Identifikační biometrické systémy

Biometric identification systems

Pavel Vyoral

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Pavel VYORAL**
Osobní číslo:	**A08681**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Identifikační biometrické systémy**

Zásady pro vypracování:

1. **Seznamte se s problematikou identifikace na základě biometrických znaků.**
2. **Popište jednotlivé metody identifikace, technické parametry.**
3. **Popište současný stav a perspektivy požadavků na využití biometrických údajů.**
4. **Navrhněte vhodný identifikační přístupový systém pro malou firmu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Laucký L. Technologie komerční bezpečnosti I. Skripta UTB ve Zlíně**
2. **Čandík M. Objektová bezpečnost II. Skripta UTB ve Zlíně**
3. **Křeček S. a kol. Příručka zabezpečovací techniky. Tiskárna Blatná, 2. Vydání.**
4. **Rak, R. Biometrie a identita člověka ve forenzních a komerčních aplikacích, 2008. ISBN 978-80-247-2365-5.**
5. **Porada, V. Kriminalistika. Brno: CERM, 2001. 746 s. ISBN 8072041940.**
6. **Ščurek, R. Biometrické metody identifikace osob v bezpečnostní praxi., 2008. Dostupný z WWW: [http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf]**

Vedoucí bakalářské práce: **Ing. Milan Navrátil, Ph.D.**
Ústav elektroniky a měření

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

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

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

První část práce je zaměřená na základní informace o autentizaci, podrobnější informace o biometrii a její význam, dělení, historii, kritéria, postupy a využití. Dále jsem zde zabýval problematikou nejpoužívanějších biometrických metod. Je zde rozebrán technologický princip každé metody, dělení, kritéria a jejich výhody a nevýhody. V praktické části jsem se zaměřil na kritéria při výběru vhodného biometrického přístupového systému a jejich současný stav na trhu. V neposlední řadě práce obsahuje návrh docházkového systému pro menší fiktivní firmu.

Klíčová slova:

Biometrie, autentizace, přístupový systém, identifikace.

ABSTRACT

The first part of this work is focused on basic information about authentication, a more detailed information about the importance of biometrics, its classification, history, criteria, procedures and applications. Furthermore, I focused on the most widely used biometric methods. There is elaborated technological principle of each method, separation, criteria, advantages and disadvantages. In the practical part, I focused on the criteria for selecting the appropriate biometric access control system and its status on the current market. The work also includes design of the attendance system for the small fictive company.

Keywords:

Biometrics, authentication, access kontrol systém, identification.

Děkuji panu Ing. Milanu Navrátilovi, Ph.D. za jeho cenné rady, ale také za jeho ochotu a trpělivost při vedení mé bakalářské práce.

„Technický vývoj směřuje vždy od primitivního přes komplikované k jednoduchému“

Antoine de Saint-Exupér

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V teoretické části práce jsem se zaměřil na objasnění problematiky biometrie, což je vědní obor založený na jedinečnosti každé osoby. V dnešní době, kdy je na trhu vysoká konkurence přístupových a identifikačních systémů založených na různých principech, je zapotřebí vybrat ten nejvhodnější pro daný objekt, jak za účelem kontroly vstupů, tak kontroly docházky uživatele. Na první pohled je biometrie u přístupových systémů díky své složitosti stále málo využívaná a místo ní je volen přístup pomocí karet, hesel či tokenů. Tam je velkou nevýhodou nutnost pamatovat si heslo nebo nosit u sebe neustále kartu, kterou musíme při ztrátě složitě deaktivovat a vyřídit si novou, což je někdy časově náročné, pokud firma nevlastní svůj vlastní poměrně nákladný přístroj na výrobu karet.

V poslední době nabírá biometrie vzrůstající směr a to i díky velké konkurenci na trhu a klesající ceně. Velkou výhodu u biometrické identifikace tvoří fakt, že se ověřuje totožnost osoby a ne pouze přítomnost správné karty nebo znalost hesla. Tím odpadá potřeba u sebe nosit kartu a pamatovat si heslo. Biometrie má velkou škálu využití, od základní funkce zámku na dveřích nebo přihlášení do systému, až po vyhledávání podezřelých osob při velkých davových shromážděních.

