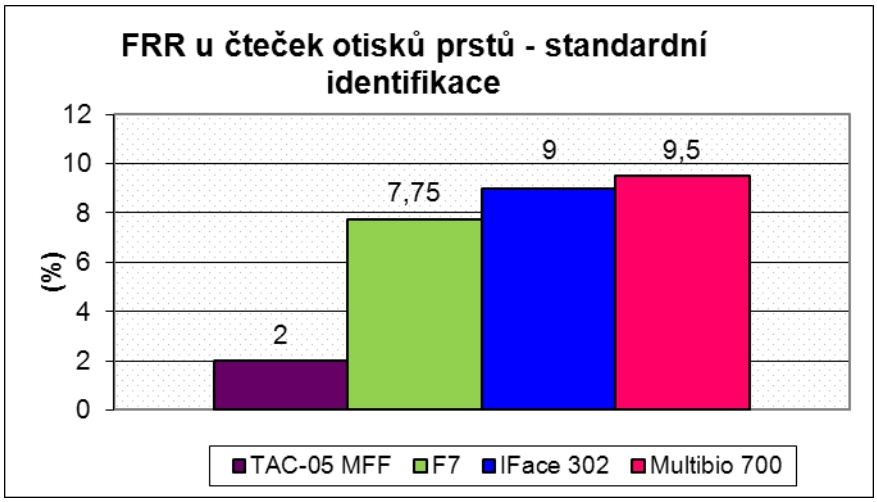
- **standardní identifikace,**
- **podchlazení prstu,**
- **podchlazení vlhkého prstu,**
- **přehřátí prstu,**
- **rozmáčení prstu,**
- **načernění prstu,**
- **prst s vrstvou lepidla Kores,**
- **prst s vrstvou vteřinového lepidla,**
- **poranění prstu,**
- **zašpinění prstu (hlína).**

5.1.1.1 Měření FRR u standardní identifikace

U tohoto měření byla provedena identifikace za klasických podmínek. To znamená, že bez jakéhokoliv zásahu byly plošky prstů postupně přikládány na snímače jednotlivých čteček. Čas, který identifikace trvala, se zanedbával, jelikož povětšinou byla tato hodnota řádově v sekundách (do 1,5s). Sledovalo se, zda byl uživatel přijat či nikoli. Z obrázku 27 je

patrné, že identifikace není stoprocentní a v závislosti na těchto výsledcích bylo měření rozšířeno o testování za ztížených podmínek.

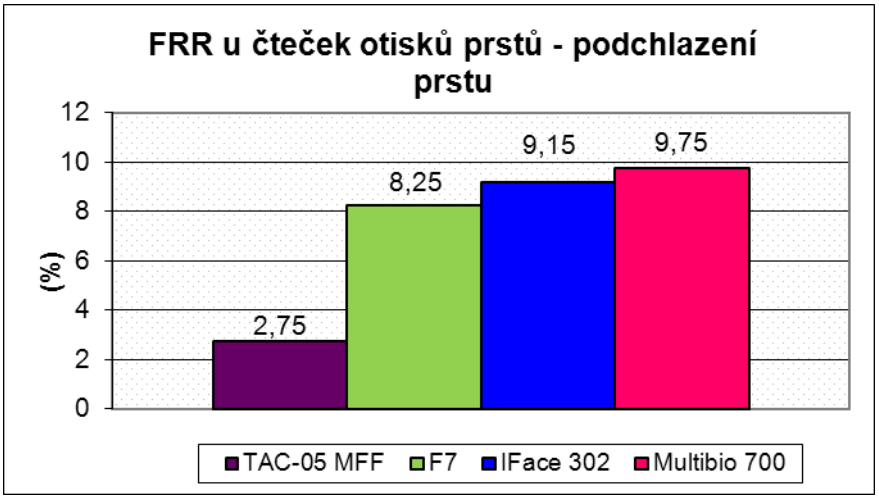
Obr. 27 Identifikace za standardních podmínek



5.1.1.2 FRR u podchlazeného suchého a vlhkého prstu

Nejprve bylo nutné podchladit prsty subjektů na stejné rozmezí teplot, které bylo 20 – 25°C. Toho se dosáhlo ledem připraveným do forem. Každá forma byla opatřena vodě nepropustnou folií, aby nedošlo k navlhnutí měřeného prstu. Tímto bylo simulováno mrazivé venkovní prostředí. Každému měření předcházelo patnáctiminutové chlazení prstu a poté byl prst přiložen na plochu senzoru. Na obrázku 28 je zobrazena spolehlivost čteček za velmi nízkých venkovních teplot, či za jiných okolností, při kterých má prst teplotu v testovaných teplotních rozmezích.

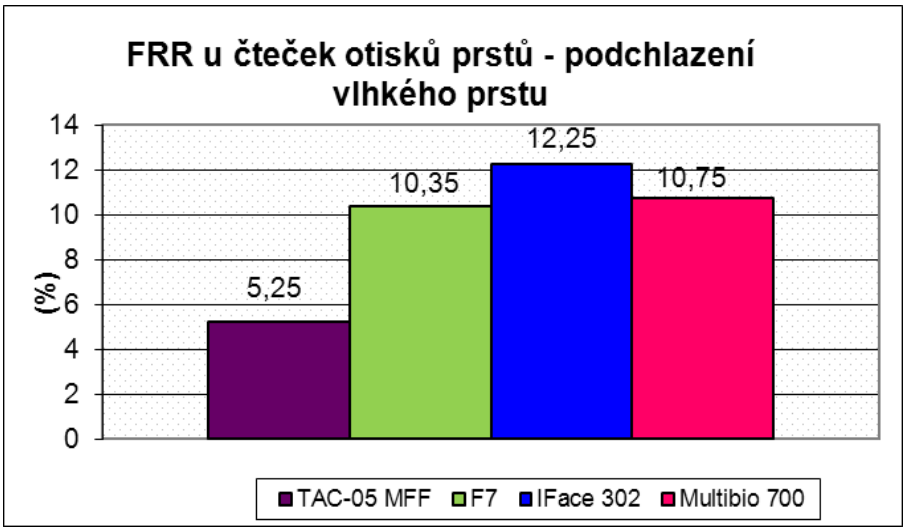
Obr. 28 Identifikace podchlazeného prstu



U podchlazení vlhkého prstu probíhalo měření stejným způsobem jako u měření při podchlazení suchého prstu, až na část s vodou nepropustnou folií. Při tomto měření se chladil

prst přímo o led. Tím, jak se led rozpouštěl, došlo k lehkému rozmočení pokožky prstu. Zároveň nedošlo k osušení prstu, což způsobilo požadovaný mokrý povrch. Na obrázku 29 je patrné, že vlhkost prstu současně s podchlazením má vyšší hodnotu FRR než pouze podchlazený prst.

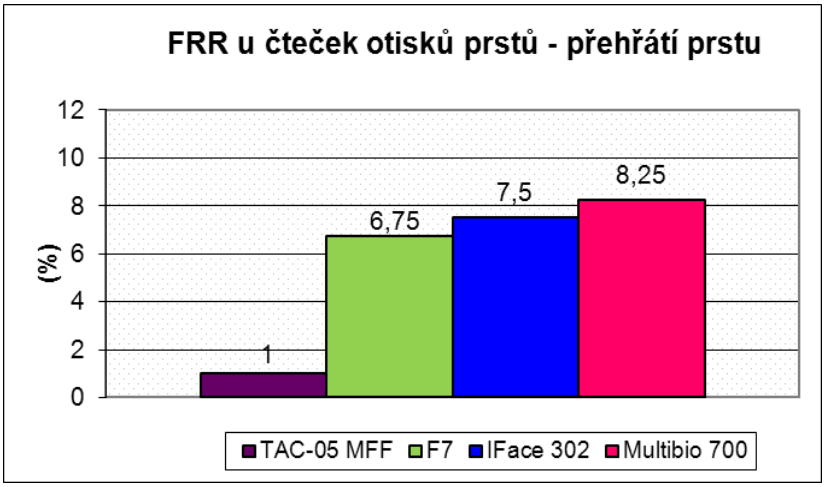
Obr. 29 Identifikace podchlazeného vlhkého prstu



5.1.1.3 FRR u přehřátého prstu

Při tomto měření se na začátku musela stanovit metoda zahřátí prstu na teplotní rozmezí, které bylo 50 – 55°C. Nejprve se zkoušel nahřát prst prostřednictvím horké vody v nádobě, toto řešení bylo zamítnuto z důvodu chladnutí vody. Aby byly zajištěny stejné podmínky pro všechny subjekty a aby byla měření relevantní, byl pro ohřev prstu zvolen USB (Universal Serial Bus) ohřívač, na který byl přidělán digitální snímač teploty. Teplota nahřívání byla konstantně 55°C, ovšem je nutné počítat s teplotními ztrátami při krátkém přesunu prstu z ohřívače na senzor čtečky. Proto je uvedeno teplotní rozmezí 50 – 55°C. Z obrázku 30 je vidět, že přehřátí prstu zvyšuje pravděpodobnost chybného odmítnutí oprávněné osoby.

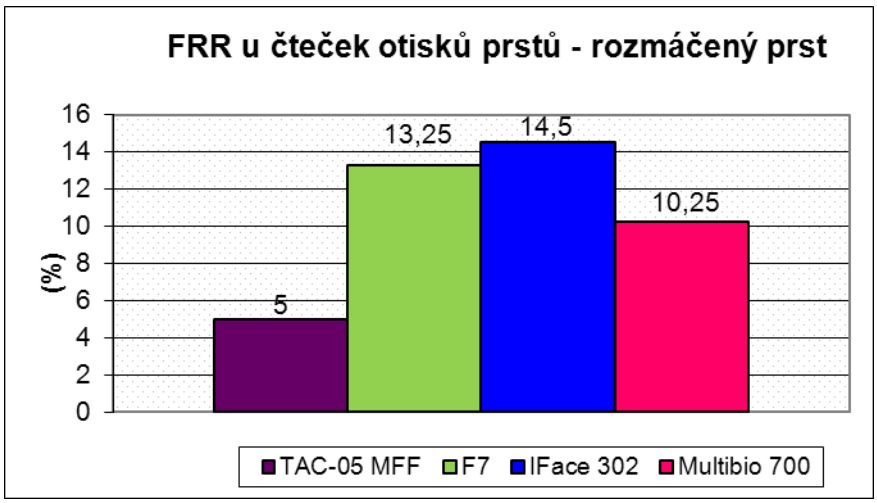
Obr. 30 Identifikace přehřátého prstu



5.1.1.4 FRR rozmáčeného prstu

Rozmáčení prstu bylo pro testování velice důležité. Takovýto případ může nastat v běžných pracovních i domácích situacích. K rozmáčení prstového lůžka došlo prostřednictvím vody v nádobě. Kapalina byla zahřívána na 40°C USB ohřívačem. Máčení prstu trvalo u každého subjektu 20 minut. Po vyjmutí prstu z vodní lázně byl prst osušen buničinou a otestován na měřícím panelu. Rozmáčení prstu má špatný vliv na spolehlivé fungování čtecích zařízení, jelikož dojde k částečnému znehodnocení viditelnosti papilárních linií – viz obr. 31.

Obr. 31 Identifikace rozmáčeného prstu

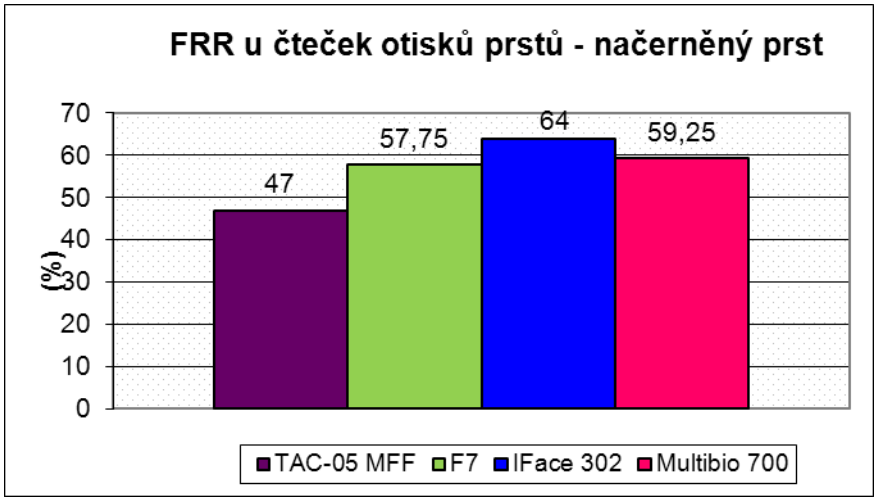


5.1.1.5 FRR u začerněného prstu

Testování začerněného prstu bylo zvoleno na základě praktických zkušeností. Před načtením do systému nebývá pravidlem umýt si ruce. Jak v zaměstnání tak i v soukromí je dosti častý případ zamazání rukou. K načernění a simulaci zamazaných rukou byl použit

černý smývatelný fix s neúplným krytím. Toto testování se zaměřilo pouze na barevný odstín, nikoli na mikročástice nečistot, jako je například hlína, prach aj. Výsledky měření viz obr. 32. Z hodnot v grafu je patrné, že biometrické systémy si s takovýmto znečištěním neumí poradit.

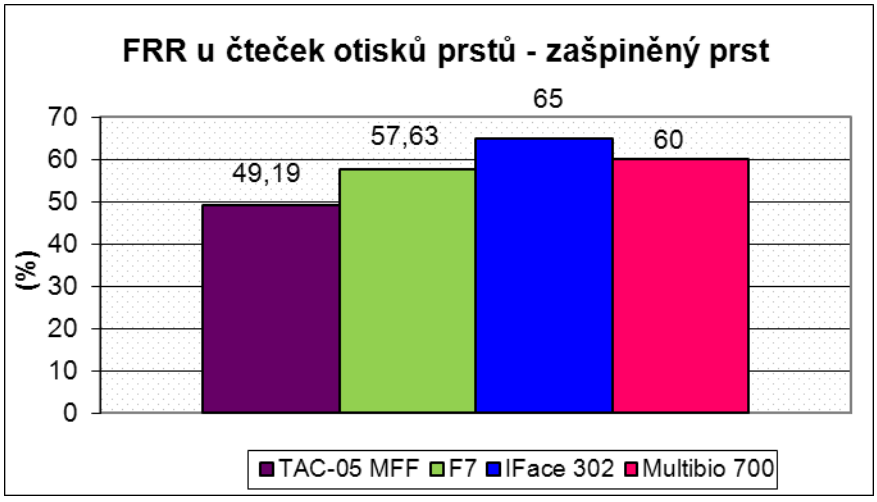
Obr. 32 Identifikace načerněného prstu



5.1.1.6 FRR zašpiněných rukou

Pro toto měření bylo využito prachu, který byl získaný ze sáčku vysavače. Prach se smíchal s rašelinou a vznikla potřebná směs. Každý testovací subjekt si tuto směs před měřením promnul mezi dlaněmi. Tento způsob se od předchozího měření začerněného prstu lišil v tom, že u tohoto znečištění byly přítomny mikročástice a prachové částečky. Tyto částečky znehodnocovaly identifikaci, viz obr. 33, jelikož se usazovaly především v prostorách mezi jednotlivými papilárními liniemi.

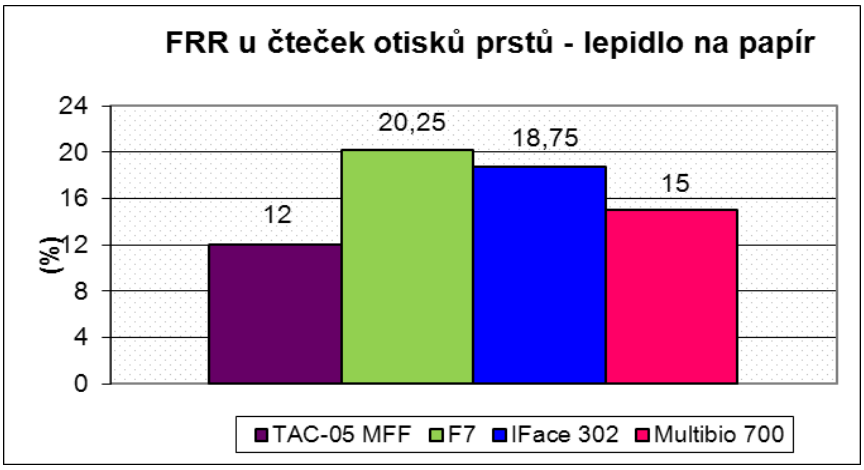
Obr. 33 Identifikace zašpiněného prstu



5.1.1.7 FRR u prstu s vrstvou lepidla Kores

Testování s vrstvou lepidla Kores bylo zvoleno, jakožto náhrada pro obdobné materiály jako je silikon, lepidla a jiná maziva, s kterými se v praktickém životě běžně setkáváme. Na prst byla nanesena tenká vrstva lepidla a po pěti minutách, ve kterých lepidlo pouze částečně ztuhlo, bylo provedeno snímání. Po každém snímání byl povrch čtecího senzoru očištěn. Výsledky měření viz obr. 34, ze kterých vyplývá, že opět došlo k částečnému zakrytí papilárních linií, a proto bylo méně osob verifikováno.

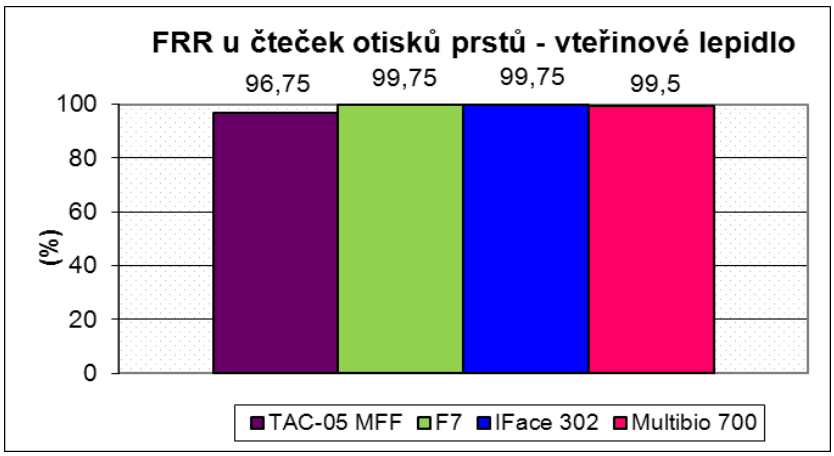
Obr. 34 Identifikace prstu s vrstvou lepidla



5.1.1.8 FRR prstu s vrstvou vteřinového lepidla

Vteřinové lepidlo bylo vybráno, protože vytváří celistvý pevný povlak. Tento povlak je transparentní a zároveň velmi tenký. Při nanesení a zaschnutí lepidla dojde k znehodnocení papilárních linií, na jejichž základě jednotlivé čtečky verifikují. Z obrázku 35 je jasné, že do mezer mezi papilárními liniemi vniklo vteřinové lepidlo a znemožnilo tím identifikaci. Vteřinové lepidlo se projevilo i jako vhodný produkt pro sabotážní techniky.

Obr. 35 Identifikace prstu s vrstvou vteřinového lepidla



5.1.1.9 FRR u poraněného prstu

K poranění prstu dochází každodenně a proto bylo nutné zajistit testování i takovýchto případů. Při sezení všech 80 subjektů se zhodnotily nejčastější možnosti poranění. Mezi tato poranění patřily řezné ranky, popálená lůžka prstu, znehodnocení pokožky obroušením a otlačení. Tyto čtyři způsoby poranění byly rozděleny mezi testované subjekty. Měření proběhlo v deseti cyklech. Dobrovolně došlo k daným poraněním. Řezné ranky byly provedeny sterilizovaným skalpelem, pro otlačení byla použita hrana pravítka. Pro obroušení byl použit smirkový papír. Popálení bylo způsobeno vyndáváním keramických výrobků z pece, nejednalo se o klasické popáleniny, nýbrž došlo vysokou teplotou k minimalizaci papilárních linií a pokožka byla bez těchto znaků potřebných k identifikaci. Proto se také toto měření viz tab. 1 dělalo jako poslední.

Tab. 1 Hodnoty FRR ovlivněné poraněním prstu

	TAC-05 MFF [%]	F7 [%]	IFace 302 [%]	Multibio 700 [%]
standardní měření	1,75	8,0	8,5	9,25
řezné ranky	2,75	8,5	10	10,5
popálená lůžka prstu	6,25	13	15,25	14,75
obroušení	26,75	24,75	38,25	41,5
otlačení	2,75	8	10	10,25

5.1.2 Chybné přijetí uživatele

Chybným přijetím uživatele se rozumí, že je do objektu vpuštěna osoba, která pro to není oprávněná. K vpuštění neoprávněné osoby může dojít dvojím způsobem a to chybou čtecího zařízení, kdy osoba nemá v úmyslu konat trestí činnost. Druhý způsob je, že otevření dveří je vyvoláno úmyslně za určitými záměry (nezákonné vniknutí, krádež aj. zločiny). Pachatel má více možností, jak obelstít biometrický identifikační systém. Jedním ze způsobů je vyvolání zkratu čtecího zařízení bez následného vyvolání poplachu (většina identifikačních systémů je napojena na ústřednu poplachových zabezpečovacích a tísňových systémů (PZTS). Dalším způsobem je zfalšování posledního přijatého otisku prstu, který je zanechán uživatelem na povrchu čtecího zařízení, v neposlední řadě může jít také o sabotáž vytvořením falešného otisku prstu. Procento chybného přijetí biometrických identifikačních systémů je dáno vztahem:

$$FAR = \frac{NFA}{NIIA}.100\ [\%] \tag{5.2}$$

FAR - chybné přijetí uživatele

NFA - počet chybných přijetí (Number of False Rejection),

NIIA - počet pokusů neoprávněných osob o identifikaci (Number of Enrolle Identification Attemps) [32]

Měření chybného přijetí uživatele otisku prstu probíhalo vždy na pěti uživatelích s padesáti opakováními.

