Česká zemědělská univerzita v Praze
Technická fakulta

Systémy identifikace osob

Bakalářská práce

Obor: Informační a řídící technologie v agropotravinářském průmyslu
Katedra vozidel a pozemní dopravy

Vypracoval: Martin Šteberl
Školitel: Ing. Veronika Hartová, Ph.D.

Praha 2018

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Šteberl

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Systémy identifikace osob

Název anglicky

Identification of persons systems

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku hodnocení systémů identifikace osob. Hlavním cílem je provést rozbor a zhodnocení jednotlivých způsobů identifikace osob.
Dílčí cíle bakalářské práce jsou:

- vytvořit přehled řešené problematiky,

- charakterizovat principy základních způsobů identifikace osob,

- zhodnotit vybrané systémy identifikace osob.

Metodika

Téma bakalářské práce se věnuje problematice identifikace osob. Rozebírá jednotlivé možnosti identifikace osob (biometrická, čipy, hesla, kódy), jejich výhody a nedostatky. Na tuto práci je možno navázat i s diplomovou prací.

Doporučený rozsah práce

30 – 40 stran textu

Klíčová slova

identifikace, čip, heslo, biometrie, okolní podmínky

Doporučené zdroje informací

HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475.

JAIN, A.; BOLLE, R.; PANKANTI, S. „Biometrics. Personal Identficaton in Networked Society.“ Norwell, Massachuse s, USA, Kluwer Academic Publisher, 1999, ISBN 0-7923-8345-1.

RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kolek v. „Biometrie a identita člověka ve forenzních a komerčních aplikacích.“ Praha, Nakladatelství Grada, 2012

Předběžný termín obhajoby

2017/18 LS – TF

Vedoucí práce

Ing. Veronika Hartová, Ph.D.

Garantující pracoviště

Katedra vozidel a pozemní dopravy

Elektronicky schváleno dne 8. 12. 2016

doc. Ing. Miroslav Růžička, CSc.

Vedoucí katedry

Elektronicky schváleno dne 8. 12. 2016

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 02. 01. 2018

„Prohlašuji, že jsem bakalářskou práci na téma: Identifikace osob vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom/a, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom/a, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

.....

Martin Šteberl

Poděkování

Chtěl bych tímto poděkovat své vedoucí práce paní Ing. Veronika Hartová, Ph.D., za vedení a podporu v průběhu celého bakalářského studia, při zpracování bakalářské práce a za cenné rady a věcné připomínky, které mi za dobu studia poskytnula. Dále děkuji celé katedře vozidel a pozemní dopravy a také celé mé rodině a přátelům za psychickou podporu a věcné rady.

Abstrakt

Bakalářská práce se zabývá spolehlivostí běžné identifikace osob, ale také biometrické identifikace osob na základě rozpoznávání obličeje uživatele při užití, či neužití dodatečného přísvitu. Bakalářská práce je rozdělena do dvou hlavních částí: teoretická a praktická.

Teoretická část práce je následně rozdělena na část věnovanou systémům, algoritmům, metodám a přístupům, které se využívají k identifikaci osob a na část věnovanou podmínkám a prostředí, které dané systémy, algoritmy, metody a přístupy ovlivňují. Součástí jsou shrnuty také výhody, nevýhody a zásady plynoucí z použití jednotlivých metod, případně obecných přístupů k biometrii a identifikaci obecně. Teoretická část práce zahrnuje popis přístupu určení spolehlivosti a chybovosti jednotlivých systémů.

Praktická část práce je věnována testování dvou nejpoužívanějších biometrických čteček obličejů v ČR s použitím dodatečného přísvitu. Dodatečný přísvit byl realizován prostřednictvím RGB LED přísvitu s regulací a měření byla realizována v rozdílných světelných podmínkách, odlišných barevných spektrech přísvitu. Byl stanoven výchozí čas přijatelné doby trvání identifikace obličeje a na tomto základě bylo prováděno měření spolehlivosti čteček. Z měření byly stanoveny závěry, zda je dodatečný přísvit u testovaných biometrických čteček přínosem, či nikoliv a zda je ovlivněna spolehlivost těchto čteček a čas identifikace, případně v jaké míře a jaká barevná spektra přísvitu jsou nejpříjemnější z hlediska vjemu lidského oka.

Abstrakt

The bachelor thesis deals with the reliability of common identification of persons, but also biometric identification of persons on the basis of recognition of the user's face when using or not using additional lighting. The bachelor thesis is divided into two main parts: theoretical and practical.

The theoretical part of the thesis is then divided into the part devoted to the systems, algorithms, methods and approaches that are used to identify people and to the part devoted to the conditions and environment that the systems, algorithms, methods and approaches influence. It also includes advantages, disadvantages and principles resulting from the use of individual methods, or general approaches to biometrics and identification in general. The theoretical part of the thesis includes a description of the approach of determination of reliability and errors of individual systems.

The practical part is devoted to testing two of the most used biometric facial readers in the Czech Republic with the use of additional lighting. The additional illumination was realized by means of an RGB LED light with control and measurement performed in different lighting conditions, different color spectra of the light. The default time of acceptable face identification time was established, and reader reliability was measured on this basis. From the measurements, conclusions were made as to whether additional bias on tested biometric readers is beneficial or not, and whether the reliability of these readers and the timing of identification, or to what extent and what color spectrum of the light are the most pleasant in terms of perception of the human eye, are determined.

OBSAH

1 ÚVOD

Svět kolem jde neustále vpřed. Vše kolem se vyvíjí a co se moderních technologií týče, pak se nejedná o žádnou výjimku. V dnešní době je v podstatě již automatickou záležitostí zabezpečení vstupu, ať už se jedná o vstup do budovy, sítě či různých informačních systému. V minulosti k tomu postačilo projít kontrolou, kterou představoval vrátný nebo hlídač, předložit doklady či zadat jednoduché, sebou zvolené přístupové heslo. Informace jsou pochopitelně velmi ceněnou záležitostí, a proto bylo více než jasné, že je pouhou otázkou času, než dojde k jejich zabezpečování. To zajistí, že se k nim může dostat jedinec pouze na základě identifikace, kdy je mu přístup povolen či odepřen.[1]

K prokázání totožnosti již neslouží jenom rodné či například sociální číslo, ale dnes je možné využívat různých metod od čipových karet, přes různá hesla, až po biometrické ověřování identit, které se v současné době stalo rapidně rozvíjející oblastí. S vývojem a rozvojem počítačů a elektroniky obecně se neustále snižují výrobní ceny elektronických součástí a identifikační systémy se stávají stále dostupnější, zejména z hlediska finančního. Identifikační systémy se používají stále více v běžných zařízeních (mobilní telefony, počítače), v domácnostech, v menších i větších firmách, korporacích a nejsou již jen doménou armády, zabezpečení jaderných zbraní, ostře střeženého finančního sektoru (bankovnictví), letištních areálů, stadionů, recepcí významných míst či jiných významně střežených míst a lokalit.[2]

V dnešním moderním světě je důraz kladen také na rychlost identifikace. V případě nedostatečné spolehlivosti, případně rychlosti těchto čteček může docházet ke značné frustraci uživatelů, zdiskreditování věrohodnosti bezpečnostního systému, zpomalení procesu identifikace mající za následek v určitých případech vzrůst ztrátovosti, případně nekorektního vpuštění nežádoucí osoby do objektu představující hrozbu.[2]

Cílem této práce je vytvořit přehledný text, který vymezí základní způsoby identifikace člověka, kontroly vstupu, a především uvede druhy technologie v oblasti identifikace osob. První kapitola se zabývá identifikací občana s ohledem na jeho autentizaci, vymezí identifikátory v rámci České republiky, zhodnotí identifikaci v soukromém a veřejném sektoru. Dále uvede elektronickou identifikaci a identifikaci v rámci EU. Druhá kapitola již rozebírá kontroly vstupu a jejich systémy s ohledem na jejich funkce, klasifikaci, standardy a

strukturu. Třetí kapitola již porovnává druhy technologií v oblasti identifikace osob. Tato kapitola jednotlivě vymezí identifikaci pomocí hesla a pinu, předmětu, biometrického systému, a také kombinaci těchto metod.

2 CÍL PRÁCE

Bakalářská práce je tematicky zaměřena na problematiku hodnocení systémů identifikace osob. Hlavním cílem je provést rozbor a zhodnocení jednotlivých způsobů identifikace osob.

Dílčí cíle bakalářské práce jsou:
- vytvořit přehled řešené problematiky,
- charakterizovat principy základních způsobů identifikace osob,
- charakterizovat a zhodnotit okolní podmínky působící na jednotlivé čtečky,
- naměřit hodnoty chybného přijmutí a odmítnutí uživatele,
- zhodnotit naměřené hodnoty,
- zhodnotit možnosti bezpečnostních rizik u různých typů identifikace osob.

3 METODIKA PRÁCE

Téma bakalářeké práce se věnuje problematice identifikace osob. Rozebírá jednotlivé možnosti identifikace osob (biometrická, čipy, hesla, kódy), jejich výhody a nedostatky. Na tuto práci je možno navázat i s diplomovou prací.

K vypracování rešeršní části bakalářské práce bude použita dostupná literatura společně s internetovými zdroji. Praktické testování přístrojů bude prováděno v laboratoři Katedry technologických zařízení staveb ČZU v Praze, přímo v Laboratoři zabezpečovacích systémů.

Před počátečním testováním bude nutno připravit testovací panel. Jedná se o dřevěnou desku, ke které jsou přidělány jednotlivé čtečky. Měření bude prováděno na rodině, spolužácích a blízkých osobách. Pro testování byly přizvány osoby jak mladší 50 let, tak starší 50 let.

Měření bude prováděno na dvou typech čtecích zařízeních, které umějí snímat 3D tvar obličeje, ale také otisky prstů. Další nedílnou součástí měření bude použití luxmetru, protože při měření půjde o to, jakou intenzitu světla bude zrovna vykazovat okolí. Pro změnu intenzity světla se bude za potřebí použití panelu, který umí měnit barevné spektrum a intenzity jednotlivých barev.

K vlastnímu měření budou vybrány čtečky Multibio 700 a I FACE 302, na kterých bude prováděno měření a budou se zde vyhodnocovat parametry, za jak dlouho a zda budou schopny čtečky rozpoznat daného uživatele při různém barevném spektru okolí.

Časy budou dále vyhodnoceny a budou se posuzovat parametry, které pomohou k rozhodování, zda je možné použít tyto čtečky v běžném provozu.

4 TEORETICKÁ VÝCHODISKA

S pojmem lidská identita se dnes člověk setkává prakticky napříč všemi obory. S tímto termínem se pracuje v psychologii, sociologii, pedagogice, antropologii, politologii a dalších oborech. Na toto téma již bylo vytvořeno velmi mnoho publikací, avšak není možné říci, že by to samotné vymezení pojmu jakkoli usnadnilo. I přes to, že se používá v běžném životě, je jeho vymezení čím dál tím více komplikované. Obecně však platí, že představuje lidské prožívání toho, kým a čím je. Lidskou identitou se zabývali i ti nejznámější myslitelé jako například John Locke, který popisoval člověka jako nepopsanou desku a až v průběhu socializace se vytváří jeho identita. Identitu jako takovou viděl jako způsob rozlišení věcí a hmot, které nemohou být v tentýž čas na různých místech.[1] *„Výsledkem je, že identita zároveň představuje to, čím člověk je, i to, čím není.“*[3]

Sociolog Roger Brubaker vytvořil ve své knize Ethnicity without groups přehled o tom, jak jednotlivé disciplíny nahlížejí na pojem identita. Psychologové ji vnímají jako jádro lidské osobnosti, a to individuální i kolektivní. Největší význam má tento pojem především pro vývojovou psychologii. Sociologové vnímají lidskou identitu jako základní předpoklad pro sociální bytí. Politologie tento pojem používá hlavně při různých politických hnutích.[4]

Identita člověka není zcela definitivní, protože se vyvíjí prakticky po celý jeho život. Sociologický slovník ji vymezuje jako *„hluboký pocit vlastní totožnosti založený na prožívání vlastní komunity. (Jakým člověkem jsem a čím se liším od druhých).“*[4] Prostřednictvím identity člověk prezentuje to, kým a čím je před ostatními jedinci. Dokáže tak přesně vymezit své vlastní já. *„Identita je nositelem osobní integrity daného jedince či skupiny. Je produktem uvědomění si vlastního „já“, tedy toho, že já nebo my jakožto uzavřená entita disponujeme jistými kvalitami, které mne či nás odlišují od jiného či jiných.“*[6]

„Intenzita identit je často v opačném poměru k jejich šíři; lidé se ztotožňují silněji se svou rodinou než se svou politickou stranou, ani to však nemusí být pravidlem. Krom toho se prestiž identit libovolného druhu může měnit v závislosti na míře interakce daného jednotlivce či dané skupiny s okolím.“[7] Současná společnost však používá identitu také k tomu, aby se člověk nějakým způsobem prokázal v rámci určité skupiny. Nejedná se tedy pouze o vnitřní vnímání sebe samého, ale také legitimní prokázání toho, kdo jsem, a k tomuto účelu slouží identifikace.