Při vysvětlování funkce jednotlivých metod se zaměřím na ty nejvyužívanější a nejběžnější. Každá metoda má své výhody, nevýhody a různé způsoby provedení. To jak samotná identifikace osob probíhá, bude popsáno v dalších částech této práce.

V praktické části bakalářské práce se zaměřím na kritéria pro výběr správné biometrické metody a nepřesnosti s nimi spojené. Při správném výběru je potřeba zvážit klady a zápory každé metody a vybrat ten nejlepší způsob zabezpečení vstupů, mimo jiné také v závislosti na lokaci a finančních podmínkách. Jde o přehled biometrických metod a rozbor těch nejpoužívanějších. U každé metody bude vysvětleno, na jakém principu je založena a definovány její parametry. Existují také možnosti neoprávněného překonání biometrických systémů, ale neexistuje žádná stoprocentní možnost, jak je obelhat.

V poslední části bude uveden jeden z mnoha možných návrhů přístupového systému pro malou nebo střední firmu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

1.1 Autentizace

Autentizaci můžeme rozdělit podle způsobu identifikace do tří skupin dle toho, co dotyčný vlastní (např. čipovou kartu) nebo co zná (např. heslo, PIN) a třetím způsobem je využití biometrie. V biometrii upřednostňujeme termín verifikace.

Tab. 1. Přehled autentizačních metod [Vlastní zpracování]

	Medium	Stupeň zabezpečení	Nevýhody a výhody
Co znám	hesla	nejnižší	snadné zapomenutí nebo vyzrazení, jsou přenosné
Co vlastním	tokeny	vyšší	snadné zničení, jsou přenosné
Kombinace	hesla a tokenů	vysoký	možnost zapůjčení tokenu, vyzrazení hesla, jsou přenosné
Biometrie		nejvyšší	jsou nepřenosné, nelze je ztratit ani předat

1.2 Verifikace

Český výraz pro pojem verifikace je ověřování. Jde o proces porovnávání získaného biometrického obrazu se šablonou uživatele v databázi.

2 BIOMETRIE

Pochází z řeckých slov bios (život) a metron (měření). Přibližně před sto lety začala vznikat biometrie, která pomohla odhalit statisíce zločinů. Postupem času se metody vyšetřování značně zdokonalily a v dnešní době se používají ty nejmodernější technologie. Biometrie je metoda autentizace, která je založená na rozpoznávání jedinečných fyziologických znaků lidského těla nebo projevu člověka. Základní myšlenkou této moderní a progresivní technologie je jedinečná a nezaměnitelná charakteristika jedince.

Nejnovější technologie umožňují člověka identifikovat automaticky, rychle a spolehlivě. Biometrie se nejčastěji využívá k ověření totožnosti před povolením vstupu. Výhodou je možnost kombinace s ostatními autentizačními způsoby a je velmi silnou metodou pro autentizaci samotnou i z hlediska obrany proti zneužití. Je zde možnost kombinace s hesly nebo zdvojení více biometrických metod, velká odolnost vůči krádežím nebo monitorování (na rozdíl od karet a hesel) a navíc uživatel nemusí mít obavu, že např. zapomene heslo či PIN.

Dříve se otisky prstů a biometrie používaly jen pro malé bezpečnostní aplikace za speciálními účely, hlavně kvůli vysoké ceně kvalitních snímacích zařízení. V roce 1998-2000 došlo k výraznému poklesu cen u snímačů otisků prstů a tím je možné v dnešní době tyto snímače všeobecně rozšířit. U dalších technologií budeme muset nejspíše na větší dostupnost ještě počkat. [6]

2.1 Historie biometrie

17. října roku 1902 byl v pařížské ulici du Faubourg Saint - Honoré zavražděn sluha zubaře Joseph Reibel. K případu byl povolán vedoucí oddělení rejstříku zločinců Alphonse Bertillon. Syn statistika vychovávaný v obdivu k exaktním vědám, který začínal jako obyčejný kopista na prefektuře, se v té době už těšil značné vážnosti. Pro vyhledávání zločinců vynalezl novou metodu zvanou antropometrie. Antropometrie spočívala v měření výšky a šířky obličeje, rozměrů pravého ucha a čísla levého chodidla. Díky údajům získaných touto technikou bylo možné odhalit recidivisty, kteří vystupovali pod falešnou identitou.