5.1.3 Oklamání čtecího zařízení vytvořením falešného otisku prstu

Každý uživatel, který se identifikuje a je vpuštěn do objektu, zanechá na sklíčku biometrického identifikačního systému otisk svého prstu. Pro oklamání čtecího zařízení byla nanesena na sklíčko čtecího zařízení tenká vrstva tekutiny olejové konzistence. Následovalo sejmutí otisku prstu oprávněné osoby. Poté na otisk prstu, který v oleji vznikl, byla nanesena tenká vrstva pudru. Tento pudr se nanesl sfouknutím ze štětce. Teplota lidského dechu simulovala lidské teplo, které je při identifikaci potřebné, jelikož všechny použité čtečky mají funkci ověření živosti identifikovaného subjektu. Celý tento proces byl ukončen identifikací a následným vpuštěním do objektu.

Dalším způsobem, jak proniknout do objektu, je vytvoření falešného otisku prstu. Při testování byla použita modelovací hmota. Do modelovací hmoty byl vytvořen otisk prstu oprávněného subjektu. Došlo k vzniku formy, do které byla nanesena tenká vrstva vteřinového lepidla. Po uplynutí 24 hodin (úplném zatuhnutí lepidla) byl z formy vyjmut falzifikát otisku prstu, s kterým bylo prováděno následné testování.

Pro vytvoření falešného otisku prstu není vždy potřeba modelovací hmoty. Jednou z možností je získání otisku prstu oprávněné osoby. Měření započalo sejmutím otisku prstu ze sklenice. Poté byl otisk na sklenici poprášen daktyloskopickým práškem a sejmut speciální fólií pro to určenou. Otisk z fólie byl vystřihnut a velice opatrně nalepen na chirurgické rukavice. Při pokusu o přijetí čtečkou byl zaznamenán částečný úspěch, viz tab. 2. Velmi důležité u tohoto měření byla kontrastní barevnost. Daktyloskopický prášek má metalickou barvu a fólie je transparentní (popřípadě lze vytvořit i bílý podklad). Prášek zvýraznil papilární linie a tím bylo způsobeno přijetí neoprávněné osoby.

Tab. 2 Úspěšnost sabotážních technik otisku prstu

	TAC-05 MFF [%]	F7 [%]	IFace 302 [%]	Multibio 700 [%]
olejovitý otisk	21	16	74	77
syntetický otisk	0	0	0,15	0,15
daktyloskopický prášek	5,75	4,75	15,85	23

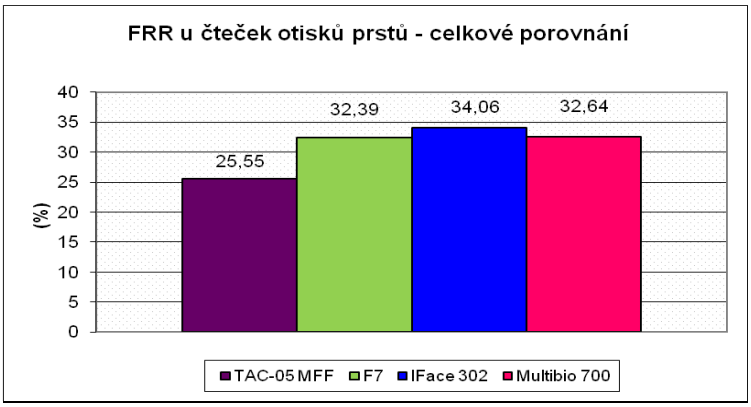
5.1.4 Duplicita otisku prstu

Při zadávání otisků prstů (vytváření předlohové šablony pro identifikaci) bylo potřeba, aby každému testovanému subjektu byly odebrány tři otisky za sebou (jednoho prstu – při měření tímto prstem byl ukazováček pravé ruky). Vždy došlo k přiložení prstu na sklíčko čtečky, následovalo oddálení ukazováčku a opětovné přiložení. Ovšem v 56 případech z 80 došlo při oddálení prstu k samovolnému načtení prstu. Vznikly tak dva naprosto totožné snímky, což není dobré pro budoucí identifikaci, jelikož verifikovaný subjekt je porovnávaný se všemi třemi předlohami (právě kvůli jedinečnosti jednotlivých předloh, která je způsobena sklonem přiloženého prstu). Tato duplicita se vyskytovala i při následně probíhajících měřeních.

5.1.5 Shrnutí, dílčí závěry a doporučení

Každý výrobce udává u biometrických identifikačních zařízení hodnoty spolehlivosti, které jsou vyjádřeny veličinami FFR a FAR. U všech testovaných čteček výrobcem udávaná hodnota FAR je ≤ 0,0001% a hodnota FRR je ≤ 1%. Při těchto testech se na čtečkách měřily hodnoty pro získání velikosti veličin chybovosti. Z grafu, který se nachází na obrázku 36, je patrné, že skutečnost se od hodnot, které udávají výrobci, značně liší. U všech čteček dosahují hodnoty FAR více než 0,0001%, pohybují se v rozmezí od 25% až po 34%, což je uživatelsky nevyhovující stav.

Obr. 36 Průměrná chybovost biometrických systémů



Hodnoty FAR, které vyjadřují procentuální počet chybně přijatých uživatelů, jinými slovy počet úmyslných vniknutí (sabotáže čtecích zařízení), či v menší míře neúmyslných vniknutí do objektu, jsou uvedeny výrobcem jako $\leq 0{,}0001\%$, ovšem i v tomto případě je skutečnost jiná. Z grafu na obrázku 36 vyplývá, že spolehlivost čteček je velmi nízká. Proto jsou biometrické identifikační systémy často používány spíše jako docházkové systémy. Ovšem firmy používající tyto systémy jako přístupové by měly vzít na vědomí, že to, co jimi chtějí chránit, není v plném bezpečí. U biometrických systémů používaných pro ochranu vstupu by se mělo využít jejich alternativních možností vstupu a to například identifikace na základě biometrického údaje v kombinaci s heslem, přístupovou kartou, popřípadě čipem, kdy pro vstup by bylo podmínkou zadání obou údajů.

5.2 Identifikace na základě obličeje

Jednou z dalších hojně využívaných metod biometrické identifikace je rozpoznání založené na rysech obličeje (3D sken obličeje). Systémy fungující na tomto principu jsou v dnešní době pro širokou veřejnost cenově přijatelné a jejich zastoupení v komerčních i státních institucích dle průzkumu je na druhém místě hned po identifikaci na základě otisku prstu. Z těchto důvodů byl tento způsob verifikace zařazen do měření.

Každé měření bylo složeno z dvaceti opakování. Měřeno bylo vždy 80 osob (16 žen a 64 mužů) s věkovým rozptylem 21 – 62 let. U 3D skenu obličeje bylo nutno dodržovat laboratorní podmínky a to zejména osvětlení (osvětlení požadované výrobcem je 0 – 800 luxů). Měření probíhalo na čtečkách MultiBio 700 a iFace 302. Obě zařízení jsou kombinací identifikace pomocí kódu, otisku prstu a snímání rysů tváře.

Byl měřen čas snímání předlohové šablony k následné identifikaci osob, zároveň počet chybných přijetí či nenačtení uživatele. Dále se zkoumala zaměnitelnost osob, což z velké míry vyjadřují hodnoty FAR.

5.2.1 Zadávání předlohové šablony

Do každého biometrického systému bylo nejprve potřeba nahrát jednotlivé uživatele. Obě testované čtečky mají shodný software a nahrání probíhalo stejným způsobem. Nejprve se každému uživateli přidělilo jeho ID číslo (identifikační číslo), poté se načetl otisk prstu (3 krát přiložení stejného prstu) a poté následovalo nahrání předlohové šablony pro 3D sken obličeje. Hlasová aplikace čteček dávala uživatelům pokyny, jak mají natáčet hlavu.

Čtečky jsou vybaveny dvěma kamerami snímajícími pod určitým úhlem tvář uživatele. Pokud kamery získají požadované hodnoty, vytvoří snímek, který následně uloží. Už při

snímání šablony je nutno, aby se snímky v minimálně 95% shodovaly s prvním snímkem. Jedná se o shodu v bodech, které vývojáři určili jako záchytné (špička nosu, šířka nosu, vzdálenost očí, lícní kosti, tvar úst, brada, aj.). Právě shoda jednotlivých snímků, které byly snímány postupně, zapříčinila časovou náročnost tvoření předlohových šablon, viz tab. 3. V tabulce jsou zadány počty osob, u kterých délka vytváření předlohových šablon byla v daných časových intervalech.

Tab. 3 Délka zadávání předlohových šablon

Délka zadávání šablony [min]	do 5 min	do 10min	do 20min
IFace302	48	28	4
Multibio700	52	16	12

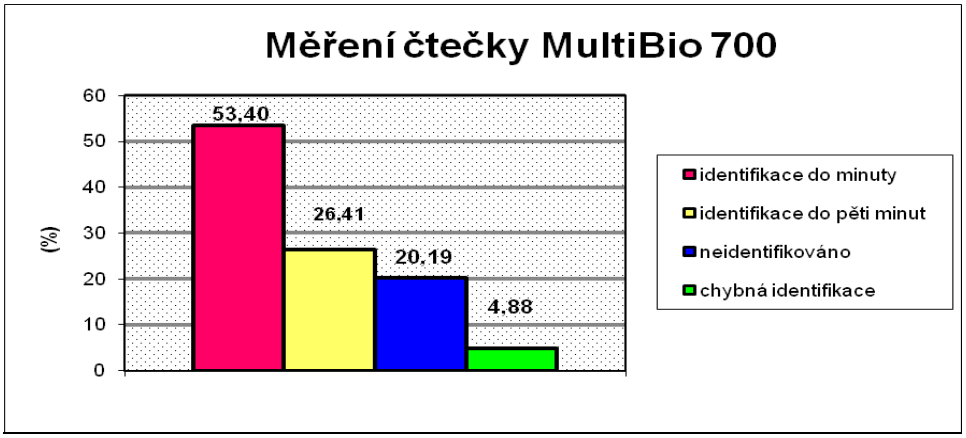
5.2.2 Chybovost 3D čteček obličeje

U biometrických identifikačních systémů pracujících s 3D skenem obličeje se také měřila chybovost, ovšem se zaměřením na konkrétní situace. Chybovost v podobě chybného odmítnutí uživatele se u těchto čteček nevyskytuje, pouze je možnost, že uživatel nebude identifikován. Pro identifikaci byla stanovena mezní časová hranice 5 minut. Pokud se nepodařilo v tomto časovém intervalu uživatele identifikovat, považovala se tato situace za chybné odmítnutí uživatele.

5.2.2.1 Standardní identifikace

Pojem standardní identifikace znamená identifikace za laboratorních podmínek. V průběhu 27 měsíců byly získávány hodnoty pro určení funkčnosti a spolehlivosti biometrických identifikačních systémů, které pracují na základě 3D skenu obličeje. Dvěma nejdůležitějšími hodnotami se stalo časové rozmezí, během kterého byli uživatelé vpuštěni do objektu a s tím související stav přijat/nepřijat (identifikován, neidentifikován). Na obrázcích 37 a 38 je znázorněno procentuální zastoupení identifikací v jednotlivých časových intervalech. Předposlední sloupec v grafu vyjadřuje chybné odmítnutí uživatele – FRR, u kterého bylo stanoveno, že k němu dochází v případě přesáhnutí 5 minut při pokusu o identifikaci. Poslední uvedená hodnota v grafech znázorňuje chybnou identifikaci uživatele (chybné přijetí uživatele – FAR). Tato hodnota je uvedena v grafu kvůli přehlednosti výsledků a je brána z celkového počtu pokusů o identifikaci.

Obr. 37 Schopnost identifikace biometrického zařízení MultiBio 700



Pravděpodobnost chybného odmítnutí u MultiBio700:

$$FRR = \frac{NFR}{NEIA}.100\ [\%]$$

$$FRR = \frac{323}{1600}.100\ [\%]$$

$$FRR = 20{,}19\ [\%]$$

Pravděpodobnost chybného přijetí FAR u MultiBio700 je dána vztahem:

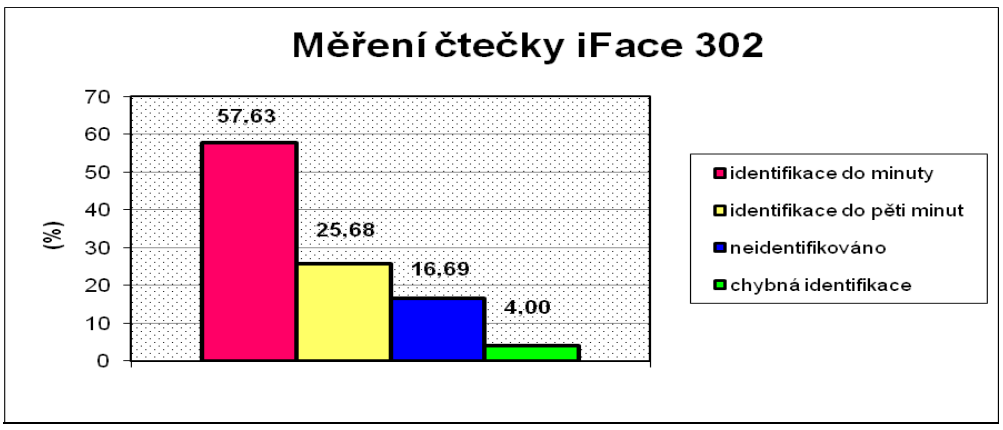
$$FAR = \frac{NFA}{NIIA}.100\ [\%]$$

$$FAR = \frac{78}{1600}.100\ [\%]$$

$$FAR = 4{,}88[\%]$$

Na obrázku 38 je zobrazeno měření na čtečce IFace302, oproti předchozí čtečce jsou výsledné hodnoty ještě nepřijatelnější. Pouhých 57,63 % uživatelů se úspěšně načetlo do systému a bylo vpuštěno do objektu. Také hodnota přes 25 % u obou čteček znamenající úspěšnou identifikaci do 5 minut je uživatelsky velice nekomfortní.

Obr. 38 Schopnost identifikace biometrického zařízení IFace 302



Pravděpodobnost chybného odmítnutí u IFace302:

$$FRR = \frac{NFR}{NEIA}.100\ [\%]$$

$$FAR = \frac{267}{1600}.100\ [\%]$$

$$FAR = 16{,}69\ [\%]$$

Pravděpodobnost chybného přijetí FAR u IFace 302 je dána vztahem:

$$FAR = \frac{NFA}{NIIA}.100\ [\%]$$

$$FAR = \frac{64}{1600}.100\ [\%]$$

$$FAR = 4{,}00\ [\%]$$

Z výpočtů a jejich grafického vyjádření vidíme, že procento chybného odmítnutí uživatele o zhruba 10 % převyšuje procento chybného přijetí. Ovšem obě tyto hodnoty jsou velice znepokojivé a je nutné se zamyslet, jestli je vhodné takovéto systémy využívat k hlídání vstupu do důležitých objektů. Z naměřených výsledků je zřejmé, že systémy pro identifikaci na základě rysů tváře je nutné stále zdokonalovat.

5.2.2.2 Identifikace v případě znečištěného obličeje

V provozech, kde bývá prašné prostředí, dochází k zamazání obličeje, také práce s mazivy a dalšími látkami může způsobit ušpinění tváře. I ve všedním životě lze nalézt situace, kdy dojde k umazání obličeje, například rozmazaný make-up po dešti.

Měření probíhalo na vybrané skupině 20 subjektů a s pěti opakováními. Na zašpinění bylo použito černé uhlí, zemina, mour, make-up, malířská barva, tmavé oleje. U subjektů s výraznými obličejovými rysy došlo k bezproblémové identifikaci. Ovšem u ostatních subjektů se na rozdíl od standardní identifikace zvýšila hodnota chybného odmítnutí uživatele, viz tab. 4.

Tab. 4 Procentuální přijetí uživatelů u 3D čteček obličeje při znečištění tváře

	IFace 302 - testování [%]	Multibio 700 - testování [%]
Standardní identifikace	84	79
Znečištění tmavým olejem	81	76
Znečištění zeminou	79	75
Znečištění make up	78	76
Znečištění mourem	54	47
Znečištění černým uhlím	48	52
Znečištění malířskou barvou	38	46

5.2.3 Zaměnitelnost uživatelů

Při měření došlo k výskytu zaměnitelnosti uživatelů. Tato situace nastala u 13 testovaných subjektů. Tito subjekty se zaměňovali mezi sebou. Nečastější záměna byla u těchto 4 mužů, kteří jsou na obrázku 39. Z jednotlivých snímků je možné si povšimnout společných rysů jednotlivých mužů. Mužům na obrázku byla přidělena čísla od jedné do čtyř a to – zleva doprava.

Obr. 39 Nejčastěji se zaměňující uživatelé

1 2 3 4

Muži 1, 2 a 3 mají velice podobný tvar očí, jednička, trojka a čtyřka se podobají tvarem obličeje. První a třetí subjekt má stejný tvar bradové části obličeje. Muži na třetím a čtvrtém snímku mají obdobný tvar obočí.

Po zjištění, že lze proniknout do objektu prostřednictvím podobnosti, bylo testování zaměřeno na úmyslné vniknutí, čili testování podobnostních znaků, do čteček neregistrovaných osob.

Prvním způsobem úmyslného vniknutí do systému bylo napodobit pomocí maskérských rekvizit tvář uživatele, kterému je přístup povolen. Nejprve se pomocí líčidel

upravil tvar obličeje (pomocí stínování), dále také tvar očí a úst a v poslední řadě se u mužů dodělaly vousy, či knírky. Po celém tomto procesu se namaskovaný uživatel pokusil překonat biometrický systém. Celkem bylo provedeno 5 pokusů po 15 opakováních. Pět různých lidí, žen i mužů (nezaregistrované do systémů) bylo tímto způsobem nalíčeno a upraveno. U biometrické čtečky IFace302 v 51 pokusech byla identifikace úspěšná (viz příloha 5) a osoba byla vpuštěna do systému. Zbylých 24 pokusů skončilo neúspěšnou identifikací. U čtečky Multibio700 byly výsledky obdobné a to 48 úspěšných pokusů o identifikaci a 27 neúspěšných pokusů. Po tak vysokém množství nedokončených identifikacích jak z úmyslné sabotáže, tak při standardním měření, se bylo nutné zamyslet, co by mohlo být příčinou.

Došlo se k závěrům, že stejného výsledku jako u stínování obličeje se dosáhne i správným nasvícením tváře. Při různých úhlech nasvícení je vržen do určitých míst tváře stín a dochází ke zkreslení tvaru obličeje a jeho jednotlivých částí. Opět jako u předchozí metody bylo provedeno měření na pěti subjektech po 15 cyklech. Z celkového počtu 75 měření bylo u systému IFace302 s úspěšnou identifikací dokončeno 26 pokusů a u zbylých 49 pokusů byla identifikace nedokončena a uživatelé nebyli systémem přijati. Biometrický systém Multibio700 byl úspěšně překonán v 18 pokusech ze 75 pokusů.

Už z hodnot, viz tab. 5, je patrné, že sabotáž prostřednictvím nasvícení obličeje je složitější než maskérské líčení, a z tohoto důvodu bylo s úspěšnou identifikací dokončeno pouze malé množství pokusů. Ovšem 44 úspěšných pokusů ze 150 svědčí o tom, že tyto čtečky lze zmást a tím tedy překonat jejich bezpečnost.

Tab. 5 Sabotáž 3D čteček obličeje

	Maskérské líčení		Nasvícení tváře	
Stav	Přijato	Nepřijato	Přijato	Nepřijato
IFace302	51	24	26	49
Multibio700	48	27	18	57

5.2.4 Dílčí závěr

Hodnoty osvětlení, které předkládá výrobce, jsou pro plnou funkčnost zařízení nevyhovující. Do uvedeného rozsahu hodnot osvětlení patří umělé osvětlení, např. 100W žárovka ve vzdálenosti 2 m má intenzitu osvětlení jen 35 luxů. V parametrech těchto čteček je uvedeno, že je lze užít i jako venkovní zařízení. Tato skutečnost je ovšem mylná, jelikož podmínky venkovního prostředí jsou nevyhovující pro jejich správné fungování. Je to z toho důvodu, že zatažená zimní obloha dává osvětlení 3000 luxů a za slunečného letního dne je osvětlení až 100 000 luxů. Z těchto hodnot je patrné, že použití čteček jako venkovních

zařízeních je nevhodné. Už jen identifikace v laboratorních podmínkách byla ne vždy úspěšná.

Časy tvorby předlohových šablon, viz tab. 3, jsou z uživatelského hlediska nepřijatelné. Většinou si tyto systémy, dle uvedeného průzkumu, nechávají instalovat větší firmy (50 – 150 zaměstnanců). Časová náročnost takového způsobu zadávání do systému není myslitelná a pro společnost je vysoce ztrátová.

Také shodné znaky v obličeji velice ovlivnily identifikaci. K překonání čtecího systému postačily divadelní rekvizity. Pouhé znázornění vousů, správný tvar očí a daný subjekt byl vpuštěn do chráněného objektu. I sabotáž v podobě nasvícení tváře byla úspěšná.

Získané hodnoty chybovostí poukazují společně s ostatními výsledky dalších testů na to, že čtečky, které identifikují uživatele na základě 3D skenu obličeje, jsou poměrně dost nespolehlivé a je nutné je stále vyvíjet a zdokonalovat. Před jejich instalací je nutno si rozmyslet, zda takováto ochrana vstupu opravdu postačí.

5.3 Elektronická sabotáž čtecích zařízení

Při instalaci čtecích zařízení může vzniknout mnoho bezpečnostních rizik, které oslabují zabezpečení celého objektu. Rizika, která vznikají z důvodů špatné instalace nebo různých sabotážních technik, jsou vždy závažným nebezpečím pro hlídané prostory. Mohou ohrozit hlídaný majetek.