4.1.1 Identifikace a autentizace člověka

Výše bylo představeno základní vymezení toho, co představuje lidská identita. Ta jé následně přímo provázána s jeho identifikací, která představuje soubor údajů o daném konkrétním jedinci. V rámci společnosti se používá především proto, aby bylo možné daného člověka rozlišit od ostatních. Roger Clark uvádí tři základní způsoby, jak je možné prokázat jedincovu identitu:

- Identifikace znalostní: jedinec se prokáže informacemi, které zná pouze on. Jedná se například o PIN u platební karty nebo například heslo k mailu.
- Identifikace důkazní: jedinec se musí prokázat určitým dokladem, který u sebe má a prokazuje jasně jeho identitu. Může se jednat o občanský nebo řidičský průkaz, ale také například permanentku do knihovny či čipovou kartu na autobus.
- Identifikace biometrická: osoba je nucena prokázat se určitým vrozeným důkazem, který je unikátní pouze pro něj. Jedná se v praxi o otisk prstu, který se používá nejčastěji. Některé disciplíny (nejčastěji z oblasti kriminalistiky) používají například vzorek slin, vlasů či dokonce zuby.[8]

Problém nastává v tom, že tyto metody se často různými způsoby padělají, a proto se metody kombinují. Nejspolehlivější z výše uvedených metod je zajisté biometrie, protože se nedá nijak ztratit či odcizit. V minulosti by bylo možné toto tvrzení říci se 100% jistotou, avšak s ohledem na vývoj vědy a techniky je i spolehlivost těchto metod často nalomitelná. Duplikace biometrických ukazatelů je sice podstatně komplikovanější než například prolomení PIN kódu či zfalšování nějakého dokladu, avšak není možné o ní již hovořit jako o nemožné. Základní identifikační prvky tedy jsou jméno, vzhled, kód, znalost a biometrika.[8]

Identita je tedy ověřována různými způsoby a tento proces je nazýván autentizací. Obecně autentizace představuje kontrolu přístupu daného člověka do určitého informačního systému. Hlavní myšlenkou tohoto ověření je, že se například do daného systému může dostat pouze ta osoba, která k tomu má oprávnění. Autentizace je procesem jednoznačného ověření identity daného uživatele a jejím cílem je zabránění přístupu neoprávněné osoby. Jako příklad je možné uvést internetové bankovnictví, kdy se člověk ke svému účtu musí přihlásit právě přes ověření identity. Nejčastěji se tento proces skládá z nějakého klientského čísla či jména a přijímaní a PIN kódu.[9] Některé banky používají k tomuto účelu také certifikáty, které jsou člověku předány při zřízení bankovního konta. Certifikát tak slouží také k ověření jeho identity, protože bez něj se do banky nemůže přihlásit. Posledním krokem pro přihlášení do

internetové banky může být ověření přes mail nebo telefon, kdy člověku přijde zpráva s nějakým číselným heslem.[10]

Před samotným procesem autentizace je klíčové od jedince získat veškeré dostupné informace o jeho identitě. Jedná se často pouze o vybrané údaje, se kterými bude daný systém pracovat v rámci rozeznání klientovy totožnosti. K získání autentizační informace slouží jednak důkaz dané znalosti, tedy hesla či určitého kódu, vlastnictví nějaké karty či čipu, či určitá tělesná charakteristika, kam spadá například otisk prstu. Každý systém má vlastní autentizační řád a protokol a cílem návrháře tohoto protokolu je to, aby byl systém co nejbezpečnější. K tomu jsou pochopitelně používány i tyto metody kombinovaně spolu, tak jak tomu bylo v příkladu u internetového bankovnictví výše. Čím dál tím více systému generuje jednorázové kódy a hesla, která fungují jen pro danou omezenou chvíli.[11]

4.1.2 Identifikátory v ČR

V České republice se používá několik druhů identifikátoru a níže budou představeny ty, se kterými se pracuje nejčastěji. Pro lepší přehlednost jsou jednotlivé identifikátory rozděleny do podkapitol.[12]

Rodné číslo představuje asi nejčastěji používaný identifikátor v ČR. Zlomovým okamžikem pro rodné číslo byl rok 2000, kdy se o něm začalo více diskutovat z hlediska práva, a to konkrétně ochrany osobních údajů. Do této doby byla právní ochrana rodného čísla nedostatečná. Rodné číslo je vymezeno zákonem č. 133/2000 Sb. o evidenci obyvatel a rodných číslech a o změně některých zákonů, který je stále platný. Rodné číslo je desetimístné a je dělitelné jedenácti beze zbytku. Prvních šest čísel je v podstatě vymezením pro datum narození a určení pohlaví jedince. Za lomítkem se nachází další čtyři číslice, které rozeznávají jedince, již se narodili ve stejný den. Podle zákona se jedná o identifikátor fyzické osoby, která splnila obecně platné podmínky pro jeho nabytí. Jedno rodné číslo může mít pouze jeden člověk, není tedy možné, aby dva lidé měli stejné rodné číslo. Stejně tak jedno rodné číslo může používat pouze jedna osoba nebo jeho zákonný zástupce.[12]

V případě zdravotního pojištění je však označován jako číslo pojištěnce. Může se ovšem stát, avšak pouze v poměrně ojedinělých případech, že osoba rodné číslo nemá, pak mu číslo pojištěnce přidělí přímo Všeobecná zdravotní pojišťovna.

Průkazy pojištěnců byly původně v papírové podobě. Bylo na nich uvedené jméno a příjmení, datum narození a rodné číslo, které bylo zároveň číslem pojištěnce.[13] V roce 2003

byly zavedeny plastové průkazy pojištěnce a zároveň jsou také Evropským průkazem zdravotního pojištění. Výjimku tvoří cizinci mimo Evropskou unii, kteří získávají zdravotní pojištění v případech, kdy jsou zaměstnání v ČR, avšak tyto průkazy nejsou Evropské průkazy zdravotního pojištění. Tito lidé však mají také nárok na plné zdravotní pojištění. Existují také průkazy, na kterých není nutně hrazená plná zdravotní péče, ale například pouze nezbytná, nutná či neodkladná péče.[14]

K nejznámější a nejpoužívanějším způsobům identifikace kromě výše jmenovaných patří bezesporu cestovní pas. Cestovní pas je určen především pro cestování mimo hranice státu. Občané EU, kteří spadají do schengenského prostoru, však nemusí mí k cestování po zemích EU pas. Ten však potřebují, pokud cestují mimo hranice EU. V cestovním pasu je uvedeno jméno a příjmení jedince, datum narození, rodné číslo, číslo pasu. Od roku 2004 byly všechny členské státy EU povinny zavést biometrické prvky, kterými jsou digitalizovaná fotografie a otisky prstů. Tyto aspekty jsou vymezeny v nařízení Rady EU 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy, schváleného dne 13.12.2004. V praxi to znamená, že lidé, kteří ještě měli od tohoto okamžiku platný pas, nemuseli pasy okamžitě měnit, ale postačilo, aby biometrické prvky měli až v novém pasu. Otisky prstů se začalo odebírat až od roku 2009. Důvodem pro zavedení biometrických prvků byly především bezpečnost a znesnadnění padělání těchto cestovních dokladů.[15]

Dalším často používaným identifikačním dokladem je řidičský průkaz. Tím se musí prokázat řidič při policejní kontrole v případě, že je řidičem zastaveného vozidla. Na řidičském průkazu je opět jméno a příjmení, datum narození, rodné číslo, datum vydání a datum ukončení platnosti, název úřadu a číslo dokladu společně s fotografií držitele a jeho podpisem. Právě kvůli velkému množství identifikačních údajů je používán jako identifikátor. Od roku 2004 je vzhled řidičského průkazu pro státy EU stejný. Řidičský průkaz je vydáván na základě složení zkoušek řidičské způsobilosti a nemá jej automaticky každý občan.[16]

4.1.3 Identifikace ve veřejném a soukromém sektoru

V rámci veřejného sektoru budou vymezeny identifikace ve školství, ve zdravotnictví, ve správním a trestném řízení, v exekučním řízení a v rámci samosprávy. Ve školách jsou zpracovávány údaje všech studentů, kteří danou školu navštěvují. Tato povinnost se týká také vysokých škol, která si musí vést databázi především z rozpočtového a statistického důvodu, a stanovuje to zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů.

Dle tohoto zákonu má škola právo vést si ve své evidenci jméno a příjmení, rodné číslo, stav, místo trvalého bydliště studenta. Pokud se jedná o studenta cizince, pak jsou tyto údaje doplněny ještě o datum narození, pohlaví, bydliště v ČR a státní občanství. Zákon také uvádí, že další údaje mít škola nemusí, ale pokud jsou studenti ochotní je sdělit, pak je pochopitelně v databázi mít mohou. Kromě osobních údajů školy evidují také údaje o zápisu ke studiu a poté i zápisu do dalšího ročníku, předchozím vzdělání, studijním programu a oboru, formě studia, složení státní závěrečné zkoušky a také titulu.[17]

Školy používají rodná čísla studentů hlavně při vydávání dokladů a osvědčení o studiu či absolvování studia, dále pak k vydávání různých stipendií a uznání zkoušek při opakování studia či při zahraničním studiu. Tyto úkony jsou povoleny ze zákona a školy tedy nepotřebují mít souhlas studenta, protože v momentě, kdy student začne na dané škole studovat, dává souhlas ke zpracování jeho osobních údajů, což je omezeno na dobu nezbytnou. Fotografie studenta není povinná.[18]

Osobní údaje studentů může zpracovávat také Ministerstvo školství, mládeže a tělovýchovy, které vede také registr docentů a profesorů. V tomto případě registr obsahuje jméno a příjmení, rodně číslo, místo trvalého bydliště. Pokud se jedná o cizince, pak jsou ještě doplněny tyto údaje: pohlaví, bydliště v ČR, státní občanství, vzdělání a údaje o pracovním poměru.[18]

Základní školy také zpracovávají údaje svých studentů. Klíčovým aspektem je to, že na základních školách platí povinná školní docházka. Některé údaje o studentech mohou být citlivé, avšak i zde je zpracování údajů potvrzené zákonem. Zákon také ukládá škole povinnost vést matriku dle §28 zákona č. 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání a jsou v ní tyto údaje: jméno a příjmení, rodné číslo, datum narození, státní občanství, místo trvalého pobytu, datum zahájení a ukončení docházky, informace o zdravotní způsobilosti a zdravotních obtížích studenta, jež by mohla nějak zasáhnout do vzdělávání a ohrozit studenta, sociální znevýhodnění. Také je v registru povinné mít uvedené údaje na zákonného zástupce a pokud s tím souhlasí, tak i kontakt na něj.[18]

V rámci zdravotnictví je pochopitelně také vedená určitá evidence osob. Jedná se především o osoby, které mají zdravotní pojištění a dle zákona jej mají všichni s trvalým bydlištěm na území ČR nebo jsou zaměstnanci zaměstnavatele se sídlem na území ČR. Pojištění je povinen hradit si zaměstnanec, osoba samostatně výdělečně činná, zaměstnavatelé a osoby, za které pojištění hradí stát.[19] V ČR se jedinec při zdravotní péči prokazuje Evropským průkazem zdravotního pojištění a klíčovým identifikátorem je tedy rodné číslo. Zdravotní péče je specifická v tom, že eviduje údaje o jedincově zdraví, které jsou nutné

k poskytnutí adekvátní péče. Jedná se o velmi citlivé údaje, jejichž ochranu zajišťuje Zákon o ochraně osobních údajů a zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování.[20] Tento zákon klade velký význam ochraně údajů člověka a jasně uvádí, že rodné číslo je možné používat pouze v souvislosti s dokumentací ohledně zdraví pacienta.[21]

Dokumentace každého pacienta musí obsahovat: jméno a příjmení, datum narození, rodné číslo, číslo pojištěnce a u cizince ještě bydliště na území ČR či mimo ČR, pokud nemá bydliště v Česku. Dále pak jeho pohlaví, informace o zdravotním stavu pacienta a jeho identifikační číslo. V případě všech pacientů je nutné vést důkladně informace o jeho zdravotním stavu, průběhu zdravotních služeb a rodinnou anamnézu. Dokumentace je vedená v tištěné a elektronické podobě a může do ní nahlížet pouze pacient nebo jeho osoba blízká, případně zákonný zástupce, a to v přítomností zdravotnického pacienta, která má k tomuto úkonu povolení.[22] V souvislosti s modernizací a zdokonalováním elektronických služeb usiluje EU o elektronickou evidenci pacientů. Tato služba je nazývána eHealth a její největší přínos tkví v tom, že lékař či zdravotnický pracovník nemusí čekat na papírovou verzi dokumentace, ale najde vše přehledně online.[23]

V případě správního řízení se i identifikace řídí správním řádem, jenž přesně vymezuje identifikaci účastníků správního řízení. Fyzická osoba se identifikuje jménem a příjmením, datumem narození, místem trvalého pobytu a dalšími údaji dle zákona, který blíže neurčuje, zdali je nutné uvádět také rodné číslo.[24] To se uvádí na dokumentech uvádějících výsledky řízení či například při žádosti o zařazení do evidence uchazečů o zaměstnání. Ten se řídí zákonem č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů.[25] Trestní řízení je upravováno v trestním řádu. Během trestního řízení je sepisován protokol, ve kterém musí být uvedeno jméno a příjmení, adresa pro doručení dokumentace, a další informace potřebné pro ověření totožnosti. Rodné číslo tedy není nutné do protokolu uvádět.[26]

Během exekučního řízení je potřebné také uvádět osobní údaje pro potřebu exekutora. K tomuto účelu dle zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti má exekutor k dispozici velké množství exekučních údajů. Úkony exekutora jsou považovány za úkony soudu, a proto je možné při tomto používat rodné číslo jedince, ale zákon nestanoví, že je nutné jej uvádět.[27] K identifikaci jedince je nutné jméno a příjmení, datum narození a bydliště jedince.[28]

Nejvíce osobních údajů o jedinci zpracovávají obce, které musí s těmito údaji nakládat dle Zákona o ochraně osobních údajů. Obce také jsou dle zákona nuceny informace podávat, při čemž může často dojít k neřešitelné situaci. Obec musí dle zákona mít úřední desku, kde jsou vyvěšeny závazné vyhlášky, nařízení, směrnice a další. Pokud obec doručuje

prostřednictvím úřední desky fyzické osobě nějaký dokument, pak musí dle zákona zveřejnit všechny potřebné údaje k jeho identifikaci, a tento předpis má v tomto ojedinělém případě přednost před Zákonem o ochraně osobních údajů. Osobní údaje jsou také zveřejňovány například ze zápisu zasedání obce.[29]

K identifikaci ovšem často dochází také v soukromém sektoru, což je výsledek zrychlování doby, kdy mnoho lidí volí rychlejší nákup přes internet. Soukromý sektor nemá možnost ověřit si identifikační údaje osob, proto si často vytváří své vlastní databáze klientů či uživatelů. V tomto je nutné jednak vytvářet systém, který bude pro klienty snadný a nenáročný na vyplňování, a také musí být brána v potaz možná kontrola Úřadu pro ochranu osobních údajů. Jednou z takových databází je například elektronické bankovnictví, které využívá prakticky v dnešní době většina lidí. V rámci této databáze klient uvádí velké množství údajů a pokud dojde k jejich narušení, pak je jako viník často viděna banka. Tento systém byl popsán již výše, proto nebude opět více rozváděn, ale nutno dodat, že je v zájmu banky, aby dostatečně zabezpečil klientské konto. Další často využívanou službou je online nákup, ať už se jedná o jakékoli zboží. V těchto případech lidé opět vyplňují celou řadu osobních údajů, které jsou potřebné k nákupu. Často také nakupující souhlasí s využitím jeho osobních údajů dle obchodních podmínek, které si kolikrát ani důkladně neprostuduje, a upíše se tak často k úkonům, o které ani neměl zájem. Při dalším nákupu je často pouhým přihlášením obchodník schopen rozeznat nakupujícího. Pro obchodníky se jedná o obrovský plus, protože díky moderním technologiím jsou schopni vytvořit marketingový plán přímo na konkrétního nakupujícího.[30]

4.1.4 Elektronická identifikace

Byla to v podstatě otázka času, než došlo k elektronické identifikaci osob. Jedná se o *„postup používání identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu.“*[31] V elektronickém, prostředí je nejčastější variantou přihlášení přes uživatelské jméno a heslo, které si určí sám uživatel, nebo mu je automaticky přidělen, a zná jej jen on sám. Ověření identity uživatele se může lišit ve své náročnosti s ohledem na povahu daných stránek a důležitost informací, které skrývá. V tomto případě se však jedná o soukromý sektor a v případě veřejné správy vymezuje možnosti ověřování identity zákon a patří mezi ně elektronický podpis a datová schránka.