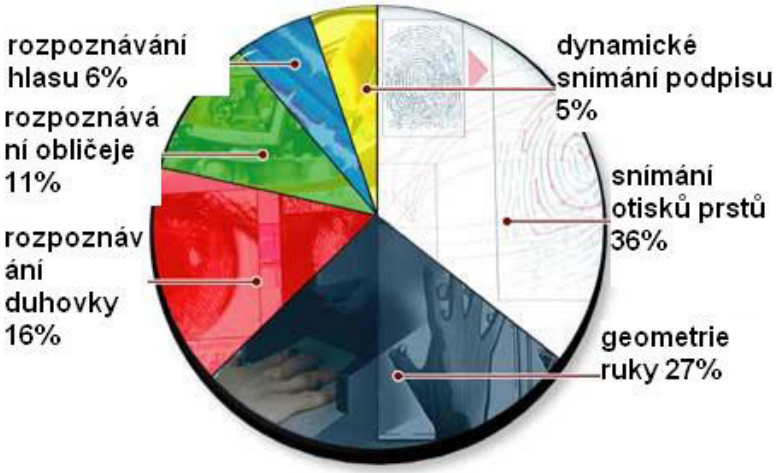
V zájmu pořádku přidával Bertillon ke svým antropometrickým záznamům i čtyři otisky pravé ruky, ačkoli v úspěšnost daktyloskopie, kterou před ním zkoušeli již Angličan Herschel a Argentinec Vucetich, nevěřil. V případu zavražděného Josepha Reibela nebyla Bertillonovi jeho metoda nic platná, protože neexistovali žádní podezřelí. Byl proto nucen použít otisky prstů z místa činu. Šlo o palec, ukazováček, prostředníček a prsteníček, které se otiskly na sklenici. Bertillon je porovnal se všemi otisky z rejstříku. Zjistil, že se shodují s otisky jistého Henriho Léona Scheffera zvaného „Dělostřelec George“. O šest dní později byl Scheffer zadržen v Marseille a k vraždě se přiznal. Použití daktyloskopie k objasnění zločinu znamenalo průlom v tehdejších vyšetřovacích metodách a vyvolalo velký ohlas.

Ačkoli jsou v poslední době zaváděny nové techniky, například analýza DNA, daktyloskopie je stále metodou číslo jedna.

2.2 Dělení biometrických systémů

Biometrii lze uplatnit na určitých částech a vlastnostech lidského těla. Obecně je dělíme na dvě základní skupiny a to na fyziologické, které má člověk již při narození a jsou pro něj charakteristické a na behaviorální, které se vyvíjejí postupem času. Mezi jednotlivé základní biometrické technologie patří:

- otisky prstů,
- oční duhovky,
- oční sítnice,
- geometrie obličeje,
- geometrie ruky,
- DNA,
- dynamiky stisku kláves,
- charakteristiky hlasu,
- charakteristiky písma.



Obr. 1. Porovnání využívání hlavních typů biometrie [9]

Tab. 2. Porovnání hlavních vlastností biometrie (podle General Accounting Office USA) [9]

	Otisk prstu	**Obličej**	**Dlaň**	**Duhovka**
Podíl chybných odmítnutí	0,2 – 36 %	3,3 – 70 %	0 – 5 %	1,9 – 6 %
Podíl chybných přijetí	0 – 8 %	0,3 – 5 %	0 – 2,1 %	pod 1%
Doba transakce	9 – 19 s	10 s	6 – 10 s	12 s
Velikost šablony	250 – 1000 B	84 – 1300 B	9 B	512 B
Počet hlavních výrobců	25+	2	1	1
Náklady na zařízení	nízké	střední	střední	vysoké
Faktory ovlivňující výkon	špinavé, suché a horké prsty	různá osvětlení obličeje, sluneční brýle, make-up a další změny ve vzhledu obličeje	zranění ruky artritida pocení	špatné vidění odrazy

2.3 Využití biometrie

V praxi se této metody využívá hlavně k:

- sledování docházky,
- autorizaci přístupů,
- bezpečnému přihlašování (tj. eliminace ztráty hesel).