Aby se předešlo nesprávnému nastavení celého systému, je důležité dbát na to, aby byla čtecí zařízení nastavována a instalována dle doporučení výrobce. Tato doporučení však nejsou dokonalým popisem, jak systém instalovat, ale jen nezbytností pro základní nastavení systému. Během instalace často dochází k chybám, které vznikají z nevědomosti, jak systém funguje a kde se nachází jeho slabiny. Ve chvíli, kdy jsou známy slabiny systémů, které se používají, lze proti nim vytvořit protiopatření.

Při pokládání kabelových rozvodů přístupových systémů je třeba dbát, aby nebyla kabeláž běžně dostupná a viditelně instalovaná. Pokud se kabelové rozvody instalují tak, že je k nim možný přístup, lze je sabotovat a tím napadnout celou instalaci přístupových systémů.

Rozvody se u čtecích zařízení dají rozdělit podle typu logiky zapojení jednotlivých čtecích zařízení do celkového systému. Jsou to:

- **systémy s centrální logikou,**
- **systémy s přímým ovládáním,**
- **systémy využívající PZTS.**

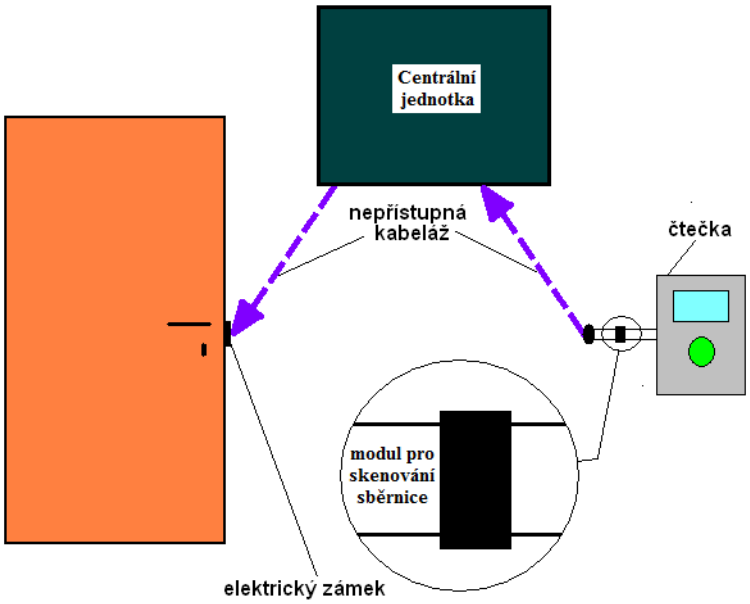
5.3.1 Systémy s centrální logikou

Systémy s centrální logikou využívají centrální jednotku, která má v sobě databázi uživatelů. Aby mohlo čtecí zařízení provést úspěšně autentizaci uživatele, nejprve přes protokol Wiegand vyšle (šifrovaně) vstupní údaje uživatele centrální jednotce. Ta vyhodnotí tyto údaje a porovná je se svojí databází. Pokud údaje odpovídají uživateli, který je v databázi a má patřičná oprávnění, tak zareaguje dle nastavení (otevře dveře, umožní přístup apod.) a zároveň kontaktuje dané čtecí zařízení a zašle mu o tom informaci (šifrovanou). Čtecí zařízení poté informuje, že uživatel byl přijatý. Pokud není uživatel autentizován, je postup obdobný jako u autentizovaného uživatele. Rozdíl je v tom, že mu je přístup zamítnut a čtecí zařízení informuje, že uživatel nebyl přijat.

Principiálně je sabotáž protokolu Wiegand možná, i když je relativně náročná. Protokol Wiegand využívá ke komunikaci dvou datových vodičů a GND (GrouND). Komunikace pomocí tohoto protokolu je řešena sekvenčně a bity se přenášejí postupně. Tato komunikace je synchronizovaná. Komunikace probíhá pomocí krátkých impulzů přivedených na jednotlivé datové vodiče.

Klasické čtečky využívají 26 bitový protokol (Wiegand 26). Ten se skládá z 8 bitů tzv. Facility code (kód zařízení), 16 bitů dat ze čtečky a dvou bitů paritních. Díky tomu je jejich elektronické napadení složitější, než u ostatních typů logiky zapojení. Na sběrnici je třeba umístit modul, který dokáže přečíst a zaznamenat (posléze i vysílat) data, která vysílá čtecí zařízení do centrální jednotky – viz obr. 40. Po přečtení zakódovaných dat je potřeba data dešifrovat (tzn. objevit správný dešifrovací algoritmus). Ve chvíli, kdy se povede dešifrovat tuto komunikaci, stačí vytvořit signál a vložit ho prostřednictvím modulu na sběrnici. Tato metoda je tak náročná, že je potřeba, aby měl případný pachatel výborné znalosti elektrotechniky, programování a šifrování.

Obr. 40 Sabotáž systému s centrální logikou



5.3.2 Systémy s přímým ovládáním

Systémy s přímým ovládáním jsou často používané, protože u nich není potřeba dokupovat drahou centrální jednotku. Jako centrální jednotku je používáno toto čtecí zařízení. Čtecí zařízení má v sobě svou databázi uživatelů a samo provádí jejich autentizaci. Zároveň slouží jako koncový prvek, který přímo ovládá otevírání dveří nebo spouštění jiných koncových zařízení.

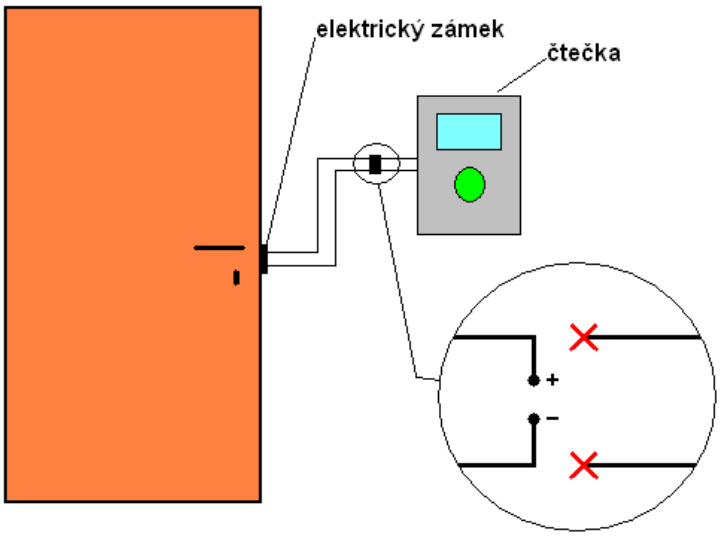
Principiálně je sabotáž systémů s přímým ovládáním velmi jednoduchá. Pokud čtecí zařízení přímo ovládá elektrický zámek, pak stačí nahradit čtecí zařízení korespondujícím napájením. Toto napájení musí odpovídat požadavkům pro daný typ elektrického zámku. Nejčastěji používané hodnoty napájení pro elektrické zámky jsou uvedeny v tabulce 6.

Tab. 6 Systém s přímým ovládáním

Výrobci	Ovládací napětí [V]
FAB	6 - 12
	8 - 12
	10 - 24
	20 - 24
TESLA	6 – 8
	8 - 12
	10 - 12
BEFO	5 - 12
Dorcas	8 - 12

Pokud tedy chceme sabotovat čtecí zařízení, které přímo ovládá elektrický zámek od firmy BEFO, dostaneme se ke kabeláži, která vede od čtecího zařízení do elektrického zámku – viz obr. 41. Tuto kabeláž přerušíme a na vodiče, které vedou k elektrickému zámku, přivedeme napájení o velikosti 5 – 12V. Díky tomuto propojení dokážeme dveře otevřít a to bez nutnosti autentizovat uživatele.

Obr. 41 Sabotáž systému s přímým ovládáním



5.3.3 Systémy využívající PZTS

Systémy využívající PZTS se používají převážně v objektech, které mají nainstalovaný PZTS. Stejně jako u systémů s přímým ovládáním je databáze uživatelů přímo ve čtecím zařízení. Podstatný rozdíl je v tom, že je čtecí zařízení napojeno na ústřednu PZTS, která reaguje na rozpojení (nebo uzavření) smyčky. Takto zapojená čtečka bývá zároveň chráněna proti sabotáži. [33-41]

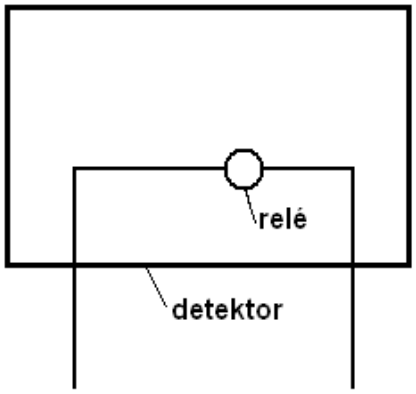
Aby bylo možné takto zapojenou čtečku sabotovat, je důležité si nejprve uvědomit principy a způsoby zapojení PZTS. PZTS běžně využívá N.C. (Normaly Close) smyčky pro klasické zabezpečení a N.O. (Normaly Open) pro požární zabezpečení. Zároveň existuje několik základních způsobů zapojení smyček do PZTS. Jsou to smyčky:

- **jednoduché,**
- **s ATZ (Advanced Technology Zoning – vyvažovací odpor),**
- **s EOL (End Of Line – koncový odpor),**
- **s EOL a ATZ.**

5.3.3.1 Jednoduchá smyčka

Jednoduché smyčky (obr. 42) byly u vzniku zabezpečovacích systémů a až na drobné odchylky se jejich princip používá až do dnešní doby. Jedná se o nejjednodušší zapojení, které je tvořeno jen obyčejnou smyčkou. Tento typ zapojení umožňuje rozeznání pouze jednoho detektoru. Smyčka není chráněna proti jednoduchému přemostění (zkrat). [33-35]

Obr. 42 Jednoduchá smyčka

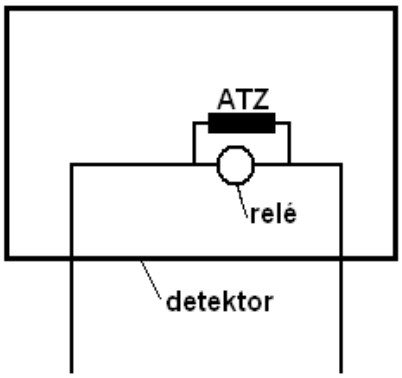


Tento způsob zapojení se v současnosti již prakticky nevyskytuje, jelikož se jedná o necertifikovanou metodu zapojení.

5.3.3.2 Smyčka s ATZ

Smyčka s ATZ (obr. 43) dává možnost zapojit na jednu smyčku víc detektorů, které může systém od sebe rozeznat. Při použití ATZ se nezvyšuje celková bezpečnost zapojení, ale zvyšuje se variabilita zapojení. Ve své podstatě se jedná o zapojení tvořené obyčejnou smyčkou, kde je relé v detektoru paralelně přemostěno odporem. Smyčka není chráněna proti jednoduchému přemostění (zkrat). [35-40]

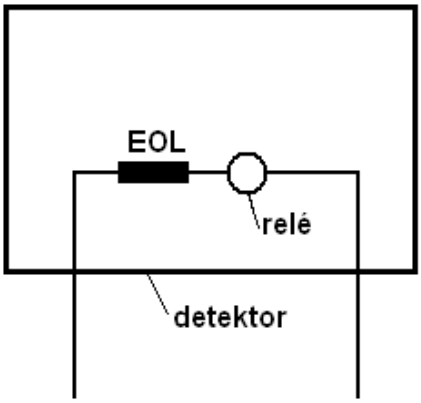
Obr. 43 Jednoduchá smyčka s ATZ



5.3.3.3 Smyčka s EOL

Smyčka s EOL (obr. 44) zvyšuje bezpečnost celkového zapojení. Jedná se o zapojení tvořené obyčejnou smyčkou, kde je v detektoru jeden odpor zapojen do série. Při použití EOL je znemožněno klasické přemostění formou zkratu. Tento druh zapojení má bezpečnostní certifikaci a lze ho sabotovat pouze pokročilejšími způsoby sabotáže. [33-38]

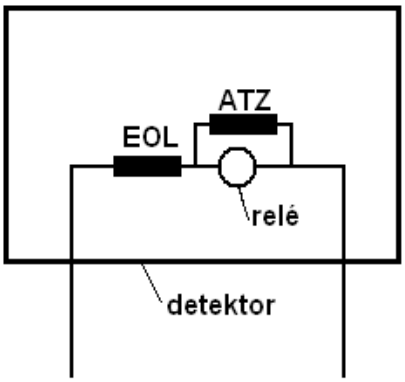
Obr. 44 Jednoduchá smyčka s EOL odporem



5.3.3.4 Smyčka s EOL a ATZ

Smyčka s EOL a ATZ (obr. 45) kombinuje předchozí varianty zapojení. Jedná se o nejvariabilnější a nejbezpečnější způsob zapojení v klasických smyčkových ústřednách. Ve své podstatě se jedná o zapojení tvořené obyčejnou smyčkou, kde je v detektoru jeden odpor zapojen do série a druhý je zapojen přes relé detektoru paralelně. Tento druh zapojení má bezpečnostní certifikaci a lze ho sabotovat pouze pokročilejšími způsoby sabotáže. [33-41]

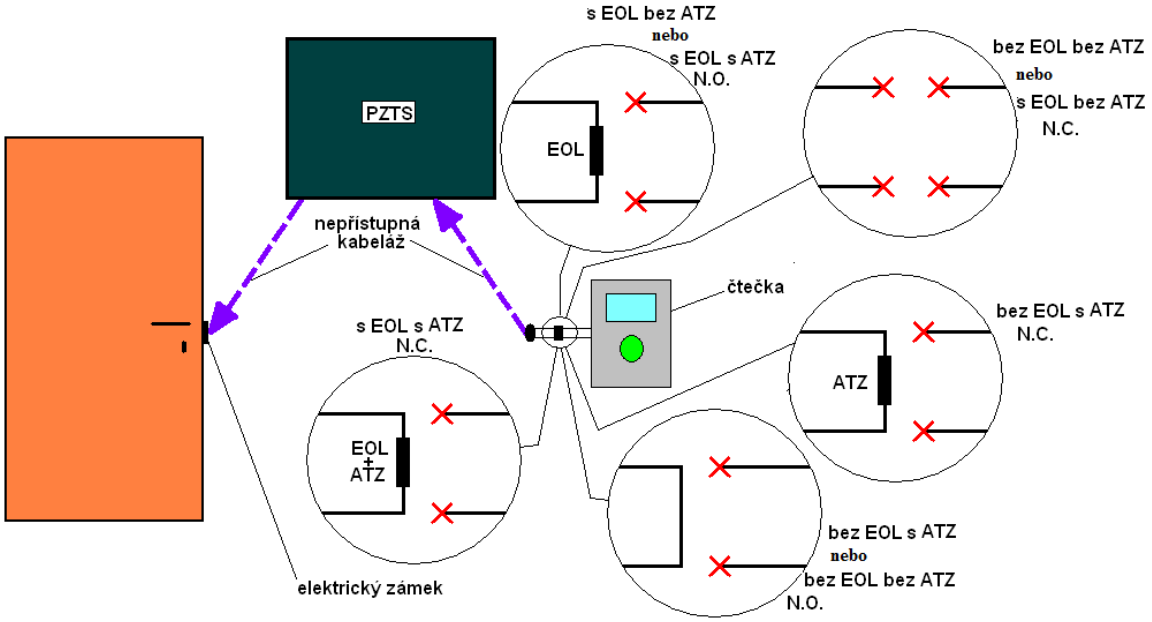
Obr. 45 Jednoduchá smyčka s rozlišením tamperu s EOL odporem



5.3.3.5 Sabotáž čtecího zařízení využívajícího PZTS

Sabotáž čtecího zařízení využívajícího PZTS je komplikovaný především proto, že se nejedná o jeden postup sabotáže, ale může nastat hned několik variant výsledného přemostění – viz obr. 46. Tyto varianty se od sebe liší způsoby zapojení zkratovacího obvodu a je třeba přesně vědět, o jaký typ zapojení se jedná a to dříve, než je daný způsob sabotáže použit.

Obr. 46 Sabotáž systému využívajícího PZTS

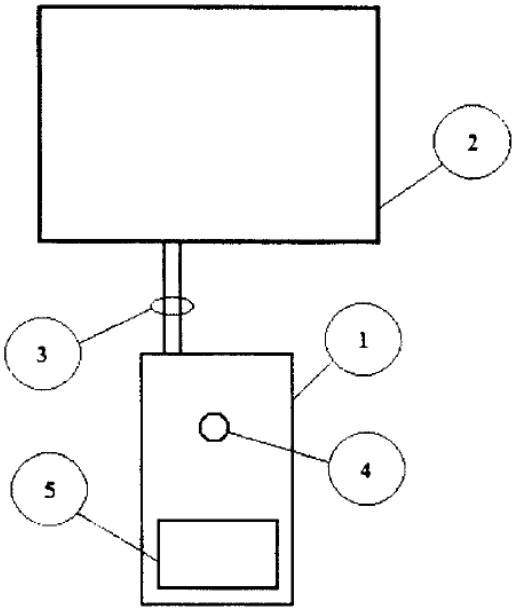


Pokud se jedná o sabotáž zapojení jednoduché smyčky a smyčky s EOL bez ATZ v N.C. obvodu, je možné použít jednoduchý zkrat. Pokud je použitý jiný způsob zapojení, je nutné použít speciální vybavení, které umožní přemostění smyčky.

Zařízení, která to umožňují, jsou „Tester vyvažovacích odporů“ a „Tester poplachových smyček pro testování odolnosti systému proti přemostění“.

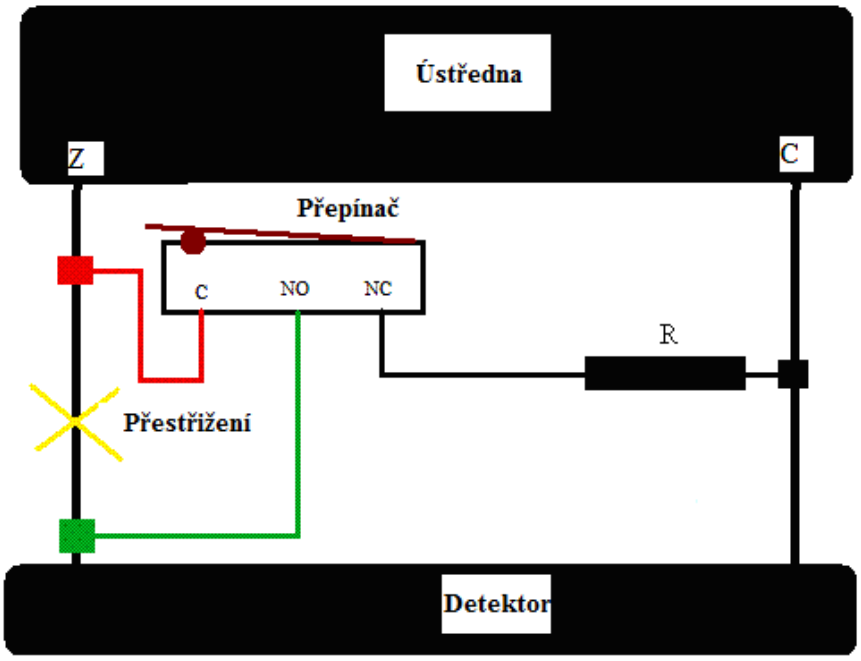
„Tester vyvažovacích odporů“ (obr. 47) testuje maximální a minimální velikost odporu, kterou ústředna akceptuje jako EOL odpor. Zároveň pomocí něho lze přemostit smyčku s EOL odporem, i když za určité kolísavosti odporu. Skládá se z těla testeru 1, na který je z ústředny 2 přivedena smyčka 3, potenciometru 4 a displaye 5. Pomocí displaye je možné zjistit aktuální velikost odporu a dle reakce ústředny vyhodnotíme, jak velký odpor toleruje.

Obr. 47 Tester vyvažovacích odporů



Stejně tak i „Tester poplachových smyček pro testování odolnosti systému proti přemostění“ (obr. 48) slouží jako „Tester vyvažovacích odporů“ k testování smyček u smyčkových ústředen. Na rozdíl od „Testeru vyvažovacích odporů“ netestuje rozmezí, ve kterém ústředna vyhodnocuje přítomnost odporů, ale reakční dobu ústředny při případné sabotáži. Pokud ústředna při testování nedokáže zareagovat, pak není odolná vůči přemostění. Vzhledem k tomu, že se jedná o jednoduchý systém přepínání obvodů, lze jej použít i při samotné sabotáži systému. Dokáže jednorázově nahradit původní obvod s odporem za obvod s identickým odporem, popřípadě za odpor libovolně zvolený.

Obr. 48 Tester poplachových smyček pro testování odolnosti systému proti přemostění



I když lze systém obejít, tak technické řešení EOL vyvažovacích odporů je u PZTS jedním z nejlepších řešení ochrany smyček proti sabotáži přemostěním. Zabraňuje přemostění „*natvrdo*“ (přímé přemostění drátem) a zvyšuje šanci na chybný postup případného sabotéra.

5.3.4 Dílčí závěr elektronické sabotáže u čtecích zařízení

Z uvedených sabotážních technik byly otestovány všechny varianty, až na dekódování sběrnice. Dekódování komunikace přes protokol Wiegand 26 nebylo provedeno z důvodů výsledné ochrany této sběrnice. Pokud by byla tato komunikace dešifrována, byl by tento dešifrovací algoritmus použitelný při sabotáži všech klasických čtecích zařízeních, což by oslabilo jejich bezpečnost.