Elektronický podpis představuje jeden z *„hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu.“*[32] Vymezuje jej zákon vytvořen na základě směrnice EU č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Elektronický podpis zastupuje vlastnoruční podpis uživatele a klíčové je, aby byl důvěryhodný, a především snadno použitelný. Má takto usnadnit elektronickou komunikaci a klíčové pro jeho platnost je, že musí mít kvalifikovaný certifikát. Elektronický podpis má tři stupně:

- Jméno a příjmení: např. za textem v mailech, dá se snadno zneužít.
- Dále se jedná o sice obyčejný elektronický podpis, který je sice uložen v elektronické podobě, ale dle zákona nesmí být veřejným sektorem používán při ověřování totožnosti.
- Podpis vytvořen na základě kvalifikovaného certifikátu.[33]

Poslední jmenovaný identifikuje původce podpisu, zaručuje integritu sdělení, nepopiratelnost a tento podpis má uživatel plně pod svou kontrolou. Reálně se jedná o komplikované číslo, které prostřednictvím algoritmu převádí do formy podpisu počítač a uživatel musí znát privátní klíč, který má pouze on.[34] Stále však platí, že papírové dokumenty jsou důvěryhodnější. Elektronický podpis má také kratší platnost, která je doplňována kvalifikovaným časovým razítkem.[35]

Další variantou je datová schránka, která je vymezena zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů ve formě datové zprávy, ve znění zákona č. 190/2009 Sb., jenž vymezuje schránku jako elektronické uložiště určené pro doručení dokumentů veřejnou správou či fyzických osob. Schránky zřizuje Ministerstvo vnitra. Fyzické osoby a podnikající fyzické osoby nemusí mít datovou schránku, ale v případě, že si o ni zažádají, jim je zřízená bezplatně. Oproti tomu právnické osoby zapsané v obchodním rejstříku nebo organizační složce zahraniční společnosti na území České republiky musí mít datovou schránku ze zákona. Obecně platí, že každá osoba může mít pouze jednu datovou schránku a musí o ní zažádat osobně či s elektronickým podpisem. K přihlášení slouží přístupové údaje: uživatelské jméno a heslo, které Ministerstvo vnitra zasílá do vlastních rukou.[36]

4.1.5 Identifikace v rámci EU

Identifikace občanů v rámci EU upravuje několik předpisů a obecně platí, že se příslušník dané země prokazuje svým osobním dokladem. Schengenský prostor umožnil lidem cestování bez předkládání pasu v rámci EU. V rámci elektronické identifikace se usiluje

o snížení rizik při přesunu informací a tuto formu upravuje Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13.12.1999 o zásadách Společenství pro elektronické podpisy. V rámci elektronické identifikací v prostoru EU byl zaveden projekt STORK 2.0, který nastoupil STORK, jenž byl v roce 2011 ukončen. Myšlenkou tohoto projektu je vytvoření jednotného prostoru elektronické identifikace v rámci Evropy. V rámci tohoto projektu došlo k vytvoření těchto čtyř identifikačních databází v soukromém i veřejném prostoru. Jedná se o elektronické vzdělávání eAcademia, elektronické bankovnictví eBanking, elektronické zdravotnictví eHealth a veřejné služby pro soukromou sféru.[37]

4.2 Kontroly vstupu a jejich systémy

Systémy kontroly slouží k opatřením zajištění a evidence vstupu osob do zabezpečených prostorů či objektu. Systém kontroly je možné obecně dělit na fyzické, mechanické, elektronické nebo systémové. Pochopitelně nejefektivnějším řešením, je kombinovat všechny výše zmíněné. Tato práce se však zabývá těmi systémovými, pro které platí, že daný jedinec má do zabezpečeného prostoru určitá přístupová práva, která jeho přístup povolí či zamítnou. Přístupové systémy pohyby těchto lidí mapují.[38]

4.2.1 Funkce kontroly vstupu

Systémy kontroly vstupu se řídí především dle normy ČSN EN 60839–11–1 o poplachových systémech a elektronických bezpečnostních systémech. Tyto systému musí dle normy obsahovat 11 základních funkcí, mezi které patří:

- zpracování – porovnávání změn, které v systému nastaly s přednastavenými pravidly,
- komunikace – přenos signálu mezi komponenty systému kontroly vstupu,
- konfigurace – nastavení pravidel zpracování,
- rozhraní míst přístupu – aktivace a monitorovaní místa přístupu,
- identifikace – rozpoznání oprávněných uživatelů žádající o přístup,
- oznámení – funkce výstrahy zobrazení nebo záznamu událostí,
- signalizace nátlaku – tiché varování o stavu probíhajícího vynucovaného požadavku přístupu,
- rozhraní pro spojení s ostatními systémy – sdílení funkcí nebo změn, k nimž v systémech dochází,
- vlastní ochrana systému – slouží k ochraně a informuje o úmyslném nebo náhodném zasahování do systému.
- napájecí zdroj,
- uživatelské rozhraní –indikace.[38]

4.2.2 Standardy týkajíc se kontroly vstupu

Technické normy řady ČSN EN 50133, které upravovaly systémové a technické požadavky na systémy kontroly vstupu, byly nahrazeny normou ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty a poté normou ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace. Ta je v platnosti společně s normou ČSN EN 50133-7 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace. Normy jsou platné do 13. dubna 2018.[39]

Norma ČSN EN 60839-11-1 byla vydána v únoru 2014 a účinnosti nabyla 11. 6. 2016, kdy nahradila normu ČSN EN 50133-1. Norma upravuje standardy pro systému kontroly vstupu v těchto sférách: terminologie, architektura systému, stupně klasifikace, funkčnost systému, odolnosti proti vlivům prostředí, způsoby zkoušek. Základními změnami oproti předchozí normě je především nová klasifikace zabezpečení dle úrovně rizika. Ty jsou rozděleny na čtyři stupně rizika. Dále také došlo ke zvýšení rozsahu zpracování funkčních požadavků a míry volnosti a inspirace funkčních požadavků pro jednotlivé systémy kontroly vstupu. V neposlední řadě došlo také k rozšíření terminologie o nové názvosloví jako EACS – Electronic Access Control Systems, FAR – False Acceptance Rate, portál a další.[40]

V březnu v roce 2016 došlo k vydání normy ČSN EN 60839-11-2 Technická norma, která svou účinnost nabude 13. dubna 2018 roku a nahradí tak normu ČSN EN 50133-7. Tato norma upravuje především problematiku spojenou s návrhy projekce, instalace, revize, provozu a údržby systémů kontroly vstupu. Norma také rozebírá nové standardy v oblasti terminologie, požadavků na odolnost proti vlivům prostředí a EMC, plánování systému a nalýzu rizik, montáž systému a uvedení do provozu. Zabývá se také s tím spojenou dokumentaci.[41]

4.2.3 Klasifikace kontroly vstupu

Klasifikace kontroly vstupu jsou rozděleny do čtyř stupňů. Tyto stupně jsou podrobně rozepsány v tabulce níže.

Stupeň	**1**	**2**	**3**	**4**
Úroveň rizika	Nízké	Nízké a střední	Střední až vysoké	Vysoké
Aplikace	Organizační prostředky, ochrana majetku nízké hodnoty	Organizační prostředky, ochrana majetku nízké a střední hodnoty	Méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty	Zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury
Dovednosti / znalosti pachatelů	Malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, malé finanční prostředky pro napadení	Střední dovednosti a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, malé až střední finanční prostředky pro napadení	Velká dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, střední finanční prostředky pro napadení	Velmi vysoká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, velké finanční prostředky pro napadení
Typické pří – klady	Hotel, penzion	Obchodní kanceláře, malé firmy	Průmysl, administrativní prostory, finanční instituce	Vysoce citlivé prostory (vojenské zařízení, vládní budovy, apod.

Tabulka 1: Stupně klasifikace

Zdroj: vlastní zpracování dle ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 33 4593.

4.2.4 Struktura kontroly vstupu

Struktura systému kontroly vstupu zahrnuje konstrukční a organizační prostředky a zařízení, jež jsou v rámci kontroly vstupu přímo vyžadovány. Struktura těchto systému je vždy vytvářená následujícími prvky:

- Místo přístupu
- Zařízení pro odchod
- Rozhraní místa přístupu
- Rozhraní pro uživatele
- Řídící jednotka kontroly vstupu
- Napájení
- Komunikační síť
- Řídící a obslužné pracoviště.[42]

Systémy kontroly vstupu se dále dělí na autonomní a modulární systémy. Autonomní systémy slouží pro zabezpečení řízení kontroly vstupu a odchodu z jednoho přístupového stanoviště a zahrnuje jedno nebo dvě snímací zařízení, jako například čtečky či biometrické zařízení. Dále zahrnuje řídící jednotku, která je integrována do snímacího zařízení nebo je tvořena samostatným modulem. Tyto systému se doporučuje umisťovat především do objektů, kde je menší četnost pohybu lidí. Oproti tomu modulární systémy najdou své využití především v případě objektů, kde je četnost lidí vysoká a mají více přístupových míst, které jsou propojeny s řídící jednotkou a řídícím pracovištěm. [43]

Systémy kontroly jsou děleny také dle způsobu propojení, a to na sběrnicové propojení řídících jednotek míst přístupu, sběrnicové propojení inteligentních čteček, sběrnicové, sběrnicové propojení s využitím RS485/LAN převodníků, propojení s využitím IP řídících jednotek, propojení s využitím IP čteček. Tyto systémy mají také elektrickou část, kam patří například řídící jednotky, snímání, biometrické prostředky, karty, čipy a další, a elektromechanickou část, kam patří zámky dveří, turnikety, otvírače a další. Čtečky karet jsou ještě děleny na základní, polointeligentní a inteligentní čtečky dle jejich funkcí.[43] Pokud se

jedná o samotný identifikační proces, pak jsou děleny do tří skupin na znalostní, tedy dle určitého hesla či kódu, na vlastnické, tedy jedinec musí mít určitou kartu, čip nebo jiné zařízení, nebo biometrické. Tyto typy se dále dělí na manuální, čipové, magnetické, optické, radiofrekvenční, biometrické.[44]

4.3 Technologie v oblasti identifikace osob

Svět je v neustálém pohybu a technologie se vyvíjí prakticky den ode dne. Nejvýznamnější změny v oblasti identifikace osob jsou právě v tom, jak se daný jedinec přihlašuje a ověřuje svou totožnost. Dnes je možné ověřit identitu několika způsoby a mezi ty nejčastější patří prostřednictvím hesla a pinu, tedy dle toho, co si daný jedinec musí pamatovat, poté prostřednictvím předmětu, tedy díky tomu, co vlastní, dále se identifikuje prostřednictvím biometrického systému, který je zatím považován za nejúčinnější. Ideální j ovšem kombinovat všechny zmíněné metody. [2]

4.3.1 Identifikace osob prostřednictvím hesla a pinu

Neznámější metodou identifikace je ta, kdy se člověk přihlásí prostřednictvím hesla či pinu. Jedná se o nejstarší metodu, ale nutno dodat, že také nejjednodušší, tedy i nejsnadněji napadnutelnou. Klíčové je, aby si daný jedinec heslo či pin zapamatoval. Jedná se o posloupnost znaků, kterými ověřuje svou totožnost. Nejčastěji se jedná o čísla, ale mohou se vyskytovat i písmena. Každá databáze má předem vymezená svá pravidla, dle kterých jsou piny a hesla sestavovány.[46] *„Použití hesla jako prostředku pro přístup do systému je stále nejpoužívanějším principem zabezpečení. Velký podíl na tom má i jeho globální použití v osobních počítačích, počítačových sítí, emailových účtech, u SIM karet mobilních telefonů a u platebních karet. Bezpečnost je v tomto případě zajištěna tím, ţe si omezený počet uživatelů (nejlépe jeden) pamatuje určitou posloupnost znaků, kterou mu umožní přístup do chráněné oblasti. Výhody hesel jsou snadný způsob realizace a nízká cena pořízení. Velká řada nevýhod ovšem použití hesel omezuje na systémy s nízkým stupněm zabezpečení.“*[47]

Heslo je složeno z 6. až 10. znaků a je zadáváno společně s nějakým uživatelským jménem. Systém následně porovnává, zdali heslo a uživatelské údaje sedí a na základě toho je odepřen nebo povolen přístup. Heslo je prolomitelné, proto se doporučuje, aby si uživatel heslo dobře chránil. Mnoho systému generuje heslo automaticky dle bezpečnostních požadavků. Zde je ovšem riziko, že jedinec heslo zapomene. Obecně se tedy doporučuje vytvořit heslo o 8. až 12. znacích, které je složeno z malých a velkých písmen, číslic a dalších znaků. Platí také zásada, že tyto hesla nejsou ve slovnících. [48]

Základní rozdíl u PINu je v tom, že uživatel má omezený počet pokusů k přihlášení. Pokud uživatel zadá několikrát PIN špatně, pak je mu přístup odepřen a PIN se zablokuje. V tomto případě se přechází k dalšímu kroku, kdy musí být nesprávný PIN a nulován, a k tomu je používán tzv. PUK. Často je možné se setkat také s tím, že po určitém časovém úseku je možné PIN zadat znovu. Vždy je to v závislosti na konkrétním systému. PIN je oproti hesla kratší a je složen z 4. až 8. znaků.[49]

U PINu i hesla je možné rozdělit možnost přihlášení do dvou skupin:

- Heslo nebo PIN dostane skupina osob, která je používá k přihlášení a ověření své totožnosti. Může se jednat například o přihlášení do určité skupiny či vstup do budovy. Nevýhodou je, že přístup má mnoho lidí na jeden PIN či heslo a kontrola je v těchto případech velmi obtížná.
- Druhou variantou je, že každá osoba má svůj PIN či heslo, prostřednictvím kterého se hlásí do systému nebo mu je umožněn vstup. Ověření konkrétního člověka je takto o dost snazší.[50]

4.3.2 Identifikace osob prostřednictvím předmětu

Pokud se osoba identifikuje prostřednictvím předmětu, pak se jedná o vlastnost daného prostředku k identifikaci k danému systému. Jedno médium má v tomto případě jedna osoba. Druhu médií je několik a vždy je potřebné dbát na bezpečnost informace, kterou médium nese, bezpečnost přenosu, spolehlivost identifikace, trvanlivost po stránce mechanické a kapacitu pro uložení potřebných dat.[51] „*Výhodou a zároveň nevýhodou tokenu je jeho přenositelnost, proto by měl být token vždy používán jen v kombinaci s heslem anebo jako nositel biometrického vzorku uživatele. V praxi používanými tokeny jsou: tokeny pouze s pamětí (magnetické, elektronické nebo optické karty) jako obdoba mechanického klíče tokeny s heslem – vyžadují zadání hesla zároveň s použitím, např. platební karty logické tokeny – dokáží zpracovávat jednoduché podněty, např. vydej klíč/cyklickou sekvenci klíčů inteligentní token – mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, mohou umět šifrovat a generovat náhodná čísla.*“[52]

1. Magnetický systém

K tomuto systému jedinec většinou má kartu, která rozměrově připomíná běžnou platební kartu. Tento tvar je klíčový, protože v jiném případě by nebylo možné kartou projet čtecím zařízením. Karta má magnetický proužek, který v sobě nese údaje o kartě a vlastníkovi. Magnetický proužek je tedy nositelem informací a úložním místem. Během

vložení karty a tažení čtečkou dojde ke zmagnetizování, kdy se vytvoří množství permanentních magnetů, a poté tyto magnety vytváření jednoduché binární rozhodování. Zmagnetizování je tvořeno logickou 1 a nezmagnetizování logickou 0.[53] Tyto karty se dále dělí na:

a. Karty s magnetickým pruhem HiCo (High Coercivity), které mají vysokou hustotu záznamu a používají se například ve věrnostních programech. Používají se hojně i v rámci kontroly vstupu. Mají poměrně nízké náklady na svou tvorbu a velmi snadné použití. Nevýhodou je menší trvanlivost a snadné poničení.
b. Karty s magnetickým pruhem LoCo (Low Coercivity), které oproti předchozím mají nízkou hustotu záznamu. Slouží k nahrávání informací o jejím uživateli.[54]

Jsou k dispozici tři stopy magnetického záznamu dle normy ISO 781, a to:

- 1 stopa (IATA) - má 79 znaků, dají se na ní nahrát jen alfanumerické znaky.
- 2 stopa (ABA) - má 40 znaků, dají se na ní nahrát jen číslice 0-9 a rovnítko.
- 3 stopa (THRIFT) - má 107 znaků, využívá se v bankovním prostředí pro uchování PIN, dají se nahrát jen číslice 0-9, rovnítko, dvojtečka.