Tab. 3. Oblasti využití biometrických identifikačních metod [5]

Bezpečnostní oblast	Oblast státní zprávy	Výpočetní technika obecně a komerční sféry
• Kriminalistika • Vězeňství • Boj proti zločinu obecně • Osoby v pátrání • Osoby v pohřešování • Sledování zájmových osob • Zpravodajství • Fyzická ostraha a zabezpečení strategických objektů	• Zdravotní pojištění • Sociální pojištění • Školství • Oprávněnost přistupovat k volbám, účastnit se referenda, sčítání lidu,.. • Vydávání řidičských oprávnění, osobních dokladů, ID karet, pasů a víz	• Bankovnictví, finančnictví a pojišťovnictví • Personální legendy • Přístupy k prostředkům počítačových informačních a telekomunikačních zařízení • Obecná ochrana proti podvodům a zpronevěrám • Řízení k platebním kartám a bankomatům • Identifikace zákazníků, zaměstnanců, návštěvníků • Zvýhodněné služby pro stálé zákazníky • Elektronické transakce • Elektronický podpis • Různé služby a marketing

2.4 Hlavní kritéria biometrických identifikačních metod

Při výběru správné biometrické metody je potřeba zvážit tato kritéria:

- rychlost,
- přesnost,
- velikost šablony,
- cena,
- velikost snímacího zařízení,
- dotěrnost,
- režim činnosti,
- vliv na soukromí,
- provozní podmínky,
- kulturní a náboženská omezení.

3 DAKTYLOSKOPIE - OTISKY PRSTŮ

Jde o nauku, která se zabývá kožními papilárními liniemi na prstech, dlaních a ploškách chodidel. Průběh těchto linií je pro každého charakteristický a z určité části i dědičný. Díky této vlastnosti můžeme v kriminalistice snadněji identifikovat osoby. Existuje asi přibližně 60 odlišných forem otisků prstů, které mohou být kombinovány do jednoho otisku prstů.

Člověk se potí, jeho kůže se odlupuje a přichází neustále do kontaktu s různými druhy špíny, s prachem, tukem, krví a podobně. Když se pak člověk dotkne nějakého předmětu nebo osoby, působí tato směs na bázi potu, která ulpívá na ruce, jako tiskařská barva. Konečky prstů po sobě zanechají otisky. Jde o reprodukci reliéfu kůže sestávajícího z drobných vystouplých čar zvaných papilární linie. Kresba papilárních linií je u každého jedince na světě jiná. Liší se dokonce i u jednovaječných dvojčat, na rozdíl od DNA, kterou mají stejnou.[24]

Mezi výhody daktyloskopie patří:

- přesnost,
- snadná dostupnost,
- malé rozměry čtecího zařízení,
- nízká pořizovací cena.

Do nevýhod daktyloskopie řadíme:

- strojní zpracování otisku prstu u některých jedinců,
- kulturní a náboženské omezení, kde některé země nedovolí využívat otisky prstů na jiné než policejní účely.

3.1 Historie daktyloskopie

K prvním vědcům, kteří začali studovat papilární linie patřil Jan Evangelista Purkyně, nicméně první praktické použití našel v roce 1877 William Herschel v Indii, kdy s jejich pomocí kontroloval, aby osoby pobírající vojenskou penzi ji obdržely pouze jednou. V této době se také používala pro stvrzování oficiálních dokumentů. Existenci tohoto způsobu „podepisování“ objevili už v sedmém století Číňané. [13]

3.2 Metody daktyloskopie

Biometrické identifikační systémy určené k daktyloskopii, skenují otisky prstů opticky, kapacitně nebo tepelně.