Výsledná složitost jednotlivých druhů elektronických sabotáží čtecích zařízeních je znázorněna v následující tabulce 7. Parametry byly určovány z pohledu sabotéra, který k sabotáži potřebuje určitý čas, technické vybavení a zároveň se při sabotáži snaží vyhnout riziku jeho odhalení.

Tab. 7 Složitost jednotlivých druhů sabotáží

		Čas sabotáže	Technické vybavení	Riziko odhalení
Systémy s centrální logikou		několik dní	profesionální	velké
Systémy s přímým ovládáním		3 min.	základní	Nulové
Systémy využívající PZTS	**Jednoduchá smyčka N.C.**	1 min.	základní	Malé
	Jednoduchá smyčka N.O.	3 min.	základní	Malé
	s ATZ N.C.	5 min.	pokročilejší	Velké
	s ATZ N.O.	3 min.	základní	Velké
	s EOL N.C.	3 min.	základní	Střední
	s EOL N.O.	5 min.	pokročilejší	Velké
	s EOL a ATZ N.C.	7 min.	pokročilejší	Velké
	s EOL a ATZ N.O.	5 min.	pokročilejší	Velké

5.4 Inovace a vývoj nových biometrických identifikačních systémů

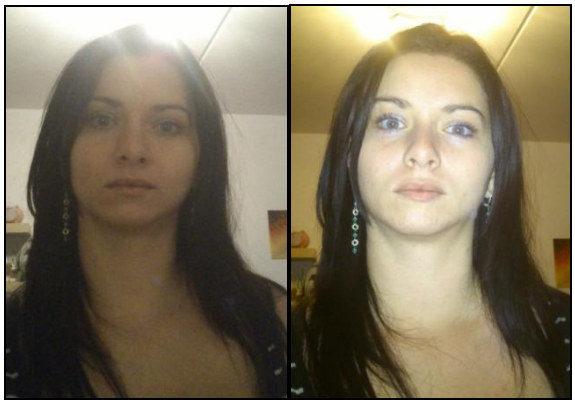
Při řešení této disertační práce bylo zjištěno mnoho nedostatků stávajících biometrických systémů. Tyto nedostatky se projevily jak při samotném měření, tak i při vyhodnocování výsledků hodnot FAR a FFR. Bylo nutné se zamyslet, co zapříčiňuje tak vysoké hodnoty chybných přijetí a odmítnutí nebo například, jak zkrátit pracovní časy 3D čtecích zařízení pro identifikaci dle obličeje.

5.4.1 Přísvit k 3D skeneru obličeje

Po získání negativních výsledků při testování spolehlivosti 3D skenů obličeje bylo nutné se zamyslet nad jednotlivými příčinami. Při standardní identifikaci hodnoty chybného odmítnutí a hodnoty chybného přijetí převýšily v průměru 22,5 %, což se značně liší od hodnot, které jsou uváděny výrobci.

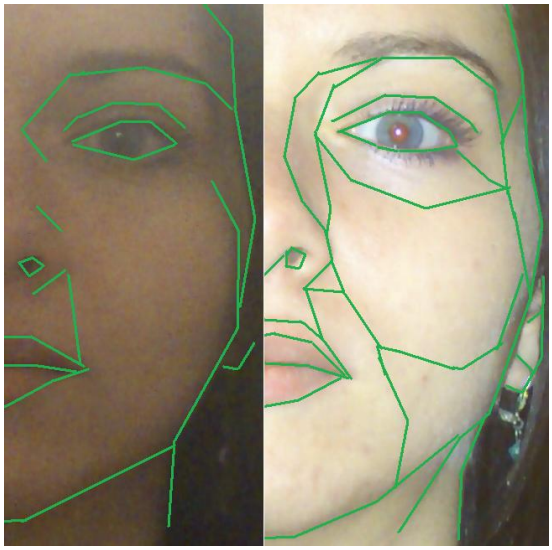
Nejprve se zkoušely různé způsoby umístění čtecího zařízení, různá intenzita osvětlení a nakonec se došlo k závěrům, že současný přísvit, který je zprostředkovaný pomocí infra diod, osvětluje obličej ve velmi malé míře. Jednotlivé znaky, podle kterých dochází k identifikaci uživatele, jsou pak nevýrazné. Při přidání bílého LED (Light Emitting Diode) přísvitu ke čtecím zařízením byly hodnoty chybného odmítnutí a přijetí uživatele nižší o 34 % v případě biometrického systému Multibio 700 a o 40 % nižší u systému IFace 302. Vycházelo se ze snímků na obrázku 49, kde levý snímek je vytvořen bez bílého LED přísvitu a světlo za uživatelem způsobilo podexponování subjektu. Na pravém snímku je přidán bílý LED přísvit, který potlačil světlo v pozadí subjektu a vytvořil správnou expozici subjektu. [42]

Obr. 49 Snímky bez bílé LED diody a s bílou LED diodou



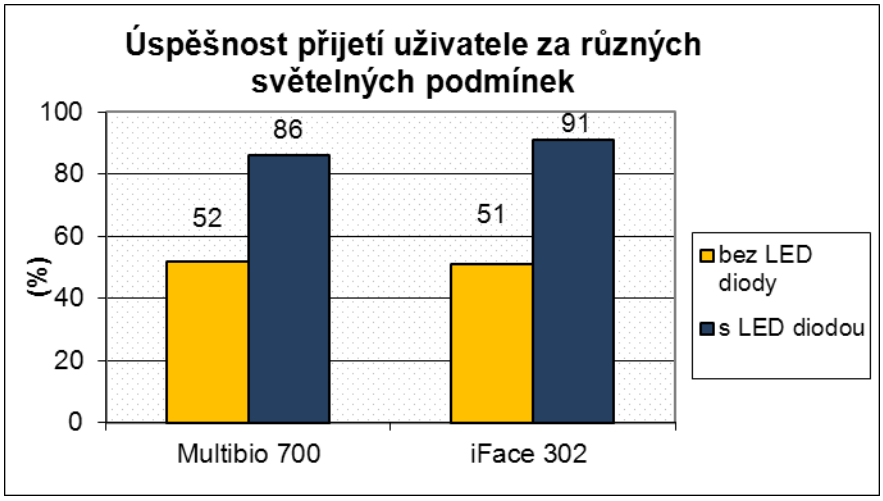
Při pohledu na obrázek 50 jsou vidět rozdíly při použití bílých LED diod na pravé části snímku a již z výroby integrovaným infra přísvitem na levé části snímku. S pouhým infra přísvitem jsou obličejové rysy nevýrazné (nečitelné). U způsobu, kdy je zařízení rozšířeno o bílé LED diody, jsou viditelné veškeré výškové přechody v obličeji (nos, ústa, tvar očí, lícní kosti, uši aj.). Zelená křivka na snímcích znázorňuje identifikační body a zóny, dle kterých dochází k verifikaci uživatele. [42]

Obr. 50 Zobrazení identifikačních linií bez bílé LED diody a s bílou LED diodou



Měření probíhalo na 80 subjektech ve dvaceti cyklech. Z obrázku 51 je zřejmé, že přísvit bílými LED diodami vysoce zvýšil hodnoty bezchybného přijetí uživatele. Krom zvýšení spolehlivosti v průměru o 37 % se také zrychlilo přijetí uživatelů. Bylo tomu z důvodů lepší čitelnosti identifikačních bodů obličeje. [42]

Obr. 51 Úspěšnost identifikace za různých světelných podmínek



5.4.2 Tvorba předlohové šablony

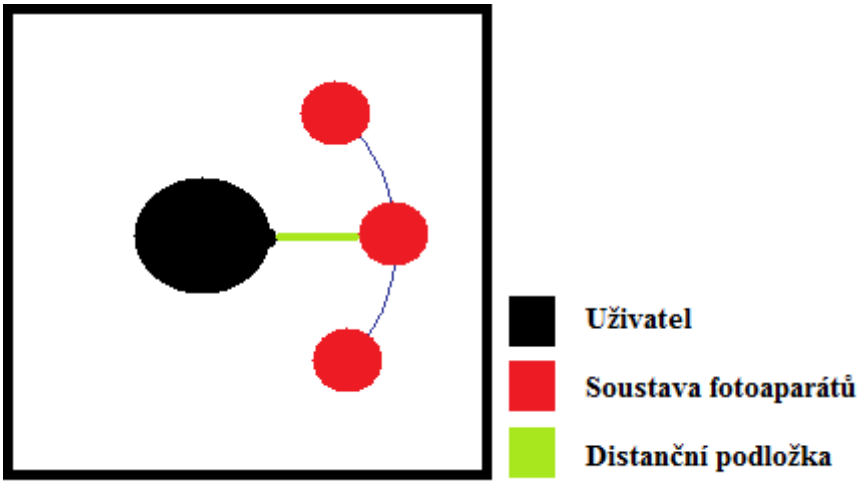
Z tabulky 3 vyplývá, že v průměru 62,5 % uživatelů je do biometrického čtecího zařízení nahráno v uživatelsky přijatelném čase. Zbylých necelých 40 % uživatelů nemá dostatečně čitelné rysy v obličeji, a tedy zadávání jejich předlohových šablon trvá velice dlouhou dobu. Celý proces zadávání uživatele do systému se skládá z šesti kroků. Nejprve se oprávněný uživatel – administrátor přihlásí do systému a zadá příkaz vytvořit nového

uživatele. Dalším krokem je, že vyplní iniciály přidávaného uživatele (jméno, příjmení) a dále mu určí jeho ID číslo (identifikační číslo) a stanový rozsah jeho pravomocí (např. kam uživatel má přístup, zda je oprávněn nahrávat další uživatele do systému). Prostřednictvím identifikačního čísla je možné, aby byl uživatel vpuštěn do objektu (pokud tato možnost není administrátorem omezena – dána další podmínka). V třetím kroku administrátor vyzve uživatele, aby nahrál do čtecího zařízení otisk prstu (3 krát za sebou položí stejný prst na sklíčko čtečky pro otisk prstu). V dalších krocích je uživatel vyzván k sejmutí předlohové šablony pro následnou další identifikaci. V této části uživatel poslouchá příkazy, které jsou v systému přednastaveny na:

1) ***Stůjte před čtečkou a dívejte se na obrazovku***
2) ***Mírně zvedněte hlavu a dívejte se na obrazovku***
3) ***Dívejte se na obrazovku***
4) ***Otočte hlavu mírně vlevo***
5) ***Otočte hlavu mírně vpravo***
6) ***Dívejte se do kamery***

Aby se vyhnulo takovému množství kroků při tvorbě předlohové šablony, bylo navrženo externí zařízení pro její tvorbu. Externí zařízení pro tvorbu předlohové šablony je čtvrt-kružnicového půdorysu, viz obr. 52.

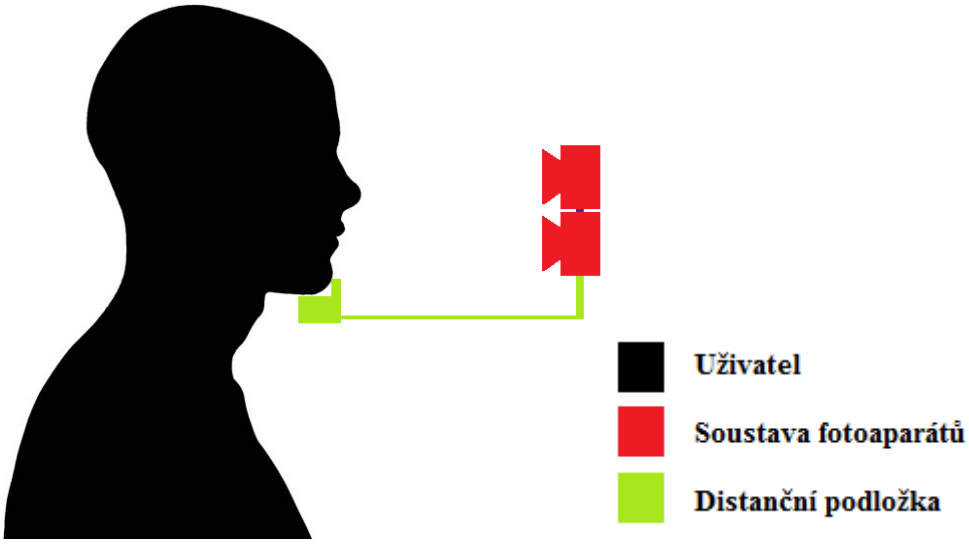
Obr. 52 Půdorys zařízení pro snímání předlohových šablon



Na krajích a ve středu zařízení jsou umístěny dva fotoaparáty (kamery) nad sebou pro snížení časové náročnosti způsobené náklony hlavy. U prostředních fotoaparátů jsou umístěny čtyři bílé LED diody pro vhodnější osvětlení obličeje, díky kterému jsou lépe viditelné

identifikační záchytné body. Ze spodní stěny zařízení vede distanční podložka (držák na podbradek), viz obr. 53.

Obr. 53 Bokorys zařízení pro snímání předlohových šablon



Tato distanční podložka je 15cm dlouhá, aby snímky uživatelů byly vždy ve stejné velikosti. Podbradek slouží k zaaretování obličeje a je nasazen na distanční podložku. Tento podbradek je ve dvou variantách. Buď univerzální, který je po každém uživateli očištěn desinfekčním ubrouskem, nebo umělohmotný jednorázový (uživatel si ho zakoupí jako nadstandardní vybavení). Vždy pro vytvoření šablony jsou sejmuty dva snímky uživatele. Toto zařízení je externí a na kompatibilitě s různými zařízeními se v současné době pracuje. Testované čtečky pracují se ZK softwarem jako většina biometrických 3D čteček obličeje na českém trhu. Propojení s biometrickým identifikačním zařízením je přes USB. Většinou se ovšem zařízení nepřipojuje k biometrické čtečce, ale k počítači, ve kterém je nahrán software pro obsluhu čteček. Prostřednictvím USB kabelu jsou předlohové šablony nahrány do systému čteček najednou. Tímto způsobem se zadávání předlohových šablon do systému časově velice zkrátí. Veškeré osobní údaje a ID uživatele jsou do systému vloženy prostřednictvím počítače, což opět zkracuje délku vytváření profilu uživatele.

5.4.3 Sken ruky

Současné biometrické identifikační systémy dokážou číst téměř všechny jedinečné údaje z lidského těla. Jedna z možností inovace tak připadá na identifikaci dle kůstek v kostře zápěstí (karpální kosti). Lze je však s jistotou číst pouze za pomoci rentgenového záření. Avšak tento způsob je z dlouhodobého hlediska používání velmi zdravotně rizikový a tedy prakticky ho nelze použít. [43]

Je však jistota, že kostra (tj. jednotlivé kosti a jejich držení) je pro každého jedince zcela typická. Informace o některých jiných kostech lze získat daleko jednodušeji bezkontaktními metodami i bez rentgenového záření. Nicméně snadno dostupnou částí těla pro identifikaci zůstává ruka a odečtené hodnoty rozměrů z ní mohou sloužit pro jednoznačnou kombinaci. Tato metoda je vhodná i pro kombinaci s čtečkami prstů či celé dlaně (skenery). [43]

Stávající zařízení dokáže snímat opticky hřbet ruky. Dlaň ruky může být ve stejný okamžik snímána pro daktyloskopickou identifikaci (sken dlaně – sken papilárních linií). Tento duální způsob identifikace je jedinečný. Zařízení lze použít pouze jako sken ruky, či jako bezpečnější duální biometrický identifikační systém. [43]

Celý vývoj duálního biometrického identifikačního systému začal stanovením identifikační zóny. Tuto zónu představovala ruka (vrch i dlaň). Za pomoci softwarového vybavení došlo k sestavení prostorového modelu ruky ze získaných snímků. Poté bylo nutno na modelu najít klíčová místa pro odečítání rozměrů a úhlů. Tím došlo ke vniku předlohového identifikačního modelu uživatele. Posléze se porovnal sejmutý údaj s údaji, které byly vloženy do databáze, a identifikovala se konkrétní osoba. [43]

Systémy, které již existují, disponují fixačními zarážkami, které se nachází mezi prsty a aretují tím položení ruky do přístroje. Pro jedinečnost snímaného objektu bylo mechanické omezování pozice dlaně v přístroji nevhodné, protože přirozeně položená ruka nabízí daleko více klíčových bodů pro identifikaci. Prostředkem k porovnání byly stanoveny pevně dané rozměry na dlani, které nemohou být ovlivněny např. okolní teplotou nebo krevním tlakem. Bylo zvoleno porovnání poměru délek prstů, sevření úhlů mezi nimi, orientace palce, postavení palce vůči dlani a ostatním prstům, oblouk dlaně na několika místech, tloušťka prstů v kloubech, tvar lůžek nehtů, pozice mateřských znamének a další. Mezi identifikační body nebylo možno zařadit absolutní rozměr dlaně či její plochy, jelikož tyto hodnoty mohou být ovlivněny mírou přítlaku k desce přístroje. [43]

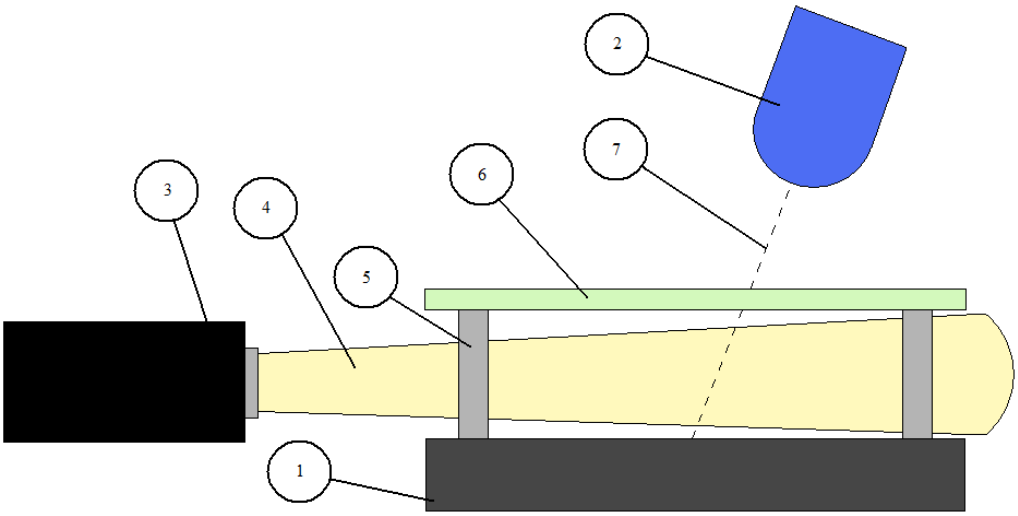
Při dalším vývoji bylo nutné mít na paměti, že ruka může být do přístroje vždy položena trochu jinak, proto bylo nutné vytvořit takový matematický model spojený s anatomickými údaji, který zajistí relevantní data. U tohoto systému nebylo možné zkoumat tvar ruky z obrysu a bylo nutné ignorovat i cizí objekty na ruce, tj. prstýnky či tetování. Taktéž ke změně délky nehtů muselo být přihlíženo. K technickému řešení duálního skeneru bylo využito znalosti snímaného objektu, který měl vždy podobný tvar, a podmínky pro snímání byly vždy stejné (laboratorní). Byly zvoleny dvě metody pro tento výzkum. [43]

První metodou bylo snímání ruky fotoaparátem z několika přesně daných úhlů a následně využití specializovaného softwaru, který ze snímků vytvořil digitální prostorový model. Ukázalo se, že dodržení doporučených úhlů, referenčních terčíků a vhodných podmínek pro fotografování je základem pro kvalitní model s dostatečnou přesností. V případě realizace přístroje v praxi, toto zařízení muselo být vybaveno několika fotoaparáty pro každý potřebný úhel, což by přístroj prodražilo, nicméně by cena přístroje byla stále přijatelná. [43]

Druhá metoda využívala pouze jeden fotoaparát a světelný zdroj, který s fotoaparátem svíral určitý úhel 30°, viz obr. 54. Tato metoda byla tedy vhodnější pro praktické užití v přístroji. Výsledkem byl stejný model jako u metody první. [43]

Z těchto dvou metod byla pro konečné sestavení prototypu vybrána metoda číslo dvě. Jako světelný zdroj se použil dataprojektor s vysokým rozlišením a širokým barevným spektrem. Světelný zdroj byl umístěn vodorovně se skleněnou plochou. Ve výšce byl zaaretován fotoaparát, který svíral s koncovou deskou úhel o velikosti 30 °. Mezi skleněnou plochou a skenerem dlaně popřípadě podkladovou deskou, která byla potažena matně černou samolepící folií, byl vytvořen uživatelsky přijatelný prostor pro vložení ruky. [43]

Obr. 54 Bokorys duálního biometrického identifikačního systému



(1) skener dlaně

(2) fotoaparát

(3) zdroj světelného záření

(4) světelné záření

(5) distanční sloupek

(6) skleněná plocha

(7) úhel snímání

U tohoto způsobu identifikace by mohl vzniknout problém v případě těžkého poranění na ruce, které by mohlo měření identifikačních bodů na ruce znemožnit. V některých případech může dojít k snížení spolehlivosti např. ztrátou prstu, v jiných případech naopak k zvýšení spolehlivosti např. špatně srostlou kostí způsobující atypický tvar prstu. [43]

Zařízení zkoumá skutečný prostorový objekt, případná sabotáž bude možná jen např. pomocí odlitku ruky. Lze však použít již známé metody, které dokážou určit, že se nejedná o živou hmotu (detekce krevního řečiště či jednodušší způsob – pyroelement). Aplikace takovéhoto vylepšení není finančně náročná a procento spolehlivosti identifikačního systému by se výrazně zvýšilo. [43]

V současné době se pracuje na miniaturizaci tohoto zařízení, jelikož současné rozměry jsou pro komerční účely příliš veliké.