Tyto karty mají poměrně velkou trvanlivost, tedy 5 až 6 let, a není obtížné je vyrobit, což snižuje jejich bezpečnost. Nízké náklady jsou tak na úkor bezpečnosti. Na základě těchto karet se používá jednostopé, dvoustopé a třístopé čtečky.[55]

2. Optický systém

V tomto případě se jedná o čárový kód a cena těchto karet je velmi nízká. Bezpečnost je velmi malá, protože k jejich duplikaci jedinci postačí kopírka. V kódu je uložena číselná informace, dle které je možné v databázi vyhledat dané hodnoty. Ty jsou snímány pomocí laserového paprsku. Nejpoužívanějšími typy čárového kódu jsou EAN 8, EAN 13, CODE 39, CODE 128, CODABAR a další. Variantou je i ukrytí kódu pod speciální barvu, ale tyto karty je možné číst pouze pod infračerveným paprskem. Snímače se dělí na laserové a digitální, kdy druhé zmíněné fungují podobně jako digitální fotoaparáty. Nejdříve je snímán čárový kód a jeho obsah je dekódován prostřednictvím dekodéru. Tyto digitální snímače čtou 1D i 2D symboly.[56]

3. Kontaktní systém

V tomto případě musí dojít ke kontaktu média s čtečkou. Jedná se nejčastěji o pouzdro či kartu, které mají kontaktní pole. Toto musí být pro četní zapojeno do obvodu. Patří sem:

a. Čipové karty

Čipové karty jsou využívány jako médium a mají široké využití. *„čipové karty mohou obecně sloužit k ukládání libovolných datových struktur (paměťové čipové karty), dnes se však spíše hovoří o kryptografických čipových kartách, které slouží k ukládání klíčového materiálu případně k operacím s těmito klíči.“*[57] Jedná se o bezpečné a spolehlivé médium, které ukrývá informace na čipu karty. Vleze se do nich větší množství dat. Nevyužívají se u kontroly vstupu, ale spíše např. k přihlášení k PC nebo dané síti. Tyto čipy musí splňovat standardy ISO 7816–1 a vyskytují se ve dvou provedeních: rozměr platební karty nebo velikost SIM karty. S vývojem technologií vznikly i hybridní karty, kdy je možné kombinovat datová média jako např. kontaktní a bezkontaktní čip.[2]

4. Bezkontaktní systém

Jedná se o nejčastěji využívanou metodu při vstupu do objektu. Tento systém je založen na rádiovém přenosu dat mezi médiem a čtečkou. Informace jsou uloženy v elektronické podobě do malých čipů či tagů a jsou čteny prostřednictvím rádiových vln. Jedná se tedy o bezkontaktní paměťové prvky, během kterých nemusí dojít ke kontaktu s čtečkou. Vzdálenost potřebná k přečtení informací je zhruba 5 až 10 cm. Celý systém pracuje na dvouanténním přístupu, kdy je jedna anténa v transpondéru a druhá je připojena ke snímači. Doba potřebná k připojení je cca 100 až 120 milisekund. Patří sem:

a. NFC technologie

NFC neboli Near Field Communication je jednou z nejnovějších technologií a začala se pozvolna rozvíjet od roku 2004. Jedná se o komunikaci mezi zařízeními na velmi krátkou vzdálenost. Za touto formou stojí společnost Sony a Philips, ale nyní jsou přijaty ISO/IEC jako standardy. NFC zařízení fungují ve třech režimech: *„Card Emulation Mode: V režimu emulace karty se NFC zařízení tváří jako tzv. Smart card (chytrá karta). Tento režim je využíván při bezkontaktních platbách nebo pro programování systému PATRON-PRO 1.0.“*[58] Druhým režimem je: *„Peer-to-peer: V režimu peer2peer probíhá komunikace mezi dvěma NFC zařízeními, která si mezi sebou vyměňují data. Jde například o vizitky, multimediální soubory a jiný obsah. Režim P2P je také využíván pro programování přístupového systému v systému PATRON-PRO 2.0.“*[59] A posledním je režim: „*Reader/Writer. V tomto režimu je*

NFC zařízení schopné číst a zapisovat NFC tagy. Tento režim je v systému PATRON-PRO využíván při editaci databáze oprávněných médií.“[60]

Ke komunikaci využívá elektromagnetické vlny na frekvenci 13.56 MHz a technologii RFID. Maximální vzdálenost přenosu je zhruba 10 cm s maximální rychlosti přenosu 424 kb/s. Dělí se na aktivní, které má anténu a zdroj energie pomocí kterého generuje elektromagnetické pole, a pasivní, který má anténu, ale nemá zdroj energie. „*V současnosti se začíná technologie NFC vyskytovat v čím dál více aplikacích. Prvním a nejvýznamnějším využitím jsou bezkontaktní platby. S touto technologií se u nás můžete setkat téměř v každém obchodě, kde je možné platit kartou. Mobilní telefon s NFC může být také využíván k načítání NFC tagů. NFC tag je obvykle bezkontaktní RFID štítek využívající standardy NFC. Do NFC tagu lze uložit například odkaz na web, vizitku, provázat ho na sociální sítě apod.*

Mezi další využití patří například NFC přístupové systémy, které umožňují vstup do chráněného objektu přiložením mobilního telefonu místo karty. Průkopníkem v této oblasti je v ČR společnost IMA s.r.o.“[61]

4.3.3 Identifikace osob prostřednictvím biometrického systému

Biometrie je pro některé spíše spojována v rámci policejního šetření, avšak dnes je již hojně využívána i v běžném životě. Pozitivem této metody je především fakt, že si člověk nemusí nic pamatovat a nemůže nic ztratit. Je velmi obtížné duplikovat tuto metodu identifikace a s ohledem na další identifikátory se tato metody vyvíjí nejrychleji. Biometrická identifikace je vymezená jako použití měřitelných, fyzikálních a fyziologických znaků či projevů člověka k jednoznačnému určení či ověření jeho identity. „*Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik a jejich následné porovnávání s údaji předem sejmutými. Cílem v oblasti bezpečnosti je vytvoření komplexních systémů založených na kombinaci měření více charakteristik. Tím se bezpečnost těchto systémů mnohonásobně zvýší. Současné biometrické systémy pracují s různými charakteristickými znaky člověka, jako jsou otisk prstu, geometrie tváře, duhovka oka, sítnice oka, geometrie ruky, geometrie prstů, struktura žil na zápěstí, tvar ucha, složky lidského hlasu, lidský pach, DNA, dynamika podpisu a dynamika psaní na klávesnici a další. Výčet a popis některých je popsán dále v tomto textu.“*[62]

Na celém světě jsou pro identifikační účely nejvíce prozkoumané a nejvíce užívané tyto identifikátory:

4.3.4 Otisk prstu

Jedná se o nejstarší biometrickou metodu. Existují archeologické důkazy, že otisky prstů byly pro identifikační účely používány již v Asýrii a Číně, minimálně 6 až 7 tisíc let před narozením Krista. V Babylónu se otisky prstů používaly k identifikačním účelům za královny Hanimurabi (1792–1750 před Kristem). První, zadokumentované vědecké poznatky o otiscích prstů na evropském kontinentu jsou spojeny až s rokem 1686. Osobnost J. E. Purkyně můžeme považovat za zakladatele teoretické analýzy fyziologických zákonitostí daktyloskopie. Tento významný český lékař rozlišoval devět základních daktyloskopických vzorů:

1. příčné záhyby (flexerae transversae),
2. střední podélný pruh (stria centralis longitudinalis),
3. šikmý pruh (stria obligua),
4. šikmý záliv (sinus obligus),
5. mandle (amygdalus),
6. spirála (spirula),
7. elipsa (elipsis),
8. kruh (circulus),
9. zdvojený vrcholek (vortex duplicatus).[2]

Jedná se o snímání pomocí senzoru otisku prstu. Daktyloskopické stopy vznikají vzájemným kontaktem mezi pokožkou pokrytou papilárními liniemi a nějakým dalším objektem.[2]

Každé zařízení, které obecně provádí jakékoliv vyhodnocení, je závislé i na kvalitě vstupních dat. Nejinak je tomu i v případě automatizované identifikace osob, založené na daktyloskopických otiscích. Snímání daktyloskopických otisků, podle časové posloupnosti a technologičnosti snímání, lze rozdělit do dvou základních skupin:

1. Klasické snímání daktyloskopických stop – Součástí tohoto procesu je vyhledávání daktyloskopických stop, jejich zviditelňování, fixace a přenášení do daktyloskopických sbírek a evidencí.
2. Bezprostřední snímání daktyloskopických otisků – Dnes spíše typické pro aplikace komerčně-bezpečnostního charakteru. Osoba, požadující vstup do určitého objektu položí prst na snímací senzor, ten sejme otisk a vzápětí následuje verifikace.[2]

Snímací senzory lze podle způsobu kontaktu snímaného povrchu tkáně s daktyloskopickou kresbou formálně rozdělit na senzory kontaktní a bezkontaktní. Kontaktní senzory můžeme podle technologie rozdělit na:

1. Optické – Tyto senzory pracují na technologii FTIR (Frustrated Total Internal Reflection). Laserový paprsek zespodu osvětluje povrch prstu, který se dotýká průhledné desky senzoru. Odrážený světelný tok je snímán CCD (Charge Coupled Device) prvkem.
2. Elektronické – Pracují na principu vzniku elektrického pole mezi dvěma paralelními, vodivými a elektricky nabitými deskami. Kolem senzoru je vodivý prstenec. Jakmile se prst dotkne tohoto prstence, dojde k uzavření elektrického obvodu. Husté pole snímacích antén, které leží nad základní deskou vysílající referenční signál, zachytí elektrické pole deformované tvarem povrchu kůže. Signál je zesílen a transformován do elektronického obrazu daktyloskopického otisku.
3. opto-elektronické – Horní vrstva, která má kontakt s kůží verifikované osoby má schopnost po dotyku emitovat světlo. To je zachyceno v další skleněné vrstvě, do které jsou v hustém poli zataveny fotodiody. Ty převádějí světelný impuls na impuls elektrický. Tímto způsobem je vytvořen elektronický obraz daktyloskopického otisku.
4. Kapacitní – Dotykem kůže papilární linie „přemosťují“ jednotlivé vodivé plošky v závislosti na kresbě papilárních linií, zatímco brázdy se chovají jako izolant. Měří se napětí a kapacitní úbytky mezi jednotlivými vodivými ploškami. Tak vzniká digitalizovaný obraz papilární kresby
5. Tlakové – Tlak papilárních linií transformuje do elektrického signálu, a tak vytváří obraz daktyloskopického obrazu.[62]

Některé tradiční snímače otisků prstů jsou nespolehlivé, protože je poměrně snadné odcizit něčí otisk na základě papilárních linií. *„Multispektrální technologie založená na spektrální analýze obrazu používá více vlnových délek světla k identifikaci otisku. Ty snímají biometrické údaje i pod povrchem kůže a tím zabraňují neoprávněné osobě s falešným otiskem správné identifikaci pod jiným uživatelským účtem. Technologie tak umožňuje rozpoznat otisk živé či mrtvé osoby a jiných organických a syntetických materiálů. Multispektrální technologie dokáže odhalit i situaci, kdy má identifikovaná osoba na svém otisku prstu nanesenou tenkou vrstvu, na které je otisk cizí osoby. Při přitlačení otisku k senzoru dochází v tomto místě prstu k odkrvení. Toto odkrvení je snímačem, který snímá i údaje pod povrchem otisku, detekováno a lze pak jednoduše určit, jestli jde o skutečný otisk nebo o falsifikát.“*[63]

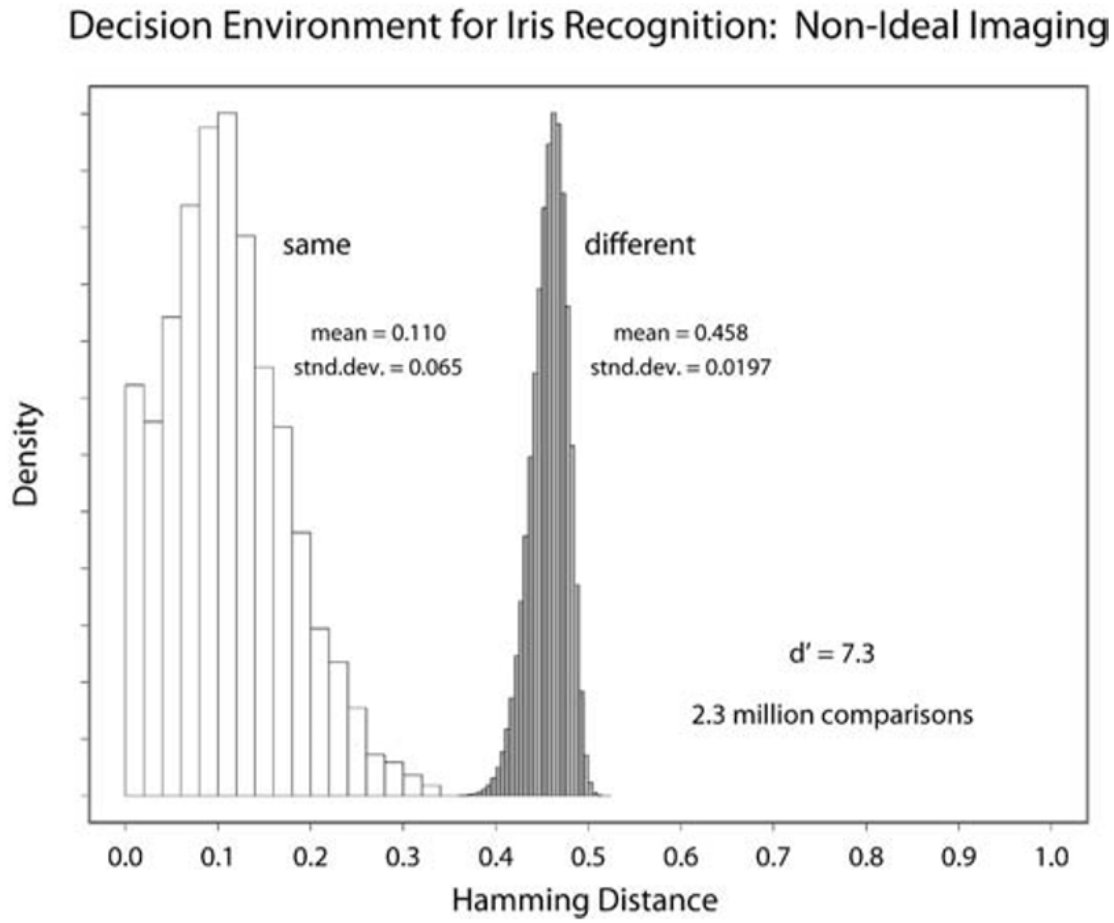
4.3.5 Duhovka oka

Pro ideální zachycení vzoru duhovky je nutné, aby snímek poskytoval alespoň 70 pixelů. K tomuto účelu se používají CCD kamery. Zaostření obrazu se provádí v reálném čase pomocí spektrálního výkonu ve středních a horních frekvenčních pásmech 2D Fourierova spektra: „*Stejně jako například otisky prstu, i duhovku oka má každý člověk jedinečnou. Proto se tohoto faktu využívá pro identifikaci osob, zvláště v případě oprávnění k přístupu do informačního systému. V takovýchto aplikacích je totiž vzhledem k otiskům prstu významný rozdíl. Nalezení dvou identických duhovek náhodným výběrem je přibližně 1050krát menší, než nalezení dvou identických otisků prstu. Duhovky dvou identických dvojčat jsou samozřejmě také rozdílné a jedinečné. Ve skutečnosti dokonce i obě duhovky jednoho člověka jsou rozdílné a jedinečné. Z tohoto pohledu neexistuje jiná externí biometrická charakteristika člověka, která by byla více rozlišovací než právě duhovka.“*[63]