- Tepelné skenování vytváří obraz detekcí teplotních rozdílů.
- Optické skenování využívá přímého optického snímku.
- Kapacitní skenování měří nepatrné změny elektrického náboje na povrchu prstu.

3.2.1 Optoelektronické snímače

Princip činnosti

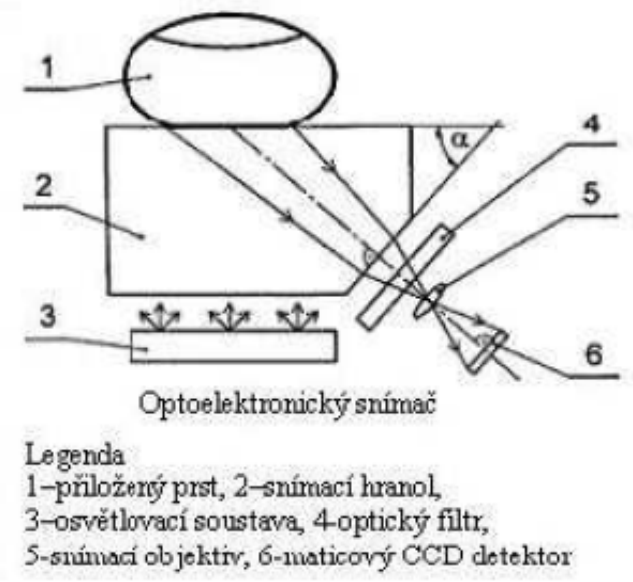
Jsou ideální především pro rozpoznání založené na markantech tzn. na speciálních útvarech na otisku prstu, které tvoří papilární linie. Optoelektronický snímač je založen na rozdílném odrazu světla, kde optický snímač zachycuje digitální zobrazení otisku pomocí viditelného světla. Obraz otisku se přenese na maticový CCD detektor a je následně digitalizován, posléze dále předán pro zpracování obrazu otisku. Pod vrstvou, kde se přikládá prst tzv. dotekový povrch, je vrstva fosforu, která osvětluje celou plochu prstu. Odražené světlo od povrchu prstu prochází luminoforní vrstvou k CCD maticovému detektoru a tam se vytvoří obraz otisku. Jednoduše řečeno - z papilárních linií se světlo odráží, z rýh mezi nimi se neodráží.

Nevýhody

- nečistoty prstu nebo jeho poškození může způsobit špatné vykreslení,
- větší rozměry čtečky nás můžou limitovat při implementaci do malých a přenosných zařízení.

Výhody

- vysoká kvalita,
- odolnost proti statickým výbojům,
- minimální vliv okolního prostředí. [8]



Obr. 2. Princip optoelektronického snímače [20]

3.2.2 Kapacitní snímače

Princip činnosti

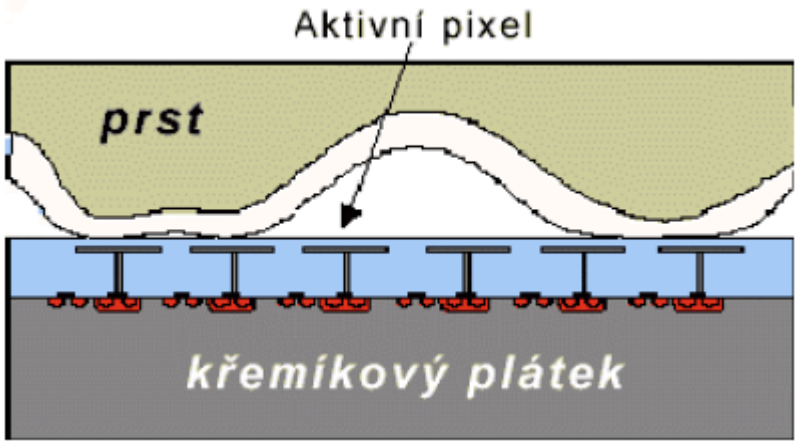
Zde je využíváno rozdílu kapacity mezi deskou snímače a povrchem prstu tzn., že snímač rozeznává vyvýšeniny nebo prohlubně. Snímač se skládá ze dvou desek a otisk se tak získává v digitální formě. Pro načtení obrazu přiložíme prst na citlivou plochu osazenou velkým množstvím elektrod. Ty převedou kapacitně otisk prstu na digitální obraz, který se dál zpracovává. Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor.