5.4.4 Biometrická autorizace pro využití služebního vozidla

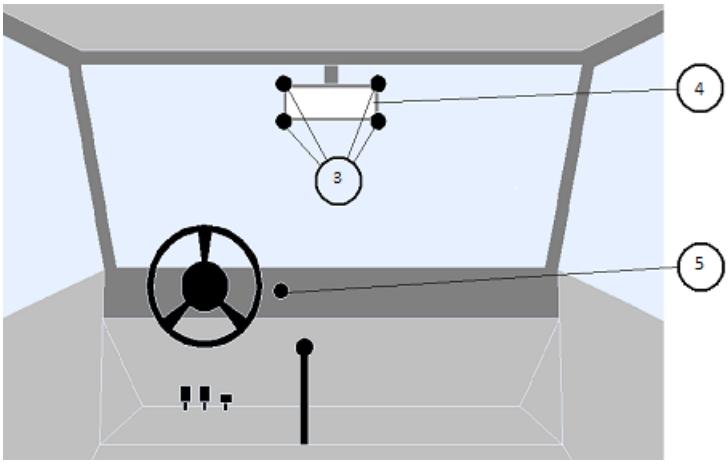
Při tomto vývoji se oblast zájmu rozšířila i do jiného odvětví a to do automobilového průmyslu. V sériové výrobě je možno vidět odemykání automobilů prostřednictvím čipů, které jsou zabudovány buď v klíčku nebo ve startovací kartě automobilu. Pouhé přiblížení tohoto zařízení k automobilu způsobí jeho odemknutí. Biometrie je u automobilového průmyslu v úplném počátku a ve stejném stádiu je i dohled nad služebními vozidly, který je v dnešní době zprostředkovaný GPS moduly, knihami jízd a tachografy. Tímto způsobem však nelze plnohodnotně určit, jaká osoba ve skutečnosti řídí služební vozidlo. Služební vozidla se pak využívají na jiné účely, než pro které jsou určeny.

Technické řešení tohoto vývoje se týká konstrukce systému na biometrickou autorizaci pro využití služebního vozidla. Toto řešení slouží k zamezení pohybu služebního vozidla neoprávněnou osobou a k evidenci osob, které služební vozidlo využijí.

Biometrická autorizace pro využití služebního vozidla se skládá ze vstupního systému, který je tvořen biometrickou čtečkou otisků prstů a biometrickým identifikačním systémem pro pořízení 3D skenu obličeje.

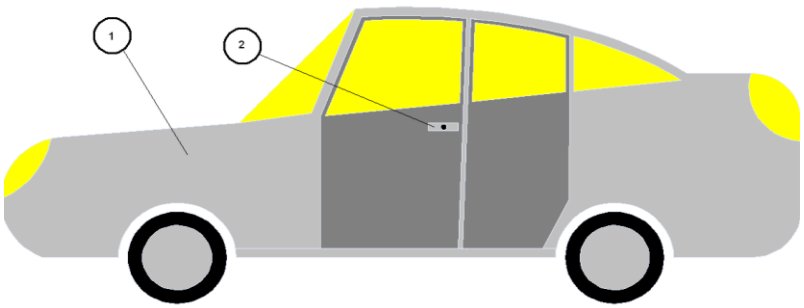
Na kliku vozidla je připevněna biometrická čtečka otisků prstů, která je propojena s vyhodnocovací jednotkou otisků prstů. Vyhodnocovací jednotka otisku prstů je připojena přívodní kabeláží z 3D skeneru a výstupní kabeláží vedoucí k řídící jednotce motoru. Vyhodnocovací jednotka otisku prstů se skládá z procesoru a integrované paměti. Na zpětném zrcátku jsou umístěny čtyři čidla pro 3D sken, viz obr. 55. To celé je taktéž propojeno se startovací jednotkou motoru i s jednotkou pro identifikaci obličeje.

Obr. 55 Zobrazení umístění čidel 3D skeneru



Každý zaměstnanec, který chce použít vozidlo, nejprve přiloží prst na čtečku otisku prstů, viz obr. 56, která vyšle získané informace do vyhodnocovací jednotky otisku prstů. Pokud dojde ke shodě otisku prstu s databází zaměstnanců, která je nahraná v integrované paměti, vyšle vyhodnocovací jednotka otisku prstů signál zámkovému systému a dojde k odemknutí vozidla. Poté se osoba usadí, zajistí se bezpečnostními pásy a následně stiskne startovací tlačítko, které spustí 3D sken obličeje. Po dokončení 3D skenu obličeje se odešle sken do vyhodnocovací jednotky pro identifikaci obličeje. Dojde-li ke shodě skenu obličeje s databází zaměstnanců, vozidlo se nastartuje a zároveň se veškeré komponenty upraví dle parametrů dané osoby (osobního nastavení).

Obr. 56 Znázornění čtečky otisku prstů na vozidle



(1) vyhodnocovací jednotka pro identifikaci

(2) klika s čtečkou otisků prstů

(3) čidla pro 3D sken

(4) zpětné zrcátko

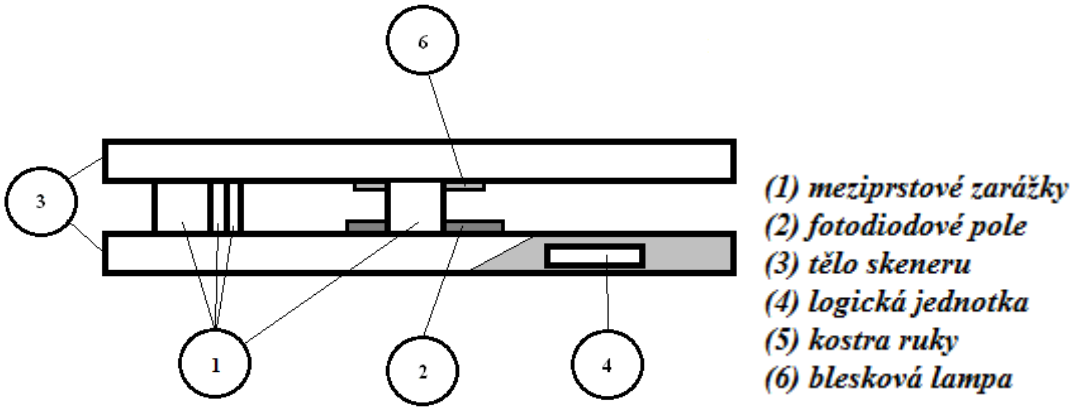
(5) startovací tlačítko

5.4.5 Biometrický sken dlaně

Technické řešení se týká konstrukce systému pro biometrickou autentizaci na základě biometrického skenu dlaně. Toto řešení slouží k zamezení neoprávněnému pohybu a vstupu osob v určitých oblastech, kde je omezen přístup.

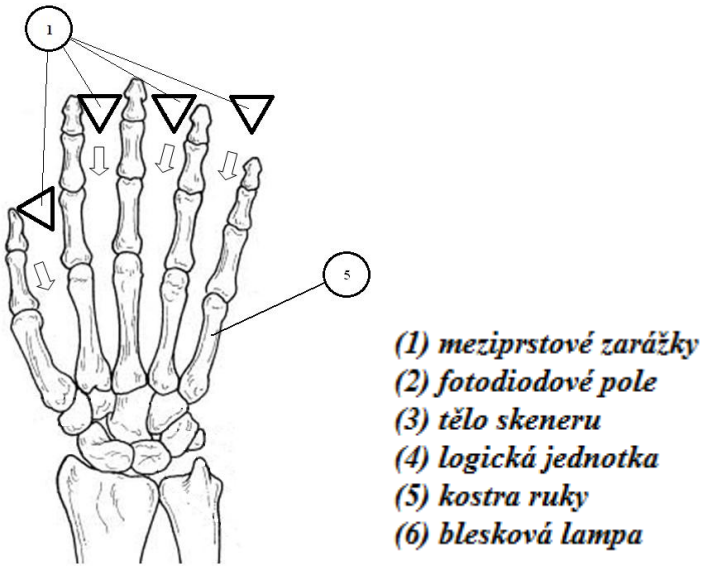
Biometrický skener dlaně se skládá z mezi-prstových zábran umístěných na spodní části těla skeneru, skenovací plochy umístěné před mezi-prstovými zábranami, logické jednotky integrované do těla skeneru a z těla skeneru, viz obr. 57.

Obr. 57 Bokorys biometrického skeneru dlaně s částečným řezem v místě logické jednotky



Mezi-prstové zábrany slouží k přesnému ukotvení dlaně a pro její znehybnění, viz obr. 58. Po upevnění dlaně se záprstní kosti nacházejí přímo nad skenovací plochou. Jakmile se dlaň celým povrchem dotkne skenovací plochy, dojde k sejmutí skenu.

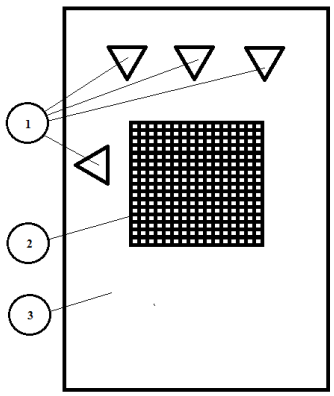
Obr. 58 Kostra ruky s mezi-prstovými zábranami



Nejprve probleskne ruku blesková lampa, která je umístěna v horní části těla skeneru a to přímo naproti skenovací ploše. Ta se skládá z malých fotodiod, které na problesknutí zareagují, viz obr. 59. Naskenovaná data jsou odeslána logické jednotce, která je součástí těla

skeneru. Zde se data zpracují a poté se porovnají s databází. Tato databáze nemusí být přímo v biometrickém skeneru dlaně, ale může být ve vyhodnocovací jednotce, ke které může být biometrický skener dlaně připojen. V případě shody dojde k otevření chráněného prostoru.

Obr. 59 Mezi-prstové zábrany se skenovací plochou



(1) meziprstové zarážky

(2) fotodiodové pole

(3) tělo skeneru

(4) logická jednotka

(5) kostra ruky

(6) blesková lampa

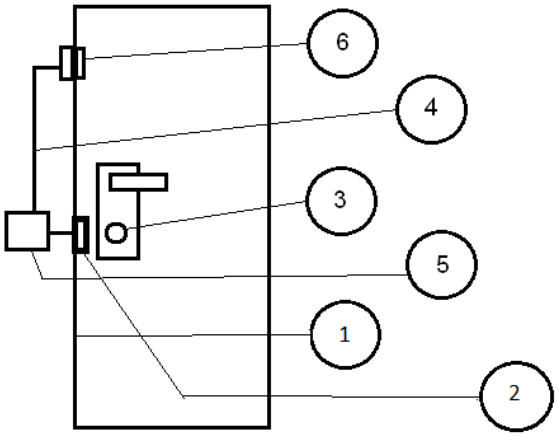
5.4.6 Zámkový systém s biometrickým skenem nehtového lůžka

Technické řešení se týká konstrukce bezpečnostního biometrického vstupního zařízení. Tento systém umožní větší zabezpečení vstupního prostoru tím, že dojde ke kombinaci mechanického zámku a skeneru nehtového lůžka. Zámkový systém s biometrickým skenem nehtového lůžka je složený z mechanického zámku, elektrického zámku, vyhodnocovací jednotky a skeneru nehtového lůžka.

Funkce zámkového systému s biometrickým skenem nehtového lůžka je založena na principu dvou vstupních fází. V první fázi dojde k odemknutí mechanického zámku (klíčem), naskenování nehtového lůžka a k identifikaci dané osoby. Na zárubni je nainstalovaný skener nehtového lůžka v takové výšce, aby byl v úrovni mechanického zámku, viz obr. 60. Při zasunutí klíče do zámkové vložky a jeho otočení, dojde k odemknutí mechanického zámku a naskenování nehtového lůžka. Scanner nehtového lůžka předá naskenované údaje do vyhodnocovací jednotky, která je kabelovými rozvody propojena jak se scannerem nehtového lůžka, tak s elektrickým zámkem. Vyhodnocovací jednotka vyhodnotí, zda je identifikační požadavek splněn. Pokud je identifikační požadavek splněn, přechází se do druhé fáze

odemykání, kde se odemkne elektrický zámek a dotyčný je vpuštěn do daného prostoru. Vyhodnocení, naskenování nehtového lůžka a identifikace probíhá v časovém rozmezí milisekund a tudíž je celkový postup odemknutí časově nenáročný.

Obr. 60 Schéma biometrického systému pro sken nehtového lůžka



(1) zárubně dveří

(2) skener nehtového lůžka

(3) mechanický zámek

(4) kabelové rozvody

(5) vyhodnocovací jednotka

(6) elektrický zámek

Vyhodnocením biometrického skenu je možno detekovat neoprávněný pokus o vniknutí do hlídaných prostor. Vyhodnocovací jednotka je napojena na elektrický zámek. Pokud není identifikační požadavek splněn, nedojde k otevření elektrického zámku a může být podána informace (o neoprávněném vstupu) do ústředny elektrických zabezpečovacích systémů, která reaguje dle svého naprogramování.

6 Vyhodnocení hypotéz

K vyhodnocení hypotéz číslo 1, 3 a 4 byl použit jedno-výběrový test relativních četností pro parametr π: [44]

1) H_0: $\pi 1 = \pi 2$
2) H_a: $\pi 1 \neq \pi 2$
3) *Byla stanovena hladina významnosti* $\alpha = 0{,}05$
4) *Testovací kritérium:*

$$u = \frac{\frac{m}{n} - \pi_0}{\sqrt{\frac{\pi_0 . (1 - \pi_0)}{n}}} \tag{6.1}$$

5) *Stanovení* $u\alpha$ *(ze statistických tabulek dle dané hladiny významnosti)* $u\alpha = 1{,}96$
6) *Kritický obor*
7) $K: (|u| > u\alpha)$ (6.2)

K vyhodnocení hypotézy číslo 2 byl použit dvou-výběrový test relativních četností pro parametr π: [44]

1) H_0: $\pi = \pi 0$
2) H_a: $\pi \neq \pi 0$
3) *Byla stanovena hladina významnosti* $\alpha = 0{,}05$
4) *Testovací kritérium:*

$$u = \frac{\frac{m_1}{n_1} - \frac{m_2}{n_2}}{\sqrt{\bar{p}.(1-\bar{p}).(\frac{1}{n_1}+\frac{1}{n_2})}} \tag{6.3}$$

$$\bar{p} = \frac{m_1 + m_2}{n_1 + n_2} \tag{6.4}$$

5) *Stanovení* $u\alpha$ *(ze statistických tabulek dle dané hladiny významnosti)* $u\alpha = 1{,}96$
6) *Kritický obor*

$K: (|u| > u\alpha)$ (6.5)

6.1 Hypotéza číslo 1

Hypotéza č. 1: Poranění prstových lůžek ve vysoké míře ovlivňuje hodnoty chybného odmítnutí uživatele.

a) Řezné ranky

H_0: $\pi 1 = \pi 2$

H_a: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{55}{800} - 0{,}0794}{\sqrt{\frac{0{,}0794.(1 - 0{,}0794)}{800}}}$$

$$u = -1{,}11$$

Stanovení $u\alpha$ (ze statistických tabulek dle dané hladiny významnosti):

$u\alpha = 1{,}96$

Kritický obor:

K: ($|u| > u\alpha$)

K: ($|-1{,}11| > 1{,}96$)

H_0 se nezamítá → poranění způsobené řeznými rankami neovlivňuje ve vysoké míře chybné odmítnutí uživatele. Naměřené hodnoty se zanedbatelně zvýšily oproti hodnotám získaných u standardní identifikace.

b) Popálení lůžka prstu

H_0: $\pi 1 = \pi 2$

Ha: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{55}{800} - 0{,}1231}{\sqrt{\frac{0{,}1231.(1 - 0{,}1231)}{800}}}$$

$$u = -4{,}685$$

Stanovení uα (ze statistických tabulek dle dané hladiny významnosti):

$u\alpha = 1{,}96$

Kritický obor:

$K: (|u| > u\alpha)$

$K: (|-4{,}685| > 1{,}96)$

H_0 se zamítá → poranění způsobené drobným popálením prstového lůžka ve vysoké míře ovlivňuje chybné odmítnutí uživatele. Hodnota chybného odmítnutí uživatele se zvýšila téměř o polovinu. Průměrná hodnota chybného odmítnutí u standardní identifikace byla 6,875 % a u poranění způsobeným popálení byla průměrná hodnota FRR = 12,31 %.

c) Obroušení

H_0: $\pi 1 = \pi 2$

H_a: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{55}{800} - 0{,}3281}{\sqrt{\frac{0{,}3281.(1-0{,}3281)}{800}}}$$

$$u = -15{,}62$$

Stanovení uα (ze statistických tabulek dle dané hladiny významnosti):

$u\alpha = 1{,}96$

Kritický obor:

$K: (|u| > u\alpha)$

$K: (|-15{,}62| > 1{,}96)$

H_0 se zamítá → poranění způsobené obroušením prstového lůžka ve vysoké míře ovlivňuje chybné odmítnutí uživatele. Hodnoty chybného odmítnutí uživatele vzrostly více než o pětinásobek oproti standardní identifikaci.

d) Otlačení

H_0: $\pi 1 = \pi 2$

H_a: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{55}{800} - 0{,}0775}{\sqrt{\frac{0{,}0775.(1-0{,}0775)}{800}}}$$

$$u = -0{,}93$$

Stanovení uα (ze statistických tabulek dle dané hladiny významnosti):

uα = 1,96

Kritický obor:

K: (| u | > uα)

K: (| -0,93 | > 1,96)

H_0 se nezamítá → poranění způsobené otlačením prstového lůžka ve vysoké míře neovlivňuje chybné odmítnutí uživatele. Hodnoty chybného odmítnutí uživatele oproti standardní identifikaci vzrostly o 0,875 %, což je statisticky zanedbatelné.

Hypotéza č. 1 se vzhledem k výsledkům jedno-výběrového testu relativních četností provedeného u testů řezné ranky, popálení lůžka prstu, obroušení a otlačení **potvrzuje pouze částečně.**

6.2 Hypotéza číslo 2

Hypotéza č. 2: Schopnost identifikace a chybovost (hodnoty FAR a FRR) by měla být u obou 3D čteček obličeje (Multibio700 a IFace302) shodná v důsledku použití stejného vyhodnocovacího softwaru.

H_0: $\pi = \pi_0$

H_a: $\pi \neq \pi_0$

Hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{266{,}56}{1600} - \frac{323{,}04}{1600}}{\sqrt{0{,}18425.(1-0{,}18425).(\frac{1}{1600}+\frac{1}{1600})}}$$

$$u = -2{,}57536$$

$$\bar{p} = \frac{266{,}56+323{,}04}{1600+1600}$$

$$\bar{p} = 0{,}18425$$

Stanovení u_α (ze statistických tabulek dle dané hladiny významnosti):

$u_\alpha = 1{,}96$

Kritický obor:

K: ($|u| > u_\alpha$)

K: ($|-2{,}57536| > 1{,}96$)

H_0 se zamítá → schopnost identifikace a chybovosti je u obou 3D čteček obličeje využívající stejný software shodná. Jednotlivé hodnoty se od sebe statisticky liší zanedbatelně.

Hypotéza č. 2 se vzhledem k výsledkům dvou-výběrového testu relativních četností **zamítá**.

6.3 Hypotéza číslo 3

Hypotéza č. 3: Znečištění obličeje vysoce ovlivňuje hodnoty chybného odmítnutí uživatele.

a) Statistický výpočet pro biometrický systém Multibio700

H_0: $\pi 1 = \pi 2$

H_a: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{79}{100} - 0{,}62}{\sqrt{\frac{0{,}62.(1-0{,}62)}{100}}}$$

$$u = 3{,}5$$

Stanovení $u\alpha$ (ze statistických tabulek dle dané hladiny významnosti):

$u\alpha = 1{,}96$

Kritický obor:

K: ($|u| > u_\alpha$)

K: ($|3{,}5| > 1{,}96$)

H_0 se zamítá → znečištění obličeje obecně, vysoce ovlivňuje hodnoty chybného odmítnutí uživatele.

b) Statistický výpočet pro biometrický systém IFace302

H_0: $\pi 1 = \pi 2$

H_a: $\pi 1 \neq \pi 2$

Byla stanovena hladina významnosti:

$\alpha = 0,05$

Testovací kritérium:

$$u = \frac{\frac{84}{100} - 0,63}{\sqrt{\frac{0,63.(1-0,63)}{100}}}$$

$$u = 4,35$$

Stanovení uα (ze statistických tabulek dle dané hladiny významnosti):

$u\alpha = 1,96$

Kritický obor:

$K: (|u| > u_\alpha)$

$K: (|4,35| > 1,96)$

H_0 se zamítá → znečištění obličeje obecně, vysoce ovlivňuje hodnoty chybného odmítnutí uživatele.

Hypotéza č. 3 se vzhledem k výsledkům jedno-výběrového testu relativních četností provedených u čteček IFace302 a Multibio700 **zamítá**.

6.4 Hypotéza číslo 4

Hypotéza č. 4: Přísvit pomocí bílých LED diod snižuje chybovost 3D čteček obličeje oproti použití samostatného integrovaného Infra přísvitu z výroby.

a) Statistický výpočet pro biometrický systém Multibio700

H_0: $\pi = \pi_0$

H_a: $\pi \neq \pi_0$

Hladina významnosti:

$\alpha = 0,05$

Testovací kritérium:

$$u = \frac{\frac{768}{1600} - 0{,}14}{\sqrt{\frac{0{,}14.(1-0{,}14)}{1600}}}$$

$$u = 39{,}19$$

Stanovení u_α (ze statistických tabulek dle dané hladiny významnosti):

$u_\alpha = 1{,}96$

Kritický obor:

K: ($|u| > u_\alpha$)

K: ($|39{,}19| > 1{,}96$)

H_0 se zamítá → přidáním bílých LED diod ve vysoké míře snižuje chybovost 3D čteček obličeje. Procentuálně se u biometrického systému Multibio700 sníží chybovost o 34 %.

b) Statistický výpočet pro biometrický systém IFace302

H_0: $\pi = \pi_0$

H_a: $\pi \neq \pi_0$

Hladina významnosti:

$\alpha = 0{,}05$

Testovací kritérium:

$$u = \frac{\frac{784}{1600} - 0{,}09}{\sqrt{\frac{0{,}09.(1-0{,}09)}{1600}}}$$

$$u = 55{,}90$$

Stanovení u_α (ze statistických tabulek dle dané hladiny významnosti):

$u_\alpha = 1{,}96$

Kritický obor:

K: ($|u| > u_\alpha$)

K: ($|55{,}90| > 1{,}96$)

H_0 se zamítá → přidáním bílých LED diod ve vysoké míře snižuje chybovost 3D čteček obličeje. Procentuálně se u biometrického systému IFace302 sníží chybovost o 40 %.