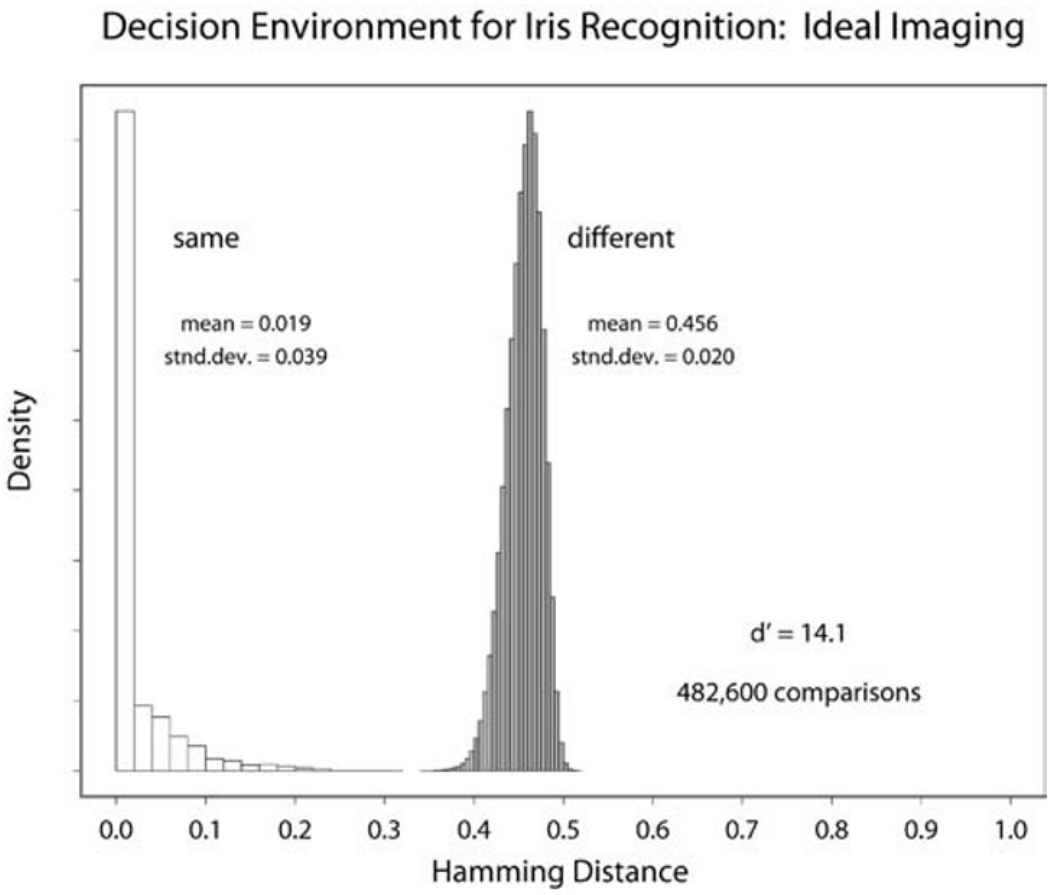
Celková „rozhodnutelnost“ úkolu rozpoznávání osob podle vzorů jejich duhovek je ukázána na rozložení Hammingových vzdáleností pro stejné a rozdílné duhovky. Hammingova vzdálenost je nejmenší počet pozic, na kterých se řetězce stejné délky daného kódu liší, neboli počet záměn, které je potřeba provést pro změnu jednoho z řetězců na druhý. Levé rozložení na obrázku 1 ukazuje Hammingovy vzdálenosti spočítané pro 7 070 různých párů stejných očí nasnímaných v různou dobu za různých světelných podmínek a obvykle též různými kamerami; pravé rozložení ukazuje 9,1 milionu srovnání různých očí uvedených již dříve. Spolehlivé rozhodnutí, zda předložený vzorek patří do levého nebo pravého rozložení na obrázku 1, je u identifikace pomocí duhovky možné provést. Tato reprezentace rozhodovacího problému se nazývá „rozhodovací prostředí“, protože ukazuje, do jaké míry jsou oba případy (stejná duhovka nebo odlišná duhovka) odlišitelné a jak spolehlivé tedy rozhodnutí bude, neboť překrývající se část obou rozložení určuje chybovost.[64]

Zatímco obrázek 1 zobrazuje rozhodovací prostředí při nepříznivých podmínkách (snímky získané pomocí různých typů kamer), obrázek 2 ukazuje rozhodovací prostředí při ideálních (téměř umělých) podmínkách. Snímky očí byly získány v laboratorních podmínkách pomocí stejných kamer s konstantním optickým přiblížením, z konstantní vzdálenosti a při stejných světelných podmínkách. Nepřekvapí, že více než polovina srovnání takto získaných snímků dosáhla Hammingovy vzdálenosti 0,00 a průměrná Hammingova vzdálenost byla

pouhých 0,019. Ze srovnání obrázků 1 a 2 je zřejmé, že „skutečné“ rozložení pro srovnávání duhovek (podobnost mezi různými snímky stejných očí zobrazená v levé části rozložení) záleží velice silně na podmínkách snímání obrázků oka. Na druhé straně však podobnost „podvodníků“ (pravá strana rozložení) je téměř zcela nezávislá na podmínkách snímání. Místo toho je pouze výsledkem kombinatoriky Bernoulliho pokusů, neboť se srovnávají bity z různých nezávislých zdrojů bitů).[2]



Obr. 1: Rozhodovací prostředí pro rozpoznávání duhovek za poměrně nepříznivých podmínek při použití snímků získaných z různých vzdáleností a různých kamer.[2]



Obr. 2: Rozhodovací prostředí pro rozpoznávání duhovek za velice příznivých podmínek (snímání stejnou kamerou ze stejné vzdálenosti a za stejných světelných podmínek) [2]

4.3.6 Geometrie tváře

V tomto případě se jedná o formu s nižší identifikační jednoznačností. Metoda je založená na bezkontaktním snímání na poměrně velkou vzdálenost. Klíčové je v této metodě brát v potaz také mimiku tváře a projevy emocí, kdy je nutno rozlišování dělit právě dle vnějších projevů a emocí. „*Lidská tvář není při pořizování snímků pro vytvoření biometrické předlohy nebo následnou identifikaci uživatele vždy dokonale stejná. Pomineme-li vliv času na vzhled tváře, například i teplota okolí může ovlivnit barvu kůže. Právě tento fakt může ovlivnit výsledky systémů založených na barevných vlastnostech obličeje. Také rozdíly mezi jednotlivými lidskými rasami mohou detektory tváří zmást.*“[64]

Rozvíjení této disciplíny je uskutečňováno již od šedesátých let dvacátého století a mnoho bezpečnostních složek využívá této identifikace dodnes. Na rozdíl od většiny ostatních způsobů biometrických identifikací je možné tuto identifikaci v praxi využívat i skrytým způsobem. Kontrolovaná osoba tak ani nemusí vědět o skutečnosti, že je právě prověřována. Tento způsob skryté identifikace se v praxi rozšiřuje zejména u bezpečnostních složek, které

mají za úkol chránit vytyčený perimetr, například metro. Takto skrytá identifikace se využívá především z preventivních důvodů nebo pro odhalení hledané osoby, například teroristy či zločince.[65]

Celý proces se rozlišuje na dva zásadní, stejně důležité kroky – detekce tváře a rozpoznání tváře.

Detekce tváře – detekce se provádí na základě rozpoznávaní samotného obličeje, zda se nachází na scéně vůbec nějaký obličej, žádný obličej či více obličejů. Scénou se rozumí například aktuální kamerový přenos do monitorovacího centra na letišti. Tento krok, ačkoliv se jeví jako banalita, není zcela jednoduchý. Algoritmus musí rozpoznat tvář při působení různých ovlivňujících faktorů – vzdálenost obličeje (čím větší vzdálenost, tím menší počet rozpoznatelných identifikačních prvků – technická omezenost snímače), pozadí scény (nutno oddělit obličej od okolí, přesná rozpoznatelnost obličeje), případné pohyby na scéně (rychlost, stabilita snímacího prvku), výrazy, orientace tváří a osvětlení celé scény (ve viditelném světelném spektru se silně ovlivňují rysy, kontury obličeje – velký vliv stínů). Algoritmus musí mimo jiné být schopen rozeznání také reálné tváře, patřící živé osobě. [65]

Rozpoznávání tváře – rozpoznávání se provádí na základě extrakce biometrických charakteristik z detekovaného obličeje. V tomto příkladu dochází k identifikaci neznámé osoby na letišti v monitorovacím centru a na základě této identifikace dochází k vyhodnocení, zda je osoba potenciální hrozbou, hledanou osobou či nikoliv. [65]

V celém automatizovaném procesu identifikace se rozlišují následující přístupy:

- 2D a 3D přístupy (dvourozměrné, třírozměrné)
- černobílé, barevné, infračervené spektrum obrazů
- pohledy čelní (en face) a z boku (profilové)
- statické obrazy
- dynamické obrazy (sekvence obrazů - změna pohybu/výrazu/emoce tváře) [65]

4.3.7 Sítnice oka

Biometrická identifikace jedince prostřednictvím oční sítnice je velmi spolehlivou metodou, kdy speciální kamera snímá vzorek sítnice. Jedná se ovšem o nákladný snímač a proces snímání není příjemný pro jedince. Tento způsob zabezpečená používají opravdu místa, kde je nutné velmi dobře zabezpečit přístup k informacím. *„Snímače sítnice lidského oka se jeví jako nejbezpečnější biometrická identifikační metoda. Neexistují chybná přijetí a*

chyba se také jeví být nemožnou. Nicméně pravděpodobnost chybného odmítnutí je vysoká, a proto tato metoda nemůže být jednoduše obecně přijatelná. Proto se použití této metody redukuje jen na velmi bezpečné kontrolní systémy jako jsou jaderné reaktory nebo vojenská zařízení.“[66]

Kamera pro snímání sítnice má stejný úkol jako retinoskop používaný očními lékaři [Hi99, Da]. Zdroj světla ozařuje oční sítnici a odražené světlo dopadá do kamery. Světlo vychází z retinoskopu v soustředěném svazku paprsků tak, aby jej oční čočka zaostřila na bod na sítnici. Sítnice odráží část světla zpět k oční čočce, která opět soustřeďuje světelné paprsky. Toto světlo opouští oko pod stejným úhlem, jakým do oka vstupuje, což je proces, který se nazývá retroodraz. Světlo odražené od sítnice je snímáno kamerou.[67]

Aby bylo zajištěno, že kruhový snímek sítnice je centrován na kruhové jamce a uživatel je pod paprsky snímače po celou dobu snímání, tak je uživateli ukázán cíl, na který se má zaměřit/zaostřit. Takovým cílem může být například řada jednoduchých optických sítí v ohniskových vzdálenostech –7, –3, 0 a +3 dioptrie. Pro většinu uživatelů alespoň jedna z těchto optických sítí bude zaostřena bez ohledu na to, zda jsou krátkozrací nebo dalekozrací.[67]

Snímání sítnice trvá asi 10 až 15 sekund. Po tuto dobu uživatel nesmí hýbat hlavou, musí mít oči široce otevřeny a soustředit se na zelený cíl. Snímání se provádí ze vzdálenosti asi 2 cm od kamery, před snímáním je nutné sundat brýle.

Při srovnávání je referenční záznam konvertován do pole o stejném počtu prvků jako má nasnímané pole. Po normalizaci je spočítána korelace polí za pomoci ekvivalentu Fourierovy korelace v časové doméně. Stupeň shody je dán hodnotou korelace pro nulový časový posun. Možné hodnoty zahrnují +1,0, což je perfektní shoda, až po –1,0, což je úplná neshoda. Zkušenost ukazuje, že hodnoty nad 0,7 již mohou být považovány za shodu.[68]

4.3.8 Dynamika podpisu

V této metodě se měří rozdíly v tlaku a rychlost psaní na základě čehož jsou osoby identifikovány. Jedná se o metodu, která je používána od 80. let 20. století.

Písmo je výsledkem mnoha složitých psychologických a fyziologických procesů, které postupně formují jeho individuální charakter. Individualizací písma se dá rozumět jeho odchylování od vyučované školní normy a zároveň jeho jedinečnost v porovnání s ostatními lidskými jedinci. Názory na vlivy, které ovlivňují individualizaci písma se liší. Taktéž není jednotný názor na to, odkdy je proces vývoje písma ukončen. Tomilin uvádí, že psaní jako složitý pohybový návyk obsahuje:[69]

- technický návyk psaní neboli správný způsob psaní (správné držení psacího prostředku, poloha papíru apod.),
- grafický návyk neboli schopnost zobrazovat tvary písmen rychle a jasně,
- pravopisný návyk, tj. znalost pravidel používání grafémů při vyjádření obsahu textu. [25]

Automatizovaná verifikace založená na rozpoznávání podpisu prověřované osoby patří k nejpraktičtějším způsobům ověřování lidské identity. Podpis jako takový nemůže být ztracen, odcizen nebo zapomenut a jeho základní výhoda spočívá v jeho přirozenosti při používání v běžném životě, při každodenních operacích. Ověřování podpisu může být proto využito v klasických oblastech, jako jsou kontrola přístupu, bezpečnost, nebo finanční či kontraktační transakce.[69]

V principu existují dva základní typy systémů na rozpoznávání osoby podle podpisu: on-line systémy a off-line systémy.[69]

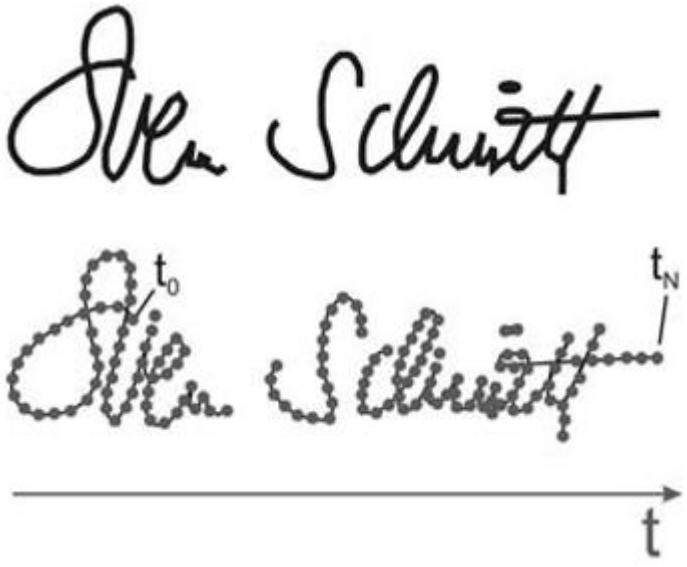
U off-line systémů je podpis napsán na papír a digitální data o jeho obrazu jsou získána snímáním nebo skenováním kamerou. Vstupní data jsou pak obrázkem podpisu s příslušnými souřadnicemi x, y pro každý bod podpisu. Off-line systémy na verifikaci osob podle vlastního podpisu nejsou dnes pro automatizované zpracování zcela vhodné. Důvodem je nevhodnost samotného principu porovnání dvou statických obrazů podpisu (předkládaného vzoru s referenční šablonou), který je v dnešní době běžně dostupných skenovacích a kopírovacích zařízení náchylný k podvrhům falzifikátů. Není totiž pracné a nesnadné získat skenováním, kopírováním nebo fotografováním podpis dané osoby, za níž se chce podvodník vydávat a tento falzifikovaný vzorek poté předložit snímacímu zařízení verifikační aplikace, viz obr. 3.[70]

Automatizované prostředky pro verifikaci osoby podle podpisu se zpravidla skládají ze tří základních etap, kterými jsou:

- předzpracování,
- extrakce biometrických charakteristik,
- vyhodnocování.[71]

Obr. 3: Statické charakteristiky podpisu[65]

On-line verifikační systémy založené na podpisu se od off-line systémů liší způsobem získávání dat. U on-line systémů se data získávají v reálném čase pomocí digitalizačního tabletu nebo pomocí speciálního pera. Dynamické, on-line systémy tedy nezískávají jenom obrazovou podobu podpisu, ale také dynamické charakteristiky. Tyto dynamické charakteristiky odrážejí unikátní zvyky podpisující se osoby a je tedy mnohem složitější falšovat podpis. K dynamickým vlastnostem patří tlak pera v jednotlivých bodech trajektorie, rychlost psaní, pořadí psaní jednotlivých částí podpisu apod. On-line systémy jsou obvykle chápány nebo representovány pomocí matematické časové funkce F(t), viz. obr. 4. [72]



Obr. 4: Podpis je u on-line systémů vnímán jako množina funkcí závislých na čase. V každém okamžiku t jsou snímány dynamické hodnoty v konkrétních bodech. [64]

„Zařízení na dynamický podpis se často mylně zaměňují s pojmy jako je elektronický podpis (šifrovaný klíč) nebo se zařízeními na snímání podpisu jako obrazu. Z ručního podpisu lze tak elektronicky zjistit tah, tvar a tlak při psaní, což lze použít pro verifikaci osoby. Jednotlivé druhy zařízení se liší dle výrobce způsobem užití a jeho významem, ale mají shodnou vlastnost použití technologií citlivých na dotek, tedy PDA záznamníků nebo digitalizačních tabulí.“[73]

4.3.9 Geometrie ruky

Tato metoda zakládá na tom, že lidská ruka je také specifická co do její šíře, tloušťky prstů a dalších specifik. K tomuto účelu jsou využívány moderní skenery, která využívají infračervené LED diody.[2]

Uživatel klade ruku na horizontální plochu skeneru, opatřenou speciálními fixačními kolíčky tak, aby při každém snímání byla poloha ruky (její orientace) pokud možno vždy stejná.[2]

Vlastní snímání je realizováno obvykle CCD2 digitální kamerou s přibližně 32 000 body (pixely). Skener snímá pouze siluetu dlaně s prsty, nikoliv otisky jednotlivých prstů, dlaně, jizvy nebo barvy. Snímaní je černobílé a připomíná promítání ruky položené např. na desku zpětného projektoru. Jeden obraz je snímán se shora kolmo na rovinu snímací desky, druhý obraz pomocí postranního zrcadla vykresluje pohled na dlaň z boku. Tato metoda je v praxi známá jako ortografické snímkování (skenování).[2]

V procesu porovnávání referenční šablony se šablonou právě sejmutou skenerem se porovnávají vzdálenosti předem určených bodů (velikosti úseček). Jejich počet a umístění záleží na konkrétním biometrickém zařízení daného výrobce. Vyhodnocuje se pak skóre porovnání těchto identifikačních markantů. U nových technologií lze předpokládat využití obecnějšího vyhodnocení podobenství dvou obrazů (referenčního a právě nasnímaného). V tomto případě je obrazem kontura (silueta) ruky snímaná ze shora a z boku.[2]

4.3.10 Hlas

V této metodě dochází ke snímání zabarvení a tónu hlasu. „*Systémy pro tento typ biometrie pracují s hlasem dvěma základními způsoby – pomocí tzv. hlasových hesel (vocal*

password) nebo pomocí průběžné analýzy hlasu (free speech). V prvním a technologicky jednodušším případě jde o vyhodnocení předem známé věty vyřčené klientem. Výhodou je, že na obsahu věty nezáleží, dokonce mohou mít všichni klienti stejné heslo – například „Můj hlas je moje heslo“. Protože systém může klientovi heslo i připomenout, nehrozí rizika spojená se zapomenutím nebo zveřejněním hesla. Komunikace s operátorem pak pokračuje až po ověření.“[74]

4.4 Kombinace metod při identifikaci osob

Jistou variantou pro identifikaci osob je pochopitelně jejich vzájemná kombinace. Kde selže jedna metoda, je možné ověřit totožnost jinou cestou. Mnoho firem používá vícestupňové ověřování, takže je zabezpečení daných informací a přístupu k nim podstatně vyšší. Jedná se tedy o případy, kdy je cílem maximální zabezpečení daného objektu. Nejčastěji se jedná o kombinaci předmětu a hesla nebo předmětu a biometriky.

5 PRAKTICKÁ ČÁST

Měření identifikace osob bylo prováděno v laboratoři technické fakulty ČZU. Měření bylo prováděno na dvou čtečkách a měřilo se za jakou rychlost dokáže čtečka přijmout uživatele. Měřilo se na pěti osobách, v laboratoři byl použit panel, na kterém byl připevněn LED pás, který měl přísvit modré, červené, bílé a zelené barvy. Osvětlení laboratoře činilo 80 luxů.

Barevné spektrum je lidským okem viditelná část elektromagnetického spektra o vlnových délkách 380 až 750 nm (odpovídá frekvenci 790 - 400 THz). Odpovídající vlnové délky ve vodě a v ostatních prostředích závisí na indexu lomu. Tento rozsah vlnových délek je nazýván viditelné světlo nebo jednoduše světlo. Oko je nejcitlivější na elektromagnetické záření vlnové délky 555 nm (540 THz), tj. na zelenou barvu.

Před počátečním testováním bylo nutno připravit testovací panel. Jedná se o panel, ke kterému, jsou přidělány jednotlivá čtecí zařízení. Panel byl vytvořen ke snadnější manipulaci a k nastavení stejných okolních podmínek při měření. Měření bylo prováděno na rodině, spolužácích a blízkých osobách. Pro testování byly přizvány osoby jak mladší 50 let, tak starší 50 let. měření probíhalo po dobu celého jednoho roku.

Při měření se bude klást důraz na hodnoty FRR a především za jakou dobu a zda vůbec čtečka identifikuje osobu za předpokladu že na daného jedince bude svítit bílý, červený, modrý a zelený přísvit o různé intenzitě.

Pro výpočet FRR byl použit vzorec:

$$FRR = \frac{Ppv}{Cppv} \times 100 \text{ [\%]} \quad (1)$$

kde: FRR – pravděpodobnost chybného zamítnutí,

Ppv – počet porovnání vzorů osoby A vedoucí k neshodě,

Cppv – celkový počet porovnání vzorů osoby A.

5.1 Identifikační systém MultiBio 700

Zařízení multiBio 700, verifikuje na základě snímání obličeje a otisků prstů. Ve světě je tento způsob verifikace jeden z nejznámějších možností biometrické identifikace. Pro identifikaci využívá tvar tváře, a to její základní rysy (oči – umístění na obličeji, vzdálenost mezi nimi a jejich velikost, dále ústa, nos, čelisti a lícní kosti). Tyto rysy slouží k vytvoření

předlohové šablony, díky které pak dochází k určení či ověření dané osoby. Také je zde možnost samozřejmě dle užití použít ID kartu či PIN. 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 zmiňovaných zálohovacích zařízeních. Toto zařízení využívá 3D technologie. Je možno nahrát až 2000 otisků prstů a 400 tváří. Nově použitý algoritmus VX7.0 je mnohem rychlejší (rychlost verifikace je < 2 sekundy) a má větší kapacitu. Výhodou tohoto přístroje pro identifikaci je, že pro uživatele není nepříjemný, jelikož identifikace tváře je naprosto bezkontaktní. Pokud uživatel není v tomto ohledu tolik náročný, lze zařízení použít i jako kontaktní (otisk prstu). Jediné, co musí uživatel při bezkontaktní identifikaci dodržet, je postavení hlavy – nesmát se, nenatáčet se, neklopit hladu vpřed ani vzad. [76,77]

Čtečku lze použít i pro venkovní přístupový systém. Může na ni být připojen alarm, zamykání, odchodové tlačítko, magnetický kontakt dveří, domovní zvonek, temperový snímač. [76,77]

Obr. 5: Čtečka MultiBio 700 [75]

5.2 Identifikační systém I FACE 302

Přístroj IFACE 302, je díky jednotlivým komponentům určen do jakéhokoli prostředí (tmavé, světlé, zima, teplo, aj.). Do zařízení byl integrován vysokorychlostní procesor o velikosti 630 MHz a infračervená kamera s velmi vysokým rozlišením. Stejně jako u minulého zařízení se i u tohoto může rozšiřovat o heslo, ID kartu a otisk prstu. Tento systém obsahuje i funkci webserver, což je správa prostřednictvím internetového prohlížeče. Čtečku lze zapojit jako dveřní senzor, odchozí tlačítko, elektrický zámek, alarm i jako drátový dveřní zvonek. Zařízení je schopné pojmout 100000 záznamů, z toho 5000 otisků prstů a 400 skenů obličeje. 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). Stejně jako u jakékoliv jiné čtečky je zde potřeba, aby uživatel dodržel pravidla snímání. [76,77]

Obr. 6: Čtečka I FACE 302 [75]

5.3 Postup při měření spolehlivosti čtecích zařízení

Měření probíhalo celkem na pěti osobách. Při měření jsme postupně měnily barvy přísvitu (modrá, červená, bílá a zelená). Intenzita byla měřena luxmetrem v Luxech. Hlavním parametrem bylo za jak rychlou dobu dokáže čtečka MultiBio 700, I FACE 302 rozpoznat uživatele, na kterého bude působit předem vybrané barevné spektrum.

V laboratorní místnosti bez přísvitu barevného světla byla intenzita 82 luxů. Na připraveném panelu, který má za úkol vyzařovat různé typy barevného světla byla vybrána barva v pořadí: modrá, červená bílá, zelená a jejich tři intenzity viz přílohy 1 a 2. Po vybrání konkrétního přísvitu a jejího odstín byl před čtečku přizván uživatel, aby proběhla jeho identifikace. Poté co uživatel stanul před čtečkou byly spuštěny stopky a měřilo se, jak rychle identifikační zařízení uživatele rozpozná.

V tabulkách viz příloha 1 a 2 je v krajním sloupci z leva zaznamenána barva použitého barevného spektra a tři druhy intenzity zaznamenané luxmetrem v Luxech. Ve zbývajících sloupcích se nacházejí čtyři měření času, za kterou dokáže čtečka rozpoznat uživatele (t_1 až t_4), na jednotlivé odstíny barev měřené v sekundách, viz tabulky 1 až 5 v přílohách.

6 ZHODNOCENÍ VÝSLEDKŮ

Cílem práce bylo ověřit kvalitu dvou čteček (Multibio 700 a I FACE 302) zda splňují parametry vhodné pro identifikaci osob. Od výrobce bylo uváděno, že obě čtečky by měly rozpoznat obličej již do jedné sekundy. Pro kladnou identifikaci stačí čas do dvou sekund.

Na grafu 1 a 2 je zobrazen průběh za jakou průměrnou dobu v sekundách byly čtecí zařízení (MultiBio 700 a I FACE 302) schopné rozpoznat tvář uživatele (osoba 1 až osoba 5) a tabulkový údaj od výrobce za jakou dobu by tvář měla být rozpoznána. Na obou grafech jsou zaznamenány průměrné časy úspěšného rozeznání daného uživatele, na kterého působil přísvit vybrané barvy přísvitu o dané intenzitě viz. příloha 1 a 2. Na ose x leží seznam osob a na ose y jsou průměrné časy identifikovaného uživatel. K naměřeným hodnotám je přidán i údaj od výrobce, za jakou doby by měla být osoba identifikována, která činí 2 sekundy. Pro obě čtecí zařízení byla analýza prováděna samostatně.

Na grafu 1 je měření identifikace čtecího zařízení MultiBio 700. Z výsledků vyplývá, že čtecí zařízení MultiBio 700 nedokázalo ani jednu osobu pod kterýmkoliv přísvitem identifikovat pod 2 sekundy. Jako nejpříznivější přísvit pro tuto čtečku byl přísvit zelené barvy, u kterého byla délka identifikace v průměru 4,48s. Nicméně ani tak nesplňuje čas určený výrobcem pro kladnou identifikaci. Naopak nejhorší barva přísvitu byla bílá barva, u které průměrný čas pro identifikaci vyšel 6,98s.