Hypotéza č. 4 se vzhledem k výsledkům jedno-výběrového testu relativních četností provedených u čteček IFace302 a Multibio700 **zamítá**.

6.5 Hypotéza číslo 5

Hypotéza č. 5: Použití jiného propojení s koncovým prvkem než po sběrnici Wiegand a zároveň využití systému centrální jednotky snižuje bezpečnost ochrany vstupu.

Na základě provedeného testování byly nastaveny váhové koeficienty u jednotlivých druhů hodnocených parametrů – viz tab. 8. U tohoto přiřazování se pomocí bodovací metody v multikriteriální analýze variant přiřadilo bodové ohodnocení následujícím způsobem. Jak u času sabotáže, technického vybavení tak i u rizika odhalení byly váhy přiřazeny od nejmenšího po největší (nejmenší čas sabotáže, nejmenší potřeba technického vybavení k sabotáži nebo nejmenší riziko odhalení se umístilo na první místo), přičemž když vznikla rovnost hodnot, tak se z výsledného hodnocení vytvořil průměr.

Tab. 8 Váhové koeficienty u složitosti jednotlivých druhů sabotáží

		Čas sabotáže	Technické vybavení	Riziko odhalení
Systémy s centrální logikou		10	10	7,5
Systémy s přímým ovládáním		3,5	3	1
Systémy využívající PZTS	**Jednoduchá smyčka N.C.**	1	3	2,5
	Jednoduchá smyčka N.O.	3,5	3	2,5
	s ATZ N.C.	7	7,5	7,5
	s ATZ N.O.	3,5	3	7,5
	s EOL N.C.	3,5	3	4
	s EOL N.O.	7	7,5	7,5
	s EOL a ATZ N.C.	9	7,5	7,5
	s EOL a ATZ N.O.	7	7,5	7,5

Výsledná suma váhových koeficientů je uvedena v tabulce 9. V této tabulce je zároveň uvedena výsledná hodnota váhového třídění. Výslednou sumu vah určuje součet bodů jednotlivých řádků tabulky číslo 8.

Tab. 9 Váhové koeficienty u složitosti jednotlivých druhů sabotáží

		∑ vah	Pořadí
Systémy s centrální logikou		27,5	**10**
Systémy s přímým ovládáním		7,5	**2**
Systémy využívající PZTS	**Jednoduchá smyčka N.C.**	6,5	**1**
	Jednoduchá smyčka N.O.	9	**3**
	s ATZ N.C.	22	**6 – 8**
	s ATZ N.O.	14	**5**
	s EOL N.C.	10,5	**4**
	s EOL N.O.	22	**6 – 8**
	s EOL a ATZ N.C.	24	**9**
	s EOL a ATZ N.O.	22	**6 – 8**

Z výsledné sumy váhových koeficientů je patrné, že největším rizikem pro zapojení čtecích zařízení je zapojení čtecího zařízení, jako systému s přímým ovládáním a systému využívajícího PZTS za použití jednoduché smyčky. Oproti tomu použití systému s centrální logikou se jeví jako nejbezpečnější varianta.

V praxi je proto důležité, aby se u čtecích zařízení opustilo od varianty využívání systémů zapojení pomocí přímého ovládání a využití PZTS a přešlo se pouze na systémy s centrální logikou.

Hypotéza č. 5 se vzhledem k jednoznačným výsledkům bodovací metody v multikriteriální analýze variant **potvrzuje**.

7 Diskuze

V dnešní době je problematika biometrických identifikačních systémů stále více diskutována. Tyto systémy slouží především k ochraně vstupu do chráněných prostor nebo ochraňují přístup k utajovaným informacím, ke kterým mají přístup pouze určité osoby. Při pohledu na kritickou infrastrukturu, kde je nejpřednějším odvětvím energetika, je nutné se zamyslet nad spolehlivostí stávajících přístupových a zabezpečovacích systémů. Tato dizertace se věnuje pouze biometrickým přístupovým systémům, a proto lze posuzovat pouze tuto stránku zabezpečení.

Z této disertační práce je patrné, že spolehlivost vybraných testovaných čtecích zařízení není příliš uspokojivá. Tato zařízení by bylo vhodné použít pouze do oblastí, do kterých není vstup neoprávněné osoby prioritní. Pokud se ovšem jedná o útvary s vysokým stupněm zabezpečení, jako jsou ministerstva, vojenské útvary, mikrobiologické ústavy, jaderné elektrárny, vládní instituce aj. jsou získané hodnoty FAR a FRR vysoce rizikové. Dle mého názoru je vývoj nových biometrických systémů zbytečný, bez otestování stávajících, jelikož jednotlivé testy mne dovedly právě k vhodným inovacím pro zvýšení spolehlivosti biometrických čteček, jako je například přidání bílých LED diod k 3D skenerům tváře, kde se spolehlivost zvýšila v průměru o 40 % u obou systémů. Jiný pohled na zvýšení spolehlivosti 3D čteček obličeje zaujímá pan Leong, který ve svém příspěvku „A Search-and-Validate Method for Face Identification from Single Line Drawings“ poukazuje na skutečnost, že algoritmus vyhledá všechny potenciální osoby (nejrychlejší cesta) a teprve poté z nich určuje shodu s konkrétní osobou. Algoritmus, který vytvořil se svými kolegy, pracuje na principu dvojích šířek, což znamená, že se vezme část obličeje a v případě shody se s největší pravděpodobností jedná o danou osobu, poté se celý obličej porovná, zda je tomu skutečně tak. [45]

U otisku prstů byla disertační práce směřována na zjištění chybovosti biometrických čteček a možností sabotáže těchto zařízení, kde bylo zjištěno, že u optického senzoru poměrně dosti znehodnocuje výsledky měření zašpinění rukou, kde se mezi papilární linie prsových lůžek dostanou nečistoty a identifikace je omezena či úplně znemožněna. Podobným problémem se zabývá i autor Yoon, který v příspěvku poukazuje na možnosti sabotování systémů prostřednictvím vytvoření syntetického otisku prstu aj.. A upravuje algoritmus, aby byl vůči této sabotáži imunní. [46]

Mnoho zahraničních vědců se věnuje převážně vývoji nových systémů, zkoumají jednotlivé neměnné charakteristiky osob a snaží se dle získaných hodnot sestavit nová zařízení. Například švédský student technické fakulty v Lundu Fredrik Leifland pře pěti lety sestrojil zařízení (Quixter), které funguje na principu platebního terminálu, ovšem s tím rozdílem, že místo platební karty lidé využívají biometrických charakteristik a to krevního řečiště ruky. Jelikož se jedná o peněžní tok, tak Fredrik Leifland pojistil celou transakci vložením čtyřmístného kódu. Tento kód má upozornit platící na výši sumy, aby si byli vědomi, kolik platí a zároveň pro případ selhání terminálu. Ovšem bez biometrického skenu k platbě nedojde. Takto využitou biometrii považuji za velký přínos. Tímto vynálezem se nechala inspirovat i firma Fujitsu, kde se toto zařízení zdokonaluje a v blízké době by mělo přijít na trh. Firma Fujitsu se zaměřila i na širší využití zařízení a to i jako přihlašovací prvek do notebooku, či počítače. Autor Jain se zaměřil také na vývoj nového zařízení pro identifikaci osoby. Jako jedinečnou charakteristiku si vybral celou plochu dlaně. Na celé ploše dlaně jsou jasněji viditelné markanty než u malého otisku prstu. Na této metodě postavil celé zařízení a otestoval jej. Z testů vyplynulo, že nové zařízení pracuje s 78% spolehlivostí a je ho tedy možné otestovat v praxi. Stejné téma je rozváděno i disertační práci, kde byl vytvořen duální skener ruky. Identifikace probíhala na základě dvojí shody a to hřbetu ruky a skenu dlaňové části. Také se vycházelo z předpokladů, že celá plocha dlaně se vyznačuje více záchytnými body než pouhý prst. [47]

Biometrické identifikační systémy jsou na celém světě ve stádiu velkého vývoje a je nutno s nimi mít trpělivost a spíše zdokonalovat stávající metody než vymýšlet stále nové. Je nutné rozvíjet či udržet si spolupráci mezi vědci po celém světě a obohacovat se vzájemně svými získanými poznatky.

8 Závěr a doporučení

Disertační práce se zabývá analýzou biometrických identifikačních systémů. Na základě měření je vyhodnocena spolehlivost (hodnoty FAR a FRR) testovaných biometrických identifikačních systémů. Dále se také poukázalo na možnosti použití sabotážních technik a na rizika, která z nich pro provozovatele vyplývají.

V teoretické části jsou rozděleny biometrické identifikační systémy. Jsou zde popsány principy, na kterých jednotlivé systémy fungují a oblasti, kde je možno biometrické identifikační systémy použít. Také jsou v této kapitole objasněny termíny týkající se problematiky biometrických identifikačních systémů.

Další část práce obsahuje praktická měření a testovaní pořízených biometrických identifikačních systémů. Samotná kapitola je rozdělena do čtyř podkapitol, kterými jsou biometrické identifikační systémy pro otisk prstu, biometrické identifikační systémy pro 3D sken obličeje, elektrická sabotáž biometrických identifikačních systémů a inovace stávajících a vývoj nových biometrických identifikačních systémů.

První měřící část je věnování biometrii otisku prstů. Nejprve došlo k otestování 80 subjektů pro standardní identifikaci, to znamená, že testování proběhlo v laboratorních podmínkách a subjekty měly před měřením očištěné ruce. Už tyto výsledky se velmi lišily od hodnot, které udávají výrobci testovaných čtecích systémů. Hodnoty udávané výrobci byly u všech testovaných čteček stejné a to FAR $\leq$ 0,0001 % a FRR $\leq$ 1 %. Výsledky, které vyšly při testování, byly v rozmezí od 2 % do 9,5 % u chybného odmítnutí uživatele (FRR) u chybného přijetí uživatele (FAR) byly hodnoty u kombinovaných biometrických systémů velmi špatné, v průměru – 30 % - 33 %. U systémů pouze pro otisk prstu byly tyto hodnoty průměrně v rozmezí od 7 % do 8,5 %. Takovéto výsledky byly naměřeny u čistých rukou, což v praktickém životě není vždy samozřejmostí. Proto následovalo měření u zašpiněných rukou. Průměrné hodnoty FRR, které vyšly u zašpiněných rukou, byly v rozmezí od 25 % do 33 %, což je oproti 1 %, které udává výrobce, uživatelsky velice nepřijatelné a je nutné zajistit vhodná opatření pro lepší funkčnost těchto biometrických systémů.

V druhé měřící části je pozornost zaměřena na biometrii 3D skenu obličeje. Opět se zde provádí měření spolehlivosti biometrických systémů a jejich vzájemné porovnání, jelikož měření se podrobila 2 čtecí zařízení. Nejprve bylo nutné všechny uživatele zadat do systému. Už v této fázi se vytvořilo první měření. Toto měření se týká doby, za jakou byla uložena do systému předlohová šablona pro následnou identifikaci. V průměru bylo 50 uživatelů načteno do 5 minut, dalších průměrně 22 osob do 10 minut a zbylých v průměru 8 osob se načetlo do

20 minut. Tyto výsledky jsou pro firmy, které si budou chtít tuto vstupní ochranu pořídit, vysoce nepřijatelné. Střední firma o 50 – 80 zaměstnancích by zadávání uživatelů řešila velice dlouho a znamenalo by to, že by vznikl ztrátový čas.

Měření spolehlivosti následovalo hned po zadávání šablon do systému, z výsledků je vidět, že spolehlivost systémů není ve shodě s hodnotami uvedenými výrobci, které se vysoce převýšily. U čtecího zařízení Multibio700 bylo 53,4 % osob identifikováno do 1 minuty, dalších 26,41 % bylo identifikováno do 5 minut a 20,19 bylo neidentifikováno. Hodnota chybné identifikace (záměny osob) byla 4,88 %. U druhého testovaného zařízení byly získané hodnoty obdobné a to identifikace do 1 minuty – 57,63 % uživatelů, do 5 minut – 25,68 % uživatelů a neidentifikováno bylo 16,69 % uživatelů. Z toho chybných identifikací bylo o něco méně než u předchozího zařízení, a to 4 % uživatelů.

Jako u měření otisku prstů, tak i zde se za provozu setkáváme s ušpiněnými obličeji, a proto vniklo další měření. Toto měření prokázalo, že lehké zašpinění prachem, olejem zhoršilo identifikaci jen o pár procent, ovšem pokapání obličeje malířskou barvou či znečištění černým uhlím ovlivnilo vpuštění do objektu ve vysoké míře, kde hodnoty přijetí uživatele klesly až na 38 %.

Krom chybného odmítnutí uživatele se také testovalo i chybné přijetí uživatele. Tato situace většinou nastane, když se neoprávněný uživatel snaží dostat do systému, kam nemá přístup, jinými slovy se jedná o sabotáž biometrických systémů pro 3D sken obličeje. Tento pokus o sabotování těchto systémů proběhl úspěšně. S pouhými maskérskými pomůckami bylo v průměru přijato 50 osob a prostřednictvím nasvícení tváře průměrně 22 osob. Tyto způsoby nejsou nikterak složité na provedení a úspěšnost průměrně 72 pokusů ze 150 celkových je více než uspokojivá.

Dále se čtečky testovaly z pohledu elektrických sabotážních technik. Tato kapitola se vztahuje k biometrickým identifikačním systémům a systémům pro vstup osob obecně. V této kapitole jsou probrány veškeré možné sabotáže z pohledu útočníka, ve vztahu k čtecím zařízením přístupových systémů, a to z hlediska zásahu do kabeláže. U výsledného hodnocení se použila bodovací metoda v multikriteriální analýze variant a přiřadilo se bodové ohodnocení jednotlivým sabotážním technikám. Z výsledné sumy váhových koeficientů je patrné, že největším rizikem pro zapojení čtecích zařízeních je zapojení čtecího zařízení jako systému s přímým ovládáním a systému využívajícího PZTS za použití jednoduché smyčky. Oproti tomu použití systému s centrální logikou se jeví jako nejbezpečnější varianta. V praxi je proto důležité, aby se u čtecích zařízení opustilo od varianty využívání systémů zapojení pomocí přímého ovládání a využití PZTS a přešlo se pouze na systémy s centrální logikou.

Poslední kapitola se týká inovací stávajících systémů a návrhů pro nové biometrické identifikační systémy. Předešlá měření poukázala na chyby stávajících čtecích zařízení, proto bylo možné provést jednotlivé inovační kroky. Jednou z hlavních inovací bylo vytvoření externího zařízení pro tvorbu předlohových šablon a jejich následného vložení do systému. Toto zařízení zkrátí získání předlohových šablon do 1 minuty. Do budoucna by mělo být zařízení plně kompatibilní se všemi biometrickými identifikačními systémy pro 3D sken obličeje. Další inovací je přidělání bílého LED přísvitu k 3D čtečkám obličeje. Tento LED přísvit zvýrazní obličejové kontury a rysy, identifikace se tak nejen zrychlí, ale i zkvalitní. S tímto LED přísvitem bylo přijato v průměru o 36 % více uživatelů než s integrovaným Infra přísvitem.

V okruhu vývoje nových systémů se věnovala pozornost části těla, na které je mnoho identifikačních bodů - ruka. Je navrhnut systém, který může fungovat samostatně jako sken ruky, či duálně v kombinaci se skenem dlaňové části. Celý systém je sestaven ze světelného zdroje, fotoaparátu, skleněné podložky a popřípadě ze skeneru pro sken dlaně. Zařízení neobsahuje mezi-prstové zarážky, které omezují pohyb ruky, ale zároveň snižují počet identifikačních bodů. Identifikačními body jsou délka části prstů, šířka prstů, šířka kloubů, oblouk dlaně, postavení prstů aj. Další vývoj se zaměřil na automobilový průmysl, kde vnikl návrh pro dohled nad služebními vozidly, samozřejmě tento způsob ochrany je možný i u osobního vozu, ale snižuje jeho flexibilitu. Jde o seskupení biometrických systémů, které slouží k ochraně před půjčováním si služebních vozů. První krok je otisk prstu na klice automobilu. Pokud je uživatel zaveden v databázi, je vpuštěn do vozidla, kde dojde k následnému sejmutí obličejových rysů prostřednictvím 3D skenu obličeje. Pokud je uživatel oprávněn užít vozidlo, je nastartován motor a vše je upraveno na míry řidiče, které jsou do systému vloženy s uložením předlohových šablon. Dalším návrhem je zabudovaný sken nehtového lůžka v zárubních dveří v úrovni zámku k dvojité kontrole vstupu. Nejprve dojde k otočení klíčku, kdy následuje sken lůžka a následně při shodě s databází je možno proces otevření dveří dokončit. Další návrhy pro nová zařízení týkající se okrajově biometrie jsou uvedeny v přílohách této dizertační práce.

Ze získaných hodnot lze uživatelům pouze doporučit, aby si před použitím jednotlivých biometrických identifikačních systémů rozmysleli, zda míra spolehlivosti těchto systémů je dostačující pro ochranu prostor. Bylo by vhodné zvážit i kombinaci biometrických systémů s dalšími možnostmi ochrany vstupu, jako jsou PINY, ID karty, hesla, popř. možnost propojení se zabezpečovacími systémy.

Tyto inovace a nové návrhy systémů budou použity v komerčních budovách. Zejména návrh (oboustranný sken ruky) bude následně po jeho miniaturizaci využit v elektrárnách. Je dohodnutá spolupráce s holandskými podniky a navazuje se komunikace a domlouvají podmínky pro uplatnění (otestování v praxi) tohoto zařízení v českých energetických podnicích. Také biometrická autorizace vozidla je již v jednání s českými automobilkami a koncerny. O další inovace v oblasti biometrie projevily zájem firmy zabývající se touto problematikou, s kterými se díky tomu navázala dlouhodobá spolupráce. Spolupráce ohledně biometrie byla navázána i s hlavní univerzitou v Zürychu (Švýcarsko). Nejvíce si cením navázání spolupráce s Ministerstvem vnitra, kde také probíhají rozsáhlé výzkumy týkající se této problematiky. Velký přínos budou mít tyto inovace nejen v komerční oblasti, ale také v osobní sféře (použití u domů, bytů, rekreačních středisek aj).

9 Seznam použité literatury

[1] BENEŠ, R. „*Autentizační metody založené na biometrických infor macích*“. Access server [online]. 18. 11. 2010, [cit. 2013-06-18]. Dostupný z WWW:

<http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>.

[2]GOLDSTEIN, A.J.; HARMOND L. D.; LESK, A. B.: *„Identification of Human Faces“* IEEE, May 1971, Vol. 59, No. 5, s. 748-760.

[3] MALTONI, D.; a kol.: *„Handbook of Fingerprint Recognition.“* Druhé vydání. Londýn: Springer, 2009. 483 s. ISBN 978-1-84882-253-5.

[4] RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kolektiv. *„Biometrie a identita člověka ve forenzních a komerčních aplikacích.“* Praha, Nakladatelství Grada, 2012

[5] NATTA, N.; McCLURE, R. „*Biometrie Solutions to Person Identification.“* Kalifornia, White Paper of Digital Persona, 1998.

[6] ASHBOURN, J. *„Biometrics Advanced Identity Verification.“* London, Springer – Verlag, 2000, ISBN 1-85233-243-3.

[7] ŠMIRAUS, M. B.P. *„Vývoj a současné trendy počítačově podporovaných technologií identifikace.“* Zlín, 2008.

[8] BRADLEY, J.; BRISLAWN,C.M. *„Wavelet scalar quantization gray-scale fingerprint compression specification.“* [online], [cit. 2011-10-22]. Dostupný z WWW:

<http://www.ccs.lanl.gov/ccs3/index.shtml>.

[9] CRAVOTTA, N. *„Looping under the surfaře of fingerprint scanners.“* EDN[online]. 05.06.2000, [cit. 2013-01-08]. Dostupný z WWW:

<http://www.ednmag.com>.

[10] HILL, R. *„Retina Identification in Biometrics: Personál Identification in Networked Society.“* Dordrecht, Kluwer academic Publisher, 1999.

[11] DAUGMAN, J. *„Statistical richness of visual phase information: Update on recognizing persóna by thein iris patterns.“* Washington, Computer Vision, 2001.

[12] Oční optik, [online], [cit. 2013-06-18]. Dostupný z WWW:

http://www.ocnioptik.eu/content/images/design/2011/oko_foto_%201.jpg

[13] Old jujitsu, [online], [cit. 2013-06-18]. Dostupný z WWW:

<http://old.jujitsu.cz/Listopadky/2004/Clanky/Img/03_Irismuster.jpg>

[14] JAIN, A.; BOLLE, R.; PANKANTI, S. *„Biometrics. Personal Identification in Networked Society.“* Norwell, Massachusetts, USA, Kluwer Academic Publisher, 1999,

ISBN 0-7923-8345-1.

[15] JANURA, M a kol. *„Kinematická analýza chůze u vybraných skupin pacientů. Laboratoř lidské motoriky.“* FTK UK Olomouc, 2003.

[16] PORADA, V. *Identifikace osob podle funkčních a dynamických znaků*. Praha: MV ČR, 2007.