Na grafu 2 je měření identifikace čtecího zařízení I Face 302. Z výsledků vyplývá, že stejně jako u předchozího čtecího zařízení, ani tohle zařízení nesplňuje údaje dané výrobcem pro kladou identifikaci do dvou sekund. Jako nejpříznivější barvou přísvitu byla naměřená modrá barva, jejíž průměrný čas pro identifikaci byl 4,15s. Stejně tak ale ani pod touto barvou přísvitu nebylo čtecí zařízení schopné identifikovat uživatele pod dvě sekundy. Naopak nejhorší barvou přísvitu byla červená barva jejíž průměrný čas pro identifikaci byl 5,74s.

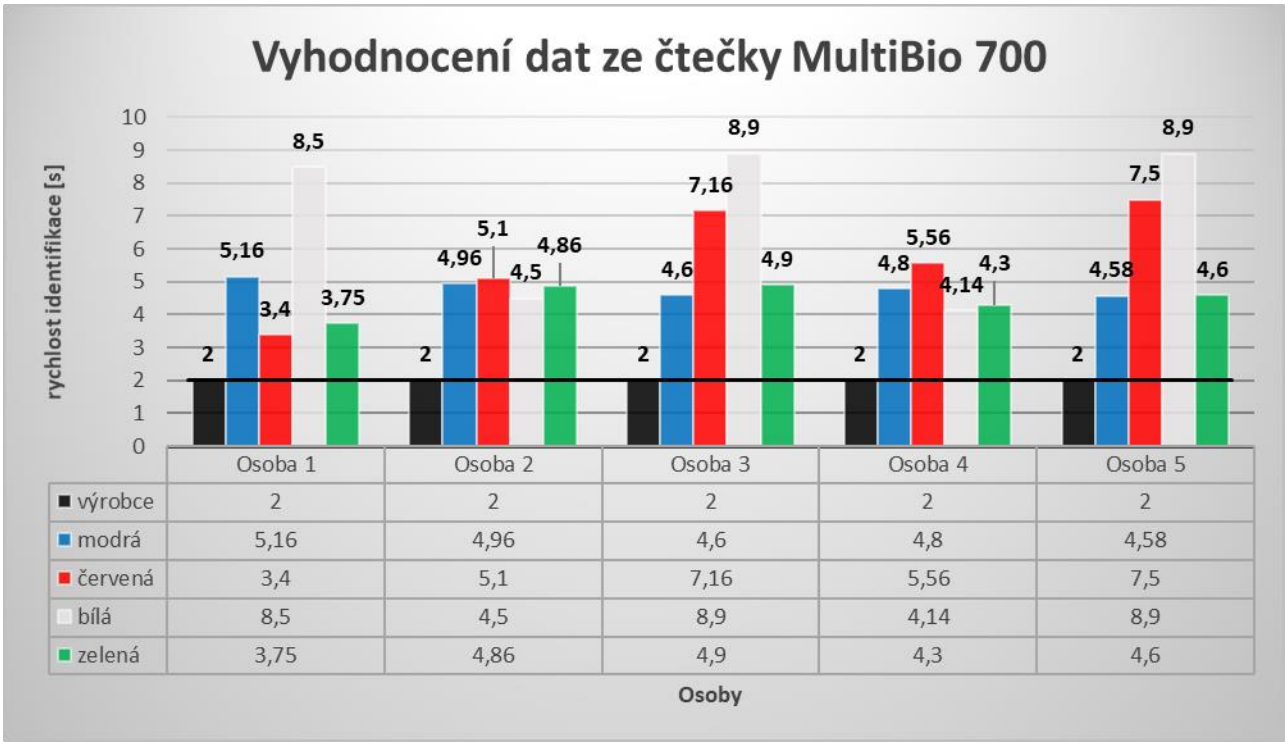
Z grafu 1 a 2 vyplývá, že ani jedno zařízení se pro rychlou identifikaci moc nehodí. Dále je zžemé, že pro čtecí zařízení MultiBio 700 se bílý přísvit nehodí. Pokud je tedy možnost bílému přísvitu v místnosti pro identifikaci se vyhnout a nahradit ho přísvitem zeleným. Rozdíl mezi těmito časy je 2,5s. Tento čas je pro uživatel příznivější. Pro čtecího zařízení I FACE 302 vyšly lepší výsledky, ale i tam je lepší vyměnit červený přísvit za přísvit modré barvy, kde časový rozdíl činil 1,59s.

Dalším cílem bylo ověřit procentuálně kolikrát může nastat možnost chybného zamítnutí (FRR). Tento stav nastává, když čtecí zařízení nesprávně odmítne uživatele, který je v systému evidovaný, tudíž čtecí zařízení musí uživatele přijmout.

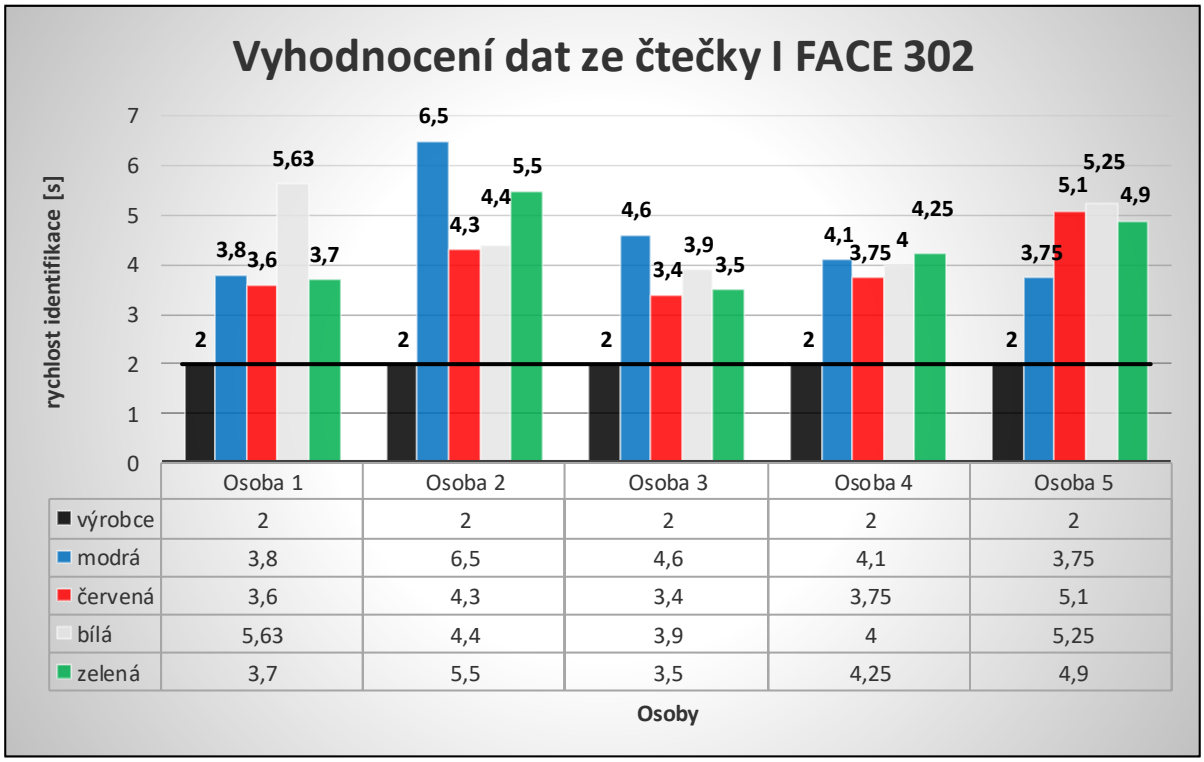
Na grafu 3 a 4 je vyobrazeno kolikrát v průměru byl uživatel nesprávně zamítnut pro jednotlivý druh barvy. Pro vypočítání chybného zamítnutí (FRR) jsme použili vzorec pro výpočet pravděpodobnosti chybného zamítnutí (viz vzorec 1) a do proměnných byly dány data z tabulek v přílohách 1 a 2. Na ose x jsou jednotliví uživatelé a na ose y jsou procenta chybných zamítnutí. Pro obě čtecí zařízení byla analýza prováděna odděleně. Z grafů 3 a 4 je patrné, kolik procent bylo chybného zamítnutí uživatele pro danou barvu u každého jedince.

Z grafu 3 a 4 vyplývá že obě čtecí zařízení neměli větší problém s chybným zamítnutím. Na čtecím zařízení Multibio 700 (viz graf 3) byl problém s chybným zamítnutím pouze u osoby 2. Tato osoba se od ostatních osob lišila věkovým rozdílem. Osobě 2 bylo v době měření devadesát let. Jelikož s identifikováním ostatních osob čtecí zařízení MultiBio 700 nemělo problém, je tedy možné, že toto zařízení může mít problém s identifikováním starších osob. U čtecího zařízení I Face 302 takový problém nenastal. Jediný případ chybného zamítnutí bylo u první osoby pod barvou bílého přísvitu.

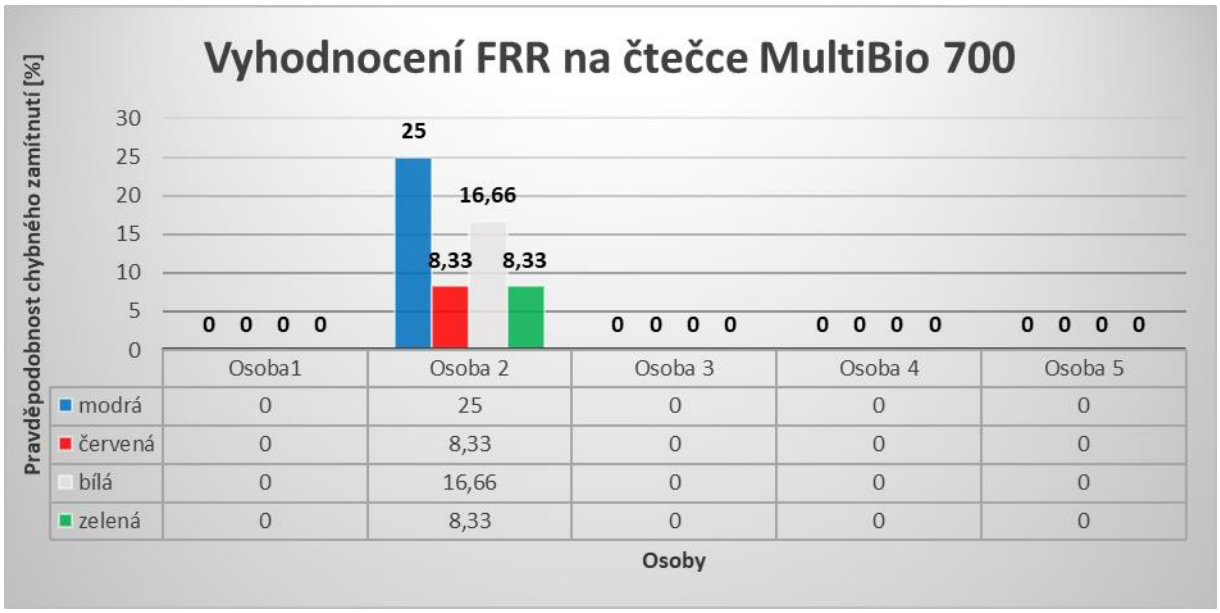
Jelikož výsledky FRR vyšli pozitivně pro obě čtecí zařízení, je možné z toho dle hlediska použít obě zařízení v provozu. Jenom u čtecího zařízení MultiBio 700 je třeba dávat pozor u osob staršího věku. Zde je ale možno brát v úvahu i chybu lidského faktoru na straně uživatele.



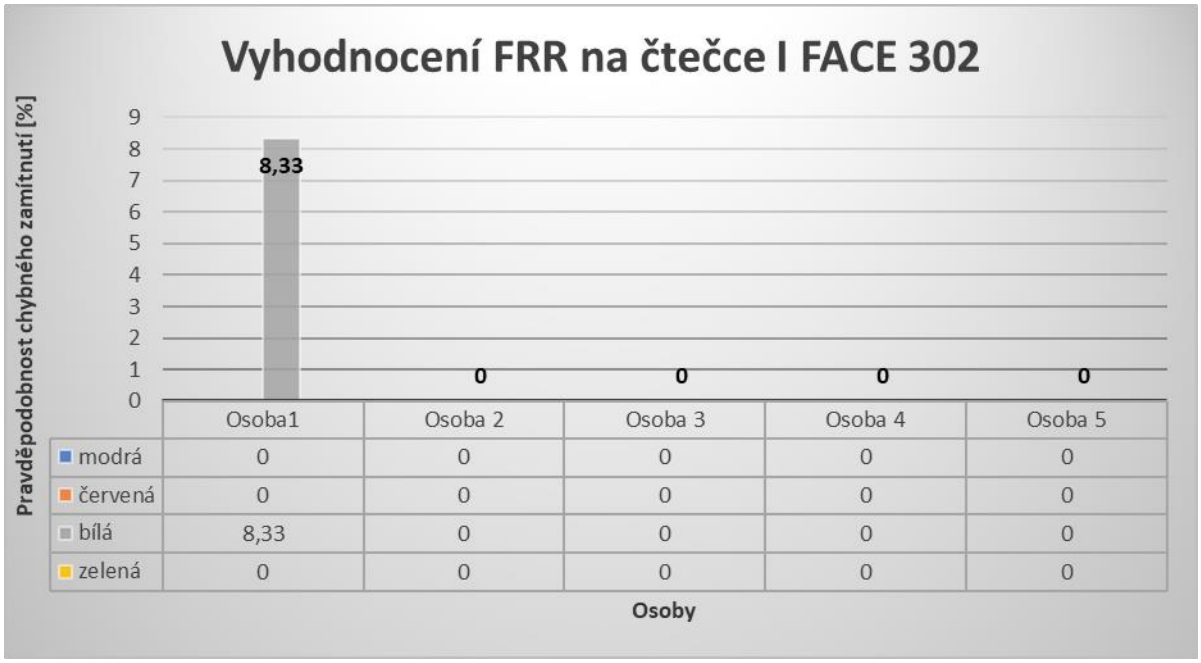
Graf 1 Vyhodonocení dat ze čtečky MultiBio 700



Graf 2 Vyhodnocení dat ze čtečky I FACE 302



Graf 3 Vyhodnocení FRR na čtečce MultiBio 700



Graf 4 Vyhodnocení FRR na čtečce I FACE 302

7 ZÁVĚR

Tato bakalářská práce se zabývala především vytvořením přehledné studie zabývající se technologií identifikace člověka a jejích možnosti. Tato technologie se vyvíjí velice rychlým tempem a to, co v minulosti používaly pouze ty největší firmy či objekty, jež zabezpečovaly cenné informace, dnes mají prakticky všechny možné objekty či služby. Všechny jmenované technologie ze třetí kapitoly jsou stále využívány s tím, že se liší jejich pozitiva a negativa, náklady na jejich pořízení, jejich životnost, správnost identifikace. Stále častěji se využívá biometrické identifikace a jako příklad je možné uvést také moderní mobilní telefony či notebooky, takže se již nejedná pouze o společnosti, ale zabezpečení údajů jedince. Dnes má většina lidí vše umístěno na "síti", ať už se jedná o rodinné fotografie, soubory z práce, osobní korespondenci či všelijaké sociální sítě. Všechny tyto služby využívají zabezpečení, takže to jen dokládá jejich důležitost, a také důvod, proč je nutné je stále modernizovat.

Další část práce obsahuje praktická měření a testovaní pořízených biometrických identifikačních systémů. V této měřící části je pozornost zaměřena na biometrii 3D skenu obličeje. Provádí se zde měření spolehlivosti biometrických systémů a jejich vzájemné porovnání, jelikož měření se podrobila 2 čtecí zařízení.

Nejprve bylo nutné všechny uživatele zadat do systému. Poté následoval proces měření. Od výrobců je uvádění, že přijetí uživatel by mělo být do 2 sekund.

Z výsledků měření je vidět, že ani jedna z obou čteček v průměru nesplnila údaje, které byly poskytnuty výrobcem. Většina měření lehce nebo i výrazně přesáhla čas uváděný výrobcem pro kladnou identifikaci, která měla být pod dvě sekundy, viz přílohy 1 a 2. Po zprůměrování výsledků je jisté že pod dvě sekundy se nevešlo ani jedno z měření, viz graf 1 a 2.

Za značnou nevýhodu obou čteček by se dala považovat i rychlost a způsob nahrávání osob do databáze čtečky. U obou čteček byl průběh pomalý i přesto, že obě čtečky navigovali jedince, jak si mají stoupnout, otočit hlavu a podobně.

Z měření lze vyvodit, že barevný přísvit až na nesplnění časů pro identifikaci nedělal čtečkám vážný problém. Jediné, v čem měla čtečka Multibio 700 problém bylo, když se před ní postavila starší osoba, viz příloha 1, tabulka 2. Tento typ čtečky měl problém z počátku sejmout obličej onoho jedince. Jelikož u ostatních osob měření proběhlo úspěšně, lze předpokládat, že ovlivnění prostředí přísvitem se může vyloučit a problém přenést na jinou část.

Tento problém byl dále rozebrán pro měření pravděpodobností chybného zamítnutí (FRR). Po dosazení všech proměnných do rovnic a vyobrazení výsledků do grafu (graf 3 a 4), je možno vidět, při které barvě bylo procentuálně dosaženo nejvíce chybného zamítnutí. Z grafu vyplívá, že nejvíce chybných zamítnutí má modrá barva dále barva bílá, červená a nakonec zelená.

Měření, které se nezdařilo nebo výchylky v prodlevě času by mohli být částečně ovlivněny přísvitem místnosti barevným spektrem, ale také učením se s čtečkami nebo špatné natočení hlavy daného jedince.

Z výsledků měření se dá říct, že obě čtecí zařízení se dají použít do provozu i s jiným barevným spektrem, než je sluneční záření. Na základě výsledků se dá usoudit, že existují rychlejší a modernější čtečky, které budou vykazovat větší přesnost a rychlost, což je uživatelsky přijatelnější. Do rozsáhlejších provozů se tedy tyto dvě čtecí zařízení moc nehodí a bylo by přijatelnější zvolit modernější čtecí zařízení, která umějí identifikovat uživatele rychleji a to i za pohybu.

REFERENCE

1. LOCKE, John.: Esej o lidském rozumu, 2012, Praha: Oikoymenh, 767 str., ISBN 978-80-7298-304-9
2. Roman Rak, Václav Matyáš, Zdeněk Říha a kol. „*Biometrie a identita člověka ve forenzních a komerčních aplikacích*“, Grada Publishing, 2008, ISBN 8024763923
3. SZALÓ, Csaba. Sociologie formování sociálních identit. In: SZALÓ, Csaba, NOSÁL, Igor. Mozaika v rekonstrukci: formování sociálních identit v současné střední Evropě, Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2003, s. 15
4. BRUBAKER, Rogers. Ethnicity without groups. 1st Harvard University Press pbk. ed. Cambridge, Mass: Harvard University Press, 2006, s. 33.
5. JANDOUREK, Jan. Sociologický slovník. Vyd. 1. Praha: Portál, 2001, s. 104
6. HUNTINGTON, Samuel P. Kam kráčíš, Ameriko?: krize americké identity. Vyd. 1. Praha: Rybka Publishers, 2005, s. 32.
7. HUNTINGTON, Samuel P. Kam kráčíš, Ameriko?: krize americké identity. Vyd. 1. Praha: Rybka Publishers, 2005, s. 38.
8. CLARKE, R.: Human Identification in Information Systems: Management Challenges and Public Policy Issues, Information Technology & People, 1982, MCB UP Ltd, ISSN: 0959-3845
9. ČSOB. InternetBanking 24 Celá banka ve vašem počítači. [online]. [cit. 2017-11-06]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking- 24#zabezpeceni
10. KOMERČNÍ BANKA. Certifikáty. [online]. [cit. 2017-11-06]. Dostupné z: https://www.kb.cz/cs/primebankovnictvi/certifikaty/vyzvednuti-a-prodlouzeni-certifikatu/
11. DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat, 2004, Brno: Computer Press, 190 str., ISBN 80-251- 0106-1
12. §13 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech
13. NEUWIRT, K.: Elektronická identifikace občana v systémech E-Government, 2008, cit. 2017.11.11, dostupné na: http://www.estat.cz/data/publikace_karel_neuwirt_1.pdf
14. Všeobecná zdravotní pojišťovna: Typy průkazů zdravotního pojištění, 2015, cit. 2017.11.11, dostupné na: https://www.vzp.cz/poskytovatele/informace-pro-praxi/typy-prukazu-zdravotniho-pojisteni

15. Ministerstvo zahraničních věcí: Jak žádat o cestovní pas s biometrickými prvky („ePas“), 2014, cit. 2017.11.11, dostupné na: http://www.mzv.cz/cairo/cz/viza_a_konzularni_informace/vydavani_cestovnich_dokladu_cr/jak_zadat_o _cestovni_pas_s_biometrickymi.html
16. NEUWIRT, K.: Elektronická identifikace občana v systémech E-Government, 2008, cit. 2017.11.11, dostupné na: http://www.estat.cz/data/publikace_karel_neuwirt_1.pdf
17. MATES, P., SMEJKAL, V.: E-governement v českém právu, 2006, Praha: Linde Praha a.s., 244 str., ISBN 80-7201-614-8
18. BARTÍK, V., JANEČKOVÁ, E.: Ochrana osobních údajů v aplikační praxi, Vybrané otázky. Praktická právnická příručka, 2013, Praha: Linde Praha a.s., 311 str., ISBN 978-80-86131-96-2
19. §2, §4, §5 zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících předpisů
20. Nahradil zákon č. 20/1966 Sb. o péči o zdraví lidu
21. Národní zdravotnický informační systém je celostátní informační systém veřejné správy, který je určený ke zpracování osobních údajů o z
22. Zákon č. 372/2011 Sb, o zdravotnických službách a podmínkách jejich poskytování
23. NEUWIRT, K.: Elektronická identifikace v projektech elektronického zdravotnictví (S využitím podkladů členů pracovní skupiny pro eIdentitu eStat.cz – EFEKTIVNÍ STÁT, 2010, cit. 2017.11.12, dostupné na: http://docplayer.cz/1232946-Identifikace-v-projektech.html
24. §18 zákona č. 500/2004 Sb., správní řád
25. BARTÍK, V., JANEČKOVÁ, E.: Ochrana osobních údajů v aplikační praxi, Vybrané otázky. Praktická právnická příručka, 2013, Praha: Linde Praha a.s., 311 str., ISBN 978-80-86131-96-2
26. § 55b zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
27. §28 zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů
28. BARTÍK, V., JANEČKOVÁ, E.: Ochrana osobních údajů v aplikační praxi, Vybrané otázky. Praktická právnická příručka, 2013, Praha: Linde Praha a.s., 311 str., ISBN 978-80-86131-96-2
29. BARTÍK, V., JANEČKOVÁ, E.: Ochrana osobních údajů v aplikační praxi, Vybrané otázky. Praktická právnická příručka, 2013, Praha: Linde Praha a.s., 311 str., ISBN 978-80-86131-96-2

30. MATES, P., SMEJKAL, V.: E-governement v českém právu, 2006, Praha: Linde Praha a.s., 244 str., ISBN 80-7201-614-8, srov. BARTÍK, V., JANEČKOVÁ, E.: Ochrana osobních údajů v aplikační praxi, Vybrané otázky. Praktická právnická příručka, 2013, Praha: Linde Praha a.s., 311 str., ISBN 978-80-86131-96-2
31. Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, [ONLINE], dostupné na: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910
32. Internetový portál Ministerstva vnitra České republiky dostupné z: http://www.mvcr.cz/egovernment.aspx
33. Mates, P., Smejkal, V.: E-governement v českém právu, 2006, Praha: Linde Praha a.s., 244 str., ISBN: 80-7201-614-8
34. Mates, P., Smejkal, V.: E-governement v českém právu, 2006, Praha: Linde Praha a.s., 244 str., ISBN: 80-7201-614-8
35. LECHNER, T.: Analysis of Some Impacts of Regulation eIDAS on Public Bodies in Czech Republic, Proceedings of the 11th International Scientific Conference: Publice Economics and Administration 2015, Ostrava, ISBN: 978-80-248-3839-7
36. MACKOVÁ, A., ŠTĚDROŇ, B.: Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem, 2009, Praha: Wolters Kluwer ČR, 528 str., ISBN: 978-80-7357-472-7
37. STORK 2.0 vytváří jednotný prostor pro elektronickou identifikaci a autentizaci v Evropě, STORK 2.0, Internetový portál Ministerstva vnitra ČR, [ONLINE], dostupné 27.2.2016, dostupné na: http://www.mvcr.cz/clanek/stork-2-0-vytvari-jednotny-prostor-pro-elektronickou-identifikaci-aautentizaci-v-evrope.aspx
38. ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Část 11- 1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 33 4593.
39. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576.
40. ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Část 11- 1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. 1. vyd.

Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 33 4593.

41. ČSN EN 60839-11-2. Poplachové a elektronické bezpečnostní systémy - Část 11- 2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. Třídící znak 334593.
42. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576
43. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576
44. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576
45. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576
46. Autentizace a identifikace uživatelů. ÚVT MU zpravodaj [online]. Brno [cit. 2017-22-14]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html
47. MGR. ING. RADOMÍR ŠČUREK, PH.D. Biometrické metody identifikace osob v bezpečnostní praxi [online]. [cit. 2017-11-19]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf, s. 5
48. Autentizace a identifikace uživatelů. ÚVT MU zpravodaj [online]. Brno [cit. 2017-22-14]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html
49. Autentizace a identifikace uživatelů. ÚVT MU zpravodaj [online]. Brno [cit. 2017-22-14]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html
50. UHLÁŘ, Jan. Technická ochrana objektů [online]. Vyd. 1. Praha: Vydavatelství Policejní akademie České Republiky, 2006, 246 s. [cit. 2017-11-14]. ISBN 80- 725-1235-8.
51. UHLÁŘ, Jan. Technická ochrana objektů [online]. Vyd. 1. Praha: Vydavatelství Policejní akademie České Republiky, 2006, 246 s. [cit. 2017-11-14]. ISBN 80- 725-1235-8.

52. MGR. ING. RADOMÍR ŠČUREK, PH.D. Biometrické metody identifikace osob v bezpečnostní praxi [online]. [cit. 2017-11-19]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf, s. 5
53. NORMAN, Thomas L. Electronic access control. Waltham: Elsevier, c2012, 1 online zdroj (xx, 423 s.). ISBN 978-0-12-382029-7. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=407848
54. NORMAN, Thomas L. Electronic access control. Waltham: Elsevier, c2012, 1 online zdroj (xx, 423 s.). ISBN 978-0-12-382029-7. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=407848
55. NORMAN, Thomas L. Electronic access control. Waltham: Elsevier, c2012, 1 online zdroj (xx, 423 s.). ISBN 978-0-12-382029-7. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=407848
56. NORMAN, Thomas L. Electronic access control. Waltham: Elsevier, c2012, 1 online zdroj (xx, 423 s.). ISBN 978-0-12-382029-7. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=407848
57. Čipové karty. Karlin [online]. , 6s. [cit. 2017-11-17]. Dostupné z: http://www.karlin.mff.cuni.cz/~kadlcak/lessons/pozn/CipoveKarty.pdf
58. Co je NFC. Patronpro [online]. , 1 [cit. 2017-11-17]. Dostupné z: https://www.patronpro.cz/co-je-nfc/
59. Co je NFC. Patronpro [online]. , 1 [cit. 2017-11-17]. Dostupné z: https://www.patronpro.cz/co-je-nfc/
60. Co je NFC. Patronpro [online]. , 1 [cit. 2017-11-17]. Dostupné z: https://www.patronpro.cz/co-je-nfc/
61. Co je NFC. Patronpro [online]. , 1 [cit. 2017-11-17]. Dostupné z: https://www.patronpro.cz/co-je-nfc/
62. MGR. ING. RADOMÍR ŠČUREK, PH.D. Biometrické metody identifikace osob v bezpečnostní praxi [online]. [cit. 2017-11-19]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf, s. 6
63. Biometrie otisku prstu [online]. [cit. 2017-11-19]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

64. Biometrie oka [online]. [cit. 2017-11-19]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/
65. Biometrie obličeje [online]. [cit. 2017-11-19]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/
66. Trisul, [online]. Dostupný z WWW: http://www.trisul.cz/bezpecnost-autentizace-autorizace/
67. Robert Hill: „Retina Identification“, in BIOMETRICS: Personal Identification in Networked Society, Kluwer academic Publisher 1999.
68. Ravi Das: „An Application of Biometric Technology: Retinal Recognition“, http:// www.htgadvancesystems.com/Advance/articles/Retinal_Recognition.html.
69. Huang, K. and Yan, H.: „*On-line Signature Verification Based on Dynamic Segmentation and Global and Local Matching*“, Optical Engineering, 1995.
70. Harrgreaves, G., Wilson, P.: „*Grafologický slovník*“, Schneider, Brno 1983.
71. Porada, V. a kol.: „*Kriminalistika*“, Brno, CERM, 2001, ISBN 80-7204-194-0.
72. Biometrie oka [online]. [cit. 2017-11-19]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/
73. MGR. ING. RADOMÍR ŠČUREK, PH.D. Biometrické metody identifikace osob v bezpečnostní praxi [online]. [cit. 2017-11-19]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf, s. 32
74. RYBA, Albert. *Možnosti využití hlasové biometrie pro ověření zákazníků* [online]. 2014 [cit. 2017-11-19]. Dostupné z: http://www.ictmanazer.cz/2014/09/moznosti-vyuziti-hlasove-biometrie-pro-overeni-zakazniku/
75. NÍDLOVÁ, V. „Biometrické identifikační systémy“. Praha, 2013. 44 s. Teze doktorské disertační práce na Technické fakultě České zemědělské univerzity na Katedra
76. ZKSoftware, [online]. Dostupný z WWW: http://www.zktechnology.com/ProductDetail.aspx?cat=Face+Readers&series=Face+a nd+Fi ngerprint+T%26A+Readers&product=Multibio+700
77. Comfis, [online]. Dostupný z WWW: http://www.comfis.cz/uvod/shop/terminaly

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM VZORCŮ

SEZNAM PŘÍLOH