[17] STRAUS, J.; PORADA, V. *„Forensic biomechanical application in criminalistic.“* In Forensic Science International. 2007, ISSN 0379-0738.

[18] KARAS,V. *„Biomechanika pohybového systému člověka.“* Praha: UK 1978.

[19] STRAUS, J.; JONÁK, J. *„Je možné identifikovat osobu podle pohybového projevu lokomoce?“* Ve: Sborník vědeckovýzkumných výstupů z realizace Výzkumného záměru PA ČR, Praha, 2007, ISBN 80-7251-229-3.

[20] ChAO, Y.*„Studies on Several Methods for Face Detection"*, Master dissertation, Tsinghua University, Beijing, China, 1999.

[21] ZHANG, D. A.*„Automated Biometrics. Technologies and Systems",* Kluwer Academic Publishers, Boston, 2000, ISBN 0-7923-7856-3.

[22] LIXIN F., KAH KAY SUNG „*A Combined Feature-texture Similarity Measure for Face Alignment Under Varying Pose"*, School of Computing National University of Singapore, 2002.

[23] BIČOVSKÝ,R. „*Tajemství písma*.“ Praha, Panorama, 1992.

[24] ZHANG, D. *„Automated biometrics Technologies and Systéme.“* Kluwer Academic Publishiers, 2000, ISBN 0-7923-7856-3.

[25] BLEHA, S.; SLIVINSKY, C.; HUSSIEN, B. *„Computer-Access Securyty Systéme Usány Keystroke Dynamics.“* In IEEE Transactiions on Pattern Analysis and Machina Inteligence. 1990.

[26] GARCIA, JOHN, D. *„Personál Identificational Aparatur.“* U.S. Patent Numer 4621334, november 1986.

[27] Variant, [online], [cit. 2013-06-18]. Dostupný z WWW:

<http://www.variant.cz/>

[28] Docházka,[online], [cit. 2013-06-18]. Dostupný z WWW:

<http://dochazka.vyrobce.cz/newweb/finger.html>

[29] Eurosat, [online], [cit. 2013-06-18]. Dostupný z WWW:

<http://www.eurosat.cz/>

[30] ZKSoftware, [online], [cit. 2013-06-18]. Dostupný z WWW:

<http://www.zktechnology.com/ProductDetail.aspx?cat=Face+Readers&series=Face+and+Fingerprint+T%26A+Readers&product=Multibio+700>

[31] Comfis, [online], [cit. 2013-06-18]. Dostupný z WWW:

<http://www.comfis.cz/uvod/shop/terminaly>

[32] SVOZIL, L. *„Aspekty biometrické identifikace osob s využitím rozpoznání tváře“,* bakalářská práce, Univerzita Tomáše Bati ve Zlíně. 2009.

[33] HEŘMAN, J., a kol.: „*Elektrotechnické a telekomunikační instalace*“. Praha: Verlag

Dashöfer, 2008. ISSN 1803-0475.

[34] KŘEČEK, S., a spol.,: „*Příručka zabezpečovací techniky*“. Blatná: Circetus,. 313s. 2006. ISBN 80-902938-2-4.

[35] UHLÁŘ, J.,: „*Technická ochrana objektů, II.díl, Elektrické zabezpečovací systémy II*“. Praha: PA ČR. 229s. 2005 ISBN 80-7251-189-0.

[36] STAFF, H., HONEY, G.: *Electronic Security Systems Pocket Book*. Elsevier Science. 226p. 1999 ISBN-13: 9780750639910.

[37] WALKER, P.: Electronic Security Systems: *Reducing False Alarms*. Elsevier Science,. 294p. 1999 ISBN-13: 9780750635431.

[38] МАГАУЕНОВ, Р.: *Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь. Горячая Линия - Телеком*. 98 стр. 2007.

ISBN: 5-93517-333-6.

[39] CAPEL, V.: *Security Systems & Intruder Alarms*. Elsevier Science. 301p. 1999

ISBN-13: 9780750642361.

[40] PETRUZZELLIS, T.: *Alarm Sensor and Security*. McGraw-Hill Professional Publishing, 1993. 256p. ISBN-13: 9780830643141.

[41] CUMMING, N.: Security: *A Guide to Security System Design and Equipment Selection and Installation*. Elsevier Science. 338p. 1994 ISBN-13: 9780750642361.

[42] NÍDLOVÁ, V.; HART, J.; HRUŠKA, M. *Biometric identification on the basis of facial features and modifications thereof* . Advanced Materials Research, roč. 905, č. 0, s. 669-672. 2014 ISSN: 1022-6680.

[43] NÍDLOVÁ, V.; HART, J.; VACULÍK, P. „*Vývoj biometrického identifikačního systému*“.[online], 14. 08. 2013, [cit. 2013-06-18]. Dostupný z WWW:

<http://www.tzb-info.cz/facility-management/9742-vyvoj-biometrickeho-identifikacniho-zarizeni>, ISSN 1801-4399.

[44] SVATOŠOVÁ, L. a PRÁŠILOVÁ, M.: „*Statistické metody v příkladech*“. Nakladatelství: Česká zemědelská univerzita v Praze, 2012. ISBN 9788021316737.

[45] Leong, M.C.; Lee, Y.T.; Fang, F. *„A Search-and-Validate Method for Face Identification from Single Line Drawings.“* V IEEE Transactions on pattern analysis and machine intelligence. 2576-2591 s. 2013 ISSN: 0162-8828

[46] Yoon, S.; Feng, J.J.; Jain, A.K. *„Altered Fingerprints: Analysis and Detection.“* V IEEE Transactions on pattern analysis and machine intelligence. 451-464 s. 2012 ISSN: 0162-8828

[47] Jain, A.K. ; Feng, J.J. *„Latent Palmprint Matching.“* V IEEE Transactions on pattern analysis and machine intelligence. 1032-1047 s. 2009 ISSN: 0162-8828

10 Publikační činnost

10.1 Článek recenzovaný

NEJEDLÁ, V. – NÍDLOVÁ, V. – VACULÍK, P. – HART, J. – VOTRUBA, Z. Nový systém nestacionární perimetrické ochrany objektů. *TZB-info,* 2013, roč. 13, č. 24, s. 1-4. ISSN: 1801-4399.

NÍDLOVÁ, V. – HART, J. – VACULÍK, P. Vývoj biometrického identifikačního zařízení. *TZB-info,* 2013, roč. 13, č. 15, s. 1-4. ISSN: 1801-4399.

HART, J. – NÍDLOVÁ, V. – NEJEDLÁ, V. Vývoj inovací a nových prvků poplachových zabezpečovacích a tísňových systémů na ČZU v Praze. *TZB-info,* 2013, roč. 13, č. 34, s. 1-5. ISSN: 1801-4399.

NÍDLOVÁ, V. – HART, J. Testování pancéřových krků určených k ochraně datových rozvodů. *Elektro,* 2014, roč. 69, č. 1, s. 10-11. ISSN: 1210-0889.

10.2 Článek scopus

NÍDLOVÁ, V. – HART, J. – HRUŠKA, M. Biometric identification on the basis of facial features and modifications thereof . *Advanced Materials Research,* 2014, roč. 905, č. 0, s. 669-672. ISSN: 1022-6680.

HART, J. – NÍDLOVÁ, V. – PŘIKRYL, M. Reliability of detection of sources of infrared radiation in security alarm and distress signal systems. *Agronomy Research,* 2014, roč. 12, č. 3, s. 949-954. ISSN: 1406-894X.

NÍDLOVÁ, V. – HART, J. The impact of light conditions on identifying facial features . *Agronomy Research,* 2014, roč. 12, č. 3, s. 889-894. ISSN: 1406-894X.

HART, J. – NÍDLOVÁ, V. The risks of data transmissions in intrusion and hold-up alarm systems and solutions thereto. *Advanced Materials Research,* 2014, roč. 905, č. 0, s. 570-574. ISSN: 1022-6680.

10.3 Kapitola resp. kapitoly v odborné knize

VOTRUBA, Z. – HART, J. – NÍDLOVÁ, V. – NEJEDLÁ, V. *Elektrotechnické a telekomunikační instalace* . Praha: Verlag Dashofer, 2012, 1300s. ISBN 80-86897-06-0. Rozvody bezpečnostních elektrických systémů kap. 11/3.3 , s. 1-17.

NÍDLOVÁ, V. *Elektrotechnické a telekomunikační instalace* . Praha: Verlag Dashofer, 2012, 1300s. ISBN 80-86897-06-0. Rozvody bezpečnostních elektrických systémů kap. 11/3.4.2, s. 1-6.

10.4 Článek ve sborníku z akce (publikovaná přednáška – proceeding)

HART, J. – NÍDLOVÁ, V. ANALYSIS OF SECURITY RISKS OF BUILDING USING I&HAS SYSTEM. In *INTERNATIONAL MASARYK CONFERENCE FOR PH.D. STUDENTS AND YOUNG RESEARCHERS 2012 10.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 3324-3329.

NÍDLOVÁ, V. – VACULÍK, P. – HART, J. – NEJEDLÁ, V. BIOMETRIC IDENTIFICATION SYSTEMS . In *Technológia Europea 2012 11.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 59-66.

HART, J. – VACULÍK, P. – NÍDLOVÁ, V. DEVELOPMENT OF NEW TECHNOLOGIES TO IMPROVE QUALITY AND SECURITY IN I&HAS SYSTEMS. In *Technológia Europea 2012 11.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 49-58.

NÍDLOVÁ, V. – HART, J. LINKING SYSTEMS PZTS AND BIOMETRIC DETECTORS DEPENDING ON THEIR SAFETY AND RELIABILITY . In *INTERNATIONAL MASARYK CONFERENCE FOR PH.D. STUDENTS AND YOUNG RESEARCHERS 2012 10.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 2849-2853.

HART, J. – NÍDLOVÁ, V. METHODS OF SABOTAGE TRANSMISSION ALARM INFORMATION IN SYSTEMS I&HAS. In *INTERNATIONAL MASARYK CONFERENCE FOR PH.D. STUDENTS AND YOUNG RESEARCHERS 2012 10.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 2854-2859.

NÍDLOVÁ, V. – HART, J. NEW SECURITY ELEMENTS IN BIOMETRIC SYSTEMS AND SYSTEMS I&HAS. In *INTERNATIONAL MASARYK CONFERENCE FOR PH.D. STUDENTS AND YOUNG RESEARCHERS 2012 10.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 3330-3336.

HART, J. – NÍDLOVÁ, V. ODOLNOST ELEKTRICKÝC ZABEZPEČOVACÍCH SYSTÉMŮ PROTI SOFISTIKOVANÝM ZPŮSOBŮM NAPADENÍ. In *XIV. MEDZINÁRODNÁ VEDECKÁ KONFERENCIA MLADÝCH 2012 11.06.2012, Zvolen.* Zvolen: Technická univerzita vo Zvolene Fakulta environmentálnej a výrobnej techniky, 2012. s. 87-92.

NÍDLOVÁ, V. – HART, J. PROPOJENÍ SYSTÉMŮ PZTS A BIOMETRICKÝCH DETEKTORŮ V ZÁVISLOSTI NA JEJICH BEZPEČNOSTI A SPOLEHLIVOSTI. In *XIV. MEDZINÁRODNÁ VEDECKÁ KONFERENCIA MLADÝCH 2012 11.06.2012, Zvolen.* Zvolen: Technická univerzita vo Zvolene Fakulta environmentálnej a výrobnej techniky, 2012. s. 235-240.

VACULÍK, P. – HART, J. – NÍDLOVÁ, V. – SUCHÝ, O. RECYCLING TECHNOLOGY OF SELECTED CONSTRUCTION WASTE. In *Technológia Europea 2012 11.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 43-48.

NEJEDLÁ, V. – VACULÍK, P. – NÍDLOVÁ, V. – HART, J. SYSTEMS OF PERIMETRIC PROTECTION. In *Technológia Europea 2012 11.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 67-70.

VACULÍK, P. – HART, J. – NÍDLOVÁ, V. TESTING ARMOR NECK TO PROTECT THE LINE SYSTEMS AT I&HAS. In *INTERNATIONAL MASARYK CONFERENCE FOR PH.D. STUDENTS AND YOUNG RESEARCHERS 2012 10.12.2012, Hradec Králové.* Hradec Králové: © MAGNANIMITAS, Hradec Králové, Česká republika, 2012, 2012. s. 2948-2954.

10.5 Výsledky s právní ochranou (užitný vzor)

HART, J. – NÍDLOVÁ, V. <i>Aplikátor inhibitorů na střešní krytinu. Úřad průmyslového vlastnictví (www.upv.cz). 24388. 08.10.2012.

HART, J. – NÍDLOVÁ, V. – ANDRT, M. – PŘIKRYL, M. <i>Aplikátor viskózních tekutin s výměnnou hlavicí. Úřad průmyslového vlastnictví (www.upv.cz). 25843. 12.09.2013.

NÍDLOVÁ, V. – HART, J. <i>Biometrický skener dlaně. Úřad průmyslového vlastnictví (www.upv.cz). 24107. 16.07.2012.

HART, J. – NÍDLOVÁ, V. <i>Detektor na ochranu tištěných dokumentů. Úřad průmyslového vlastnictví (www.upv.cz). 24281. 06.09.2012.

HART, J. – NÍDLOVÁ, V. <i>Distanční plastový sloupek s nevratnou pojistkou. Úřad průmyslového vlastnictví (www.upv.cz). 24020. 25.06.2012.

NÍDLOVÁ, V. – HART, J. <i>Hydraulický parkovací sloupek. Úřad průmyslového vlastnictví (www.upv.cz). 24021. 25.06.2012.

HART, J. – NÍDLOVÁ, V. <i>Infradetektor okenních výplní. Úřad průmyslového vlastnictví (www.upv.cz). 24427. 15.10.2012.

HART, J. – NÍDLOVÁ, V. <i>Infrapřevodník drátových systémů. Úřad průmyslového vlastnictví (www.upv.cz). 24383. 08.10.2012.

NÍDLOVÁ, V. – HART, J. <i>Integrovaný laserový detektor okna. Úřad průmyslového vlastnictví (www.upv.cz). 26094. 14.11.2013.

HART, J. – NÍDLOVÁ, V. <i>Integrovaný radiový snímač. Úřad průmyslového vlastnictví (www.upv.cz). 24319. 17.09.2012.

HART, J. – NÍDLOVÁ, V. <i>Klávesnicový modul. Úřad průmyslového vlastnictví (www.upv.cz). 24323. 17.09.2012.

NÍDLOVÁ, V. – HART, J. <i>Systém biometrické autorizace pro využití služebního vozidla. Úřad průmyslového vlastnictví (www.upv.cz). 24121. 19.07.2012.

HART, J. – NÍDLOVÁ, V. <i>Systém pro upínání kabelů do detektoru. Úřad průmyslového vlastnictví (www.upv.cz). 23960. 11.06.2012.

NÍDLOVÁ, V. – HART, J. <i>Zámkový systém s biometrickým scanem nehtového lůžka. Úřad průmyslového vlastnictví (www.upv.cz). 23925. 04.06.2012.

HART, J. – NÍDLOVÁ, V. <i>Zvukový okenní detektor. Úřad průmyslového vlastnictví (www.upv.cz). 24382. 08.10.2012.

10.6 Ostatní výsledky, které nelze zařadit do žádného z výše uvedených druhů výsledku

VOTRUBA, Z. – HART, J. – KOTEK, T. – NÍDLOVÁ, V. – NEJEDLÁ, V. Podtyp: Článek v nerecenzovaném časopise (mimo kategorie RIV); Bezpečnostní systémy v rámci projektu inteligentních budov (technické řešení a možnosti). 2011, Security magazín
ISSN 1210-8723.

HART, J. – NÍDLOVÁ, V. Podtyp: Příspěvek ve sborníku (mimo kategorie RIV); OCHRANA DATOVÝCH ROZVODŮ POMOCÍ PANCÉŘOVÝCH KRKŮ. 2013, Místo vydání Nitra
Název sborníku XV. Medzinárodná vedecká konferencia mladých 2013
Místo konání Račkova dolina.

NÍDLOVÁ, V. – HART, J. Podtyp: Příspěvek ve sborníku (mimo kategorie RIV); VÝVOJ NOVÝCH ZABEZPEČOVACÍCH A BIOMETRICKÝCH PRVKŮ NA ČZU V PRAZE. 2013, Název sborníku XV. Medzinárodná vedecká konferencia mladých 2013
Místo konání Račkova dolina.

11 Seznam obrázků

12 Seznam tabulek

13 Seznam vzorců

14 Seznam zkratek

ATZ – Advanced Technology Zoning

CCD – Charged Couplet Device

EOL – End Of Line

FAR – False Acceptance Rate

FRR – False Rejection Rate

FTIR – Frustrrated Total Internal Reflection

ID – Identification

LED – Light Emitting Diode

N.C. – Normaly Close

NEIA – Number of Enrolle Identification

NFA – Number of False Rejection

NFR - Number of False Rejection

NIIA - Number of Enrolle Identification

N.O. – Normaly Open

PIN – Personal Identification Number

PZTS – Požární Zabezpečovací a Tísňové Systémy

USB – Universal Serial Bus

15 Seznam příloh

Příloha 1

Integrovaný radiový snímač

Oblast techniky

Technické řešení se týká konstrukce integrovaného radiového snímače. Tato konstrukce umožňuje rychlejší vstupu do prostor s kontrolovaným přístupem.

Dosavadní stav techniky

V současnosti se pro přístup do prostor s kontrolovaným přístupem využívá přístupových karet, přístupových kódů a radiových přístupových systémů, které využívají pro identifikaci radiový čip, který má oprávněná osoba u sebe a který nesmí ztratit. Tento systém identifikace obtěžuje identifikovanou osobu a prodlužuje přístup do kontrolovaných prostor.

Podstata technického řešení

Technické řešení spočívá ve vytvoření integrovaného radiového snímače, který slouží pro urychlení kontroly a identifikace osob, při vstupu do prostor s kontrolovaným přístupem.

Integrovaný radiový snímač se skládá z pasivního radiového členu integrovaného do podpatku boty, aktivního čtecího zařízení umístěného do podlahy a z identifikační jednotky. Ve chvíli kdy se radiový snímač dostane do pole čtecího zařízení, tak se jeho identifikační kód vyšle do identifikační jednotky. Ta vyhodnotí, jestli jde o oprávněný přístup a popřípadě otevře vstupní dveře.

Přehled obrázků na výkresech

Na obr.1 je znázorněn pohled na systém používající integrovaný radiový snímač a na obr.2 je znázorněn částečný boční řez botou s integrovaným radiovým snímačem.

Příklady provedení technického řešení

Integrovaný radiový snímač se skládá z pasivního radiového členu 1 integrovaného do podpatku 2 boty 3, který je znázorněn částečným bočním řezem podpatku označeného řezovou linií 4, aktivního čtecího zařízení 5 umístěného do podlahy a z identifikační jednotky 11, která je ke čtecímu zařízení 5 připojena kabeláží 12 nebo bezdrátově.

Když se někdo v přístupovém směru 7 pokusí projít vstupem 6, tak je nucen projít přes čtecí zařízení 5. Ve chvíli kdy se pasivní radiový člen 1 dostane do pole čtecího zařízení 5, tak se jeho identifikační kód vyšle do identifikační jednotky 11. Ta vyhodnotí, jestli jde o

oprávněný přístup a když vyhodnotí shodu s databází zaměstnanců, tak otevře vstupní dveře 8.

Tento systém přístupu do kontrolovaného prostoru může být jištěn fyzickou ostrahou 9. Té se na monitoru 10 objeví údaje a popřípadě i fotografie osoby žádající o přístup do kontrolovaného prostoru. Když se pokusí projít někdo bez pasivního radiového členu 1 nebo s pasivním radiovým členem 1, který nepovoluje přístup do kontrolovaného prostoru, tak je informována fyzická ostraha 9 a dveře 8 se neotevřou.

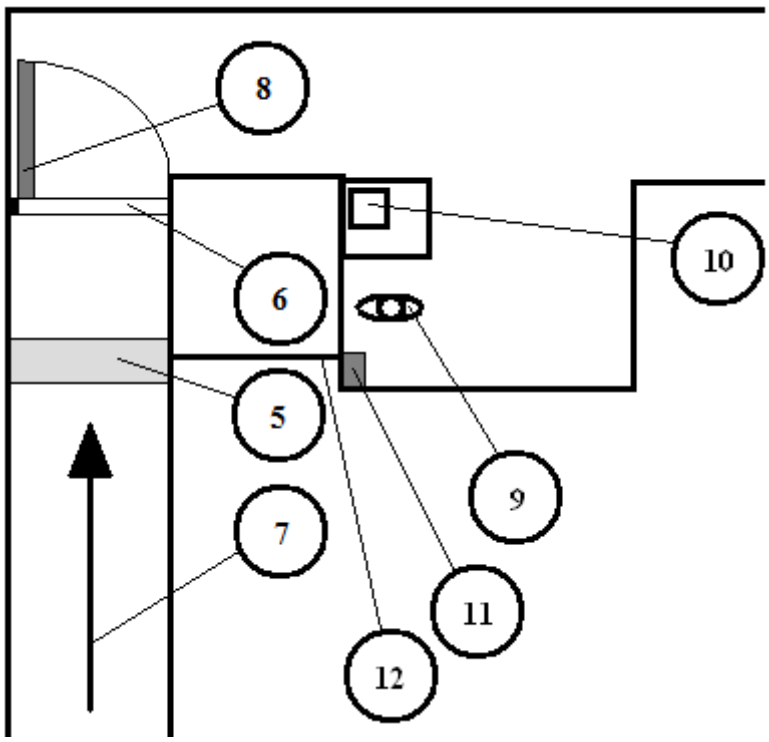
Průmyslová využitelnost

Integrovaný radiový snímač nalezne uplatnění u velkých firem, které mají určité prostory s kontrolovaným přístupem, u kterých zvýší komfort pracujících a rychlost přístupu do kontrolovaného prostoru. Pro svou vysokou efektivitu při odbavování zaměstnanců a jednoduchosti provedení je vhodný pro sériovou výrobu.

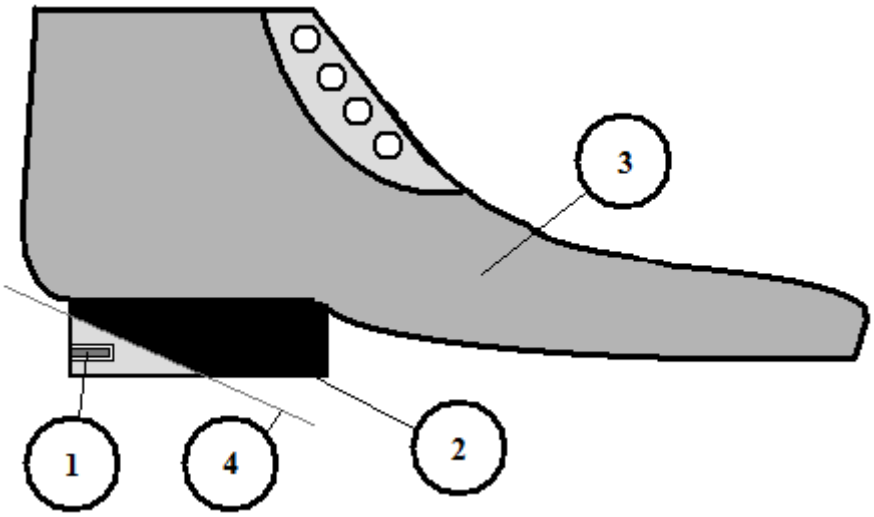
Nároky na ochranu

1. Integrovaný radiový snímač **vyznačující se tím**, že se skládá z pasivního radiového členu (1) integrovaného do podpatku (2) boty (3), aktivního čtecího zařízení (5) umístěného do podlahy umístěného před vstupem a z identifikační jednotky (11), která je ke čtecímu zařízení (5) připojena kabeláží (12) nebo bezdrátově.

2. Integrovaný radiový snímač **vyznačující se tím**, že je vybaven monitorem (10), který je propojen s vyhodnocovací jednotkou (11).



Obr.1



Obr.2

Příloha 2

Infrapřevodník drátových systémů

Oblast techniky

Technické řešení se týká konstrukce infrapřevodníku drátových systémů. Tato konstrukce umožňuje bezdrátové propojení přes prostory s přímou viditelností.

Dosavadní stav techniky

V současnosti se pro bezdrátový přenos v elektrických zabezpečovacích systémech využívají přenosy pomocí bezdrátových pásem na frekvencích 433 a 868MHz. Tyto přenosy jsou relativně náchylné k externímu rušení a pro nahrazení drátu nejsou příliš vhodné z důvodu jejich ceny a bezpečnosti přenosu.

Podstata technického řešení

Technické řešení spočívá ve vytvoření infrapřevodníku drátových systémů, který slouží pro převod drátové komunikaci v elektrických zabezpečovacích systémech na infrapřenos.

Infrapřevodník drátových systémů se skládá z infrajednotky s integrovaným infravysílačem a infrapřijímačem, převodní jednotky a propojovací kabeláže.

Do převodní jednotky infrapřevodníku je zapojena smyčka nebo sběrnice elektrických zabezpečovacích systémů. Tam je převedena na infrakomunikaci, která je odeslána pomocí propojovací kabeláže do infrajednotky. Ta vysílá infrapaprsek do sesterské jednotky, která tuto komunikaci dekóduje a předá do své převodní jednotky.

Přehled obrázků na výkresech

Na obr.1 je znázorněn pohled na komunikaci mezi sesterskými infrapřevodníky drátových systémů a na obr.2 je znázorněn detail infrapřevodníku.

Příklady provedení technického řešení

Infrapřevodník 1 drátových systémů se skládá z infrajednotky 6 s integrovaným infravysílačem a infrapřijímačem, převodní jednotky 7 a propojovací kabeláže 9, která propojuje infrajednotku 6 s převodní jednotkou 7.

Do převodní jednotky 7 infrapřevodníku 1 je zapojena smyčka nebo sběrnice 8 elektrických zabezpečovacích systémů. Tam je převedena na infrakomunikaci, která je

odeslána pomocí propojovací kabeláže 9 do infrajednotky 6. Ta vysílá infrapaprsek 2 do sesterské jednotky, která tuto komunikaci dekóduje a předá do své převodní jednotky 7.

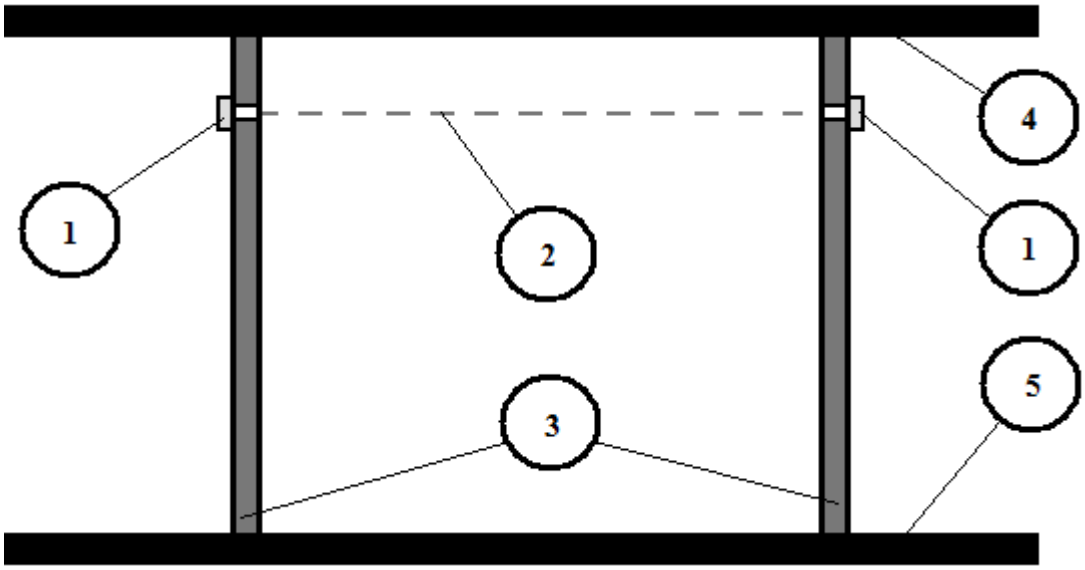
Infrapřevodník 1 drátových systémů se montuje pod strop 4 tak, aby měl přímou viditelnost na svůj sesterský převodník. Infrapřevodník 1 drátových systémů se provrtává skrz zdi objektu 3 tak, že je infrapřevodník 1 z vnější části místnosti, kterým je tento bezdrátový přenos veden. Je důležité aby byl tento systém co nejdál od podlahy 5, aby nedocházelo k přerušení paprsku průchodem.

Průmyslová využitelnost

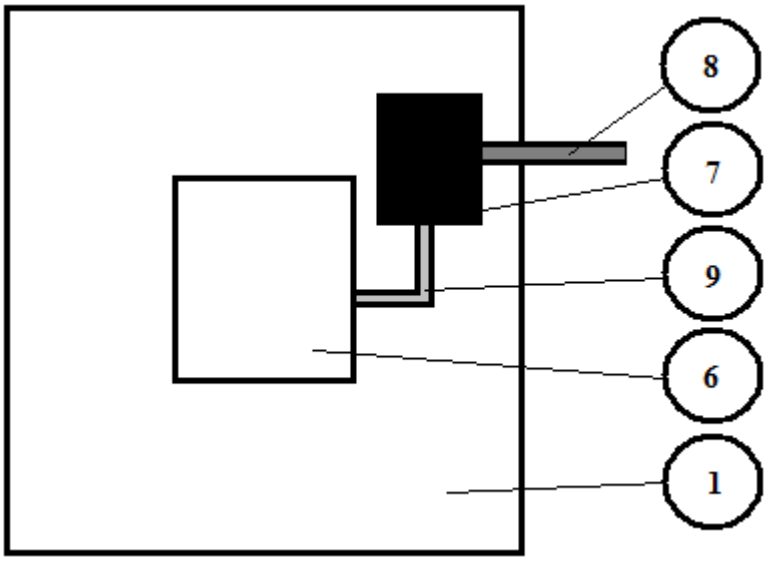
Infrapřevodník drátových systémů nalezne uplatnění v elektrických zabezpečovacích systémech, kde zvýší variabilitu bezdrátových přenosových médií. Pro svou vysokou efektivitu při nahrazování drátové komunikace za bezdrátovou a jednoduchosti provedení je vhodný pro sériovou výrobu.

Nároky na ochranu

1. Infrapřevodník (1) drátových systémů **vyznačující se tím**, že se skládá z infrajednotky (6) s integrovaným infravysílačem a infrapřijímačem, převodní jednotky (7) a propojovací kabeláže (9), která propojuje infrajednotku (6) s převodní jednotkou (7), přičemž je do převodní jednotky (7) infrapřevodníku (1) zapojena smyčka nebo sběrnice (8) elektrických zabezpečovacích systémů.



Obr.1



Obr.2

Příloha 3

Systém pro upínání kabelů do detektoru

Oblast techniky

Technické řešení se týká konstrukce systému pro upnutí kabelů do detektoru s využitím samoúchytného systému. Tento systém umožňuje rychlé uchycení vodičů do detektoru a tím snižuje náročnost při instalaci zabezpečovacích systémů.

Dosavadní stav techniky

V současnosti se využívá šroubovacích svorkovnic umístěných na tištěném spoji a nebo na plastovém krytu detektoru. Nynější systém, ačkoli je funkční, je dost nepraktický, protože se doba instalace detektoru díky šroubování několikrát prodlouží. Tím vznikají zbytečné časové prodlevy, které se podepíší i při konečném vyúčtování.

Podstata technického řešení

Technické řešení spočívá ve vylepšení stávajícího systému uchycení vodičů, v elektrických zabezpečovacích systémech, do detektorů, klávesnic, komunikátorů apod. Systém pro upínání kabelů do detektoru se skládá ze samoupínací svorkovnice se samozářeznými čelistmi, odřezávacího břitu a plastového krytu.

Samoupínací svorkovnice je připevněna k tištěnému spoji nebo je umístěna do krytu detektoru. Díky systému pro upínání kabelů pak není třeba vodiče složitě upevňovat do šroubovací svorkovnice, ale stačí je jen vložit do samozářezných čelistí na samoupínací svorkovnici a pomocí plastového krytu zatlačit vodiče do otvoru. Při zatlačování vodičů do samozářezných čelistí se přebytečná délka vodičů odřízne o odřezávací břit.

Přehled obrázků na výkresech

Na obr.1 je znázorněna samoupínací svorkovnice, na obr.2 je znázorněn boční průřez systému pro upínání kabelů do detektoru a na obr.3 je znázorněn boční průřez systému pro upínání kabelů do detektoru s plastovým krytem.

Příklady provedení technického řešení

Systém pro upínání kabelů do detektoru se skládá ze samoupínací svorkovnice 1 se samozářeznými čelistmy 2, z odřezávacího břitu 3 a z plastového krytu 4, který je vybaven zatlačovacím klínem 8.

Uchycení vodičů 6 probíhá tak, že se umístí do prostoru samozářezných čelistí 2 tak, aby procházely napříč samoupínací svorkovnicí 1 a volně ležely na odřezávacím břitu 3. Poté nasadíme plastový kryt 4 na samoupínací svorkovnici 1 a ve směru nasazování 5 jej přitlačíme. Tím dojde v bodě dotyku 7, odřezávacího břitu 3 a plastového krytu 4, k odříznutí vodičů 6. Zároveň dochází pomocí zatlačovacího klínu 8 i k zatlačení vodičů 6 do samozářezných čelistí 2 a tím vznikne vodivé propojení mezi vodičem 6 a samozářeznými čelistmi 2, které jsou propojeny s tištěným spojem detektoru detektoru.

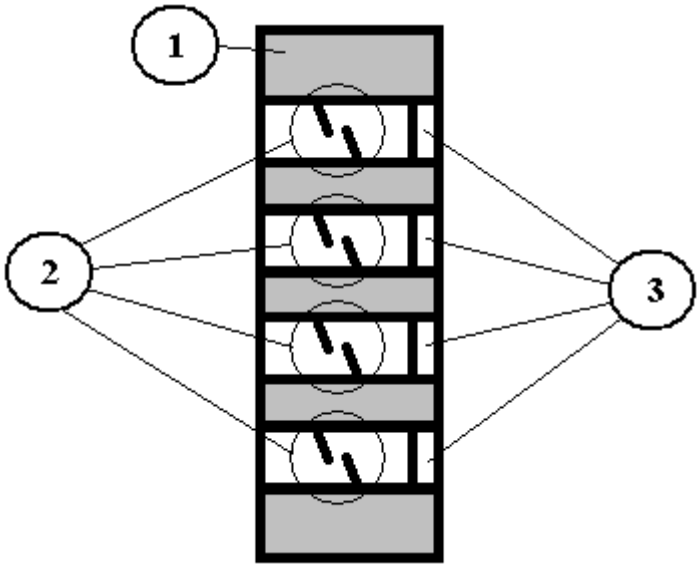
Průmyslová využitelnost

Systém pro upínání kabelů do detektoru nalezne uplatnění při instalaci elektrických zabezpečovacích systémů a jejich komponent ke kabeláži. Pro svou jednoduchou konstrukci a nízké náklady na výrobu je vhodný pro sériovou výrobu.

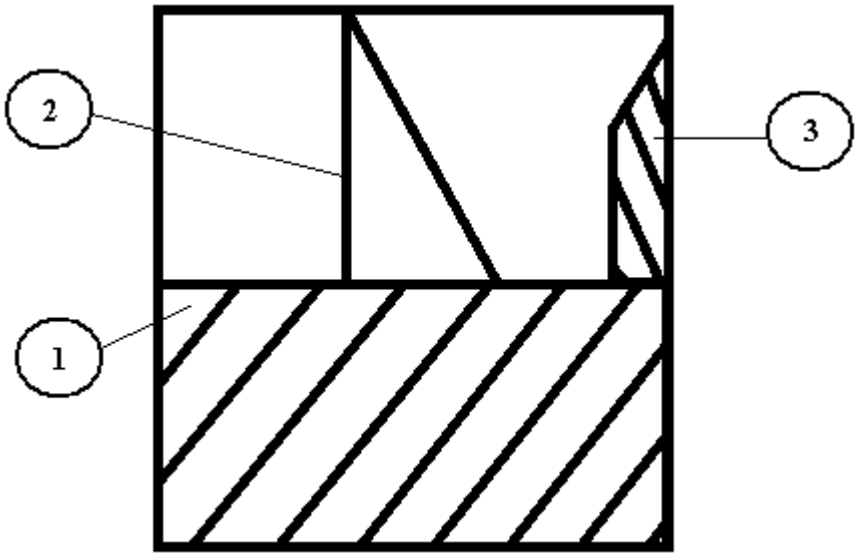
Nároky na ochranu

1. Systém pro upínání kabelů do detektoru **vyznačující se tím**, že se skládá ze samoupínací svorkovnice (1) s implementovanými samozářeznými čelistmi (2), které jsou propojeny s tištěným spojem detektoru, z odřezávacího břitu (3) a z plastového krytu (4), přičemž plastový kryt obsahuje zatlačovací klín (8).

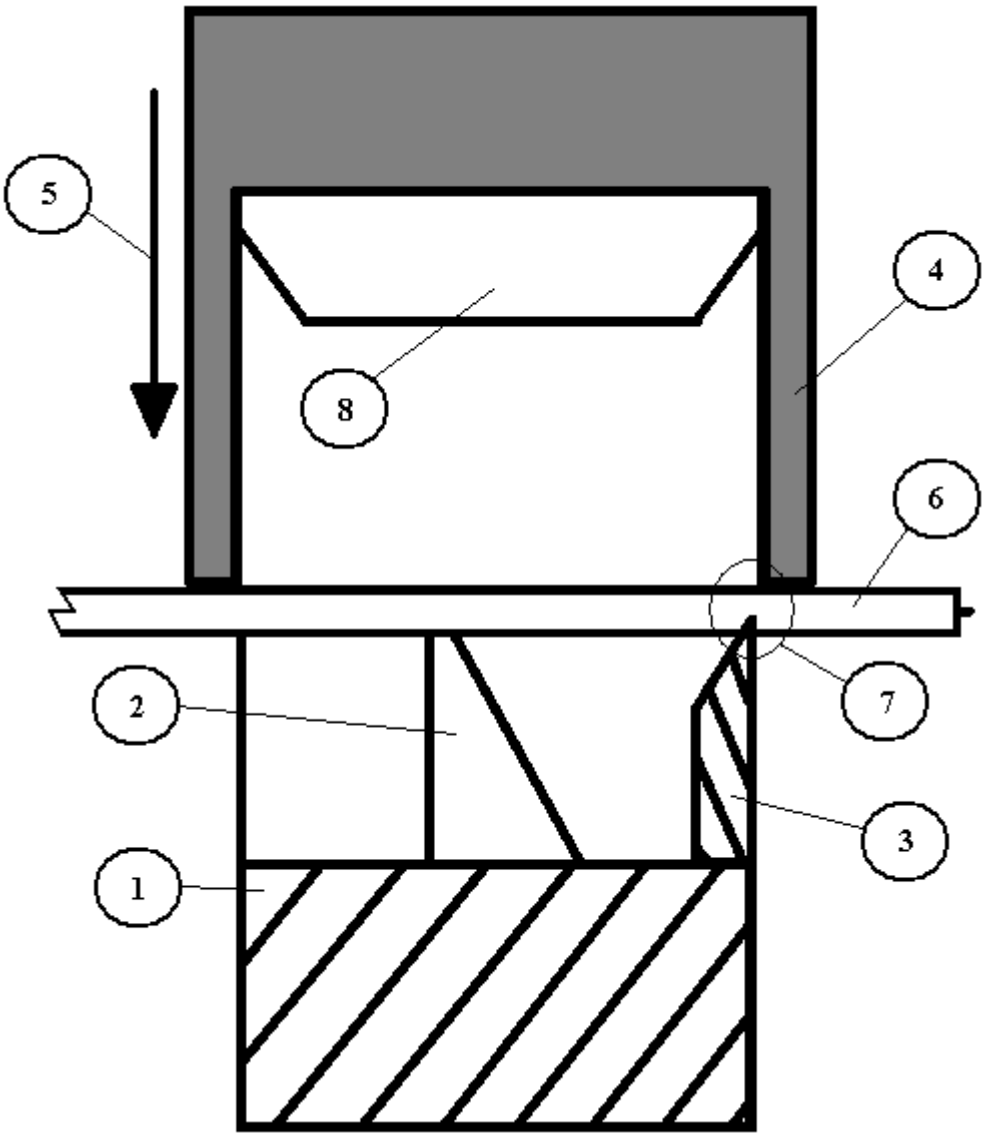
2. Systém pro upínání kabelů do detektoru podle nároku 1, **vyznačující se tím**, že samoupínací svorkovnice (1) lze umístit do krytu detektoru.



Obr.1



Obr.2



Obr.3

Příloha 4

Měřící panel

Čtečky otisku prstů

3D čtečky obličeje (kombinované čtečky)

Příloha 5

Ukázka měření IFace302 – sabotáž 3D čteček obličeje (maskérské líčení)

č.m.	Uživatel 1	Uživatel 2	Uživatel 3	Uživatel 4	Uživatel 5
1	1	0	1	0	1
2	1	1	0	0	1
3	1	0	1	0	0
4	1	1	0	1	0
5	1	1	1	1	0
6	1	0	0	0	0
7	0	0	0	0	1
8	0	0	1	1	1
9	1	1	1	0	1
10	1	1	0	1	1
11	0	1	0	0	1
12	1	0	0	1	0
13	0	0	0	0	0
14	0	0	1	1	0
15	1	1	1	1	0
16	1	0	1	1	1
17	1	1	0	1	1
18	1	0	0	1	1
19	0	1	1	1	1
20	1	0	1	0	1
21	1	1	1	0	1
22	1	1	0	0	1
23	1	1	1	0	0
24	1	0	0	1	0
25	1	0	1	1	0
26	0	1	0	1	1
27	1	1	1	1	1
28	1	1	1	1	0
29	1	1	1	1	1
30	0	1	0	1	0
31	1	1	0	0	0
32	1	1	0	1	0
33	1	1	0	0	1
34	1	1	1	0	1
35	0	1	1	1	1
36	1	1	1	1	0

č.m.	Uživatel 1	Uživatel 2	Uživatel 3	Uživatel 4	Uživatel 5
37	1	1	0	0	1
38	0	0	0	1	0
39	0	1	0	0	1
40	1	0	1	1	1
41	1	1	1	1	1
42	1	0	1	0	0
43	1	0	1	0	1
44	1	0	1	0	0
45	1	1	1	1	1
46	1	1	1	1	1
47	0	1	0	1	0
48	1	1	1	1	1
49	1	1	1	1	1
50	1	1	1	1	1
51	0	1	1	1	0
52	1	0	0	1	1
53	1	1	1	0	1
54	1	1	1	0	0
55	1	1	1	0	1
56	1	1	1	0	1
57	1	1	0	1	1
58	0	1	0	1	0
59	1	1	1	1	1
60	1	1	1	1	0
61	1	1	1	0	0
62	0	1	1	0	0
63	0	1	1	1	1
64	1	1	1	1	0
65	0	1	1	1	0
66	0	1	1	1	1
67	0	1	1	1	1
68	0	0	1	1	1
69	1	1	1	1	1
70	1	1	1	1	1
71	1	1	1	1	1
72	0	1	1	1	1
73	0	1	1	1	1
74	1	1	1	1	1
75	1	1	1	1	1