Nevýhody

- doba životnosti je malá z důvodu zničení snímače vlivem statické elektřiny,
- snímače je většinou nutné měnit v rozmezí 3 let.

Výhody

- malý rozměr,
- jednoduchý princip funkčnosti,
- vysoká kvalita,
- nízká pořizovací cena. [8]



Obr. 3. Princip kapacitního snímače [11]

3.2.3 Teplotní snímače

Princip činnosti

Tyto snímače obsahují malý citlivý pyrodetektor a ten snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostoru mezi nimi. Pro získání obrazu otisku prstu musíme přejíždět prstem přes citlivou plochu. Výsledný obraz otisku je ve formě digitálních pásů. Následně se digitální obrazy skládají do výsledného obrazu otisku.

Nevýhody

- nízká kvalita,
- problémy s algoritmy pro zpracování markant,
- snímání otisků lze pouze pohybem prstu a proto každé sejmutí může být z jiné části prstu,
- obtížné vytváření databáze otisků,
- nejsou vhodné pro použití v přístupových systémech. [8]

3.2.4 Elektroluminiscenční snímače

Princip činnosti

Tyto snímače využívají speciální vrstvy reagující na tlak způsobený luminiscenčním efektem. Zde je důležité z hlediska funkčnosti eliminující vrstva, která filtruje světlo z míst, kde na ní tlačí papilární linie. Zpracování je zajištěno pomocí fotodiod a výsledný výstup je v digitální formě. Jedná se o extrémně suchý otisk, ale kvalita při opakování je srovnatelná.

Nevýhody

- menší odolnost proti mechanickému poškození,
- náchylnost proti znečištění prachem či vodou.

Výhody

- miniaturní rozměry,
- dobrá cena,
- dobré rozlišení,
- kvalita je srovnatelná, i když se jedná o extrémně suchý otisk. [8]

3.2.5 Radiofrekvenční snímače

Princip činnosti

Práce radiofrekvenčních snímačů spočívá v připojení generátoru střídavého signálu na 2 rovnoběžné desky. Na plochu snímače a na plochu otisku prstu. Z důvodu, že je vlnová délka mnohem větší než délka desek, se zde vyskytuje pouze složka elektrického pole a to bez přítomnosti magnetického pole. Pokud tedy jedna z desek bude náš otisk prstu, tak se tvar pole změní a bude kopírovat tvar linií výběžků a prohlubní. Vodivého prostředí mezi prstem a plochou je docíleno vodivou plochou kolem každého snímače a tím nám odpadá problém velmi suchých prstů, jelikož se pracuje s živou tkání těsně pod povrchem pokožky.

Zvlněním pole, které je způsobeno přiloženým otiskem prstu, dopadá na senzory signál s rozdílnou velikostí signálu, výběžky mají větší signál a prohlubně signál nižší. Kapacitní senzory tak měří rozdílnou permitivitu mezi výběžky a prohlubní. Při problému snímání z vysušené nebo poškozené kůže je pořizováno několik snímků, které jsou postupně optimalizovány až do doby přesného přijetí nebo odmítnutí snímků. [8]

Výhody

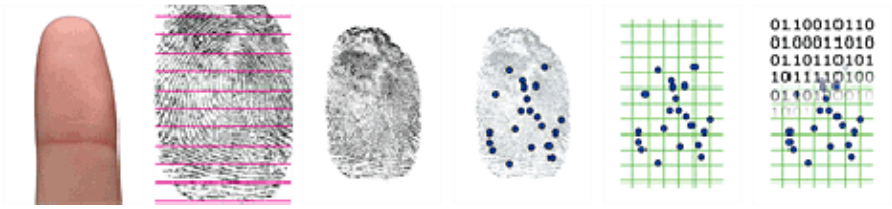
- nečistoty v prohlubních nám nedělají problém,
- schopnost snímání vysušené nebo částečně poškozené kůže.

3.2.6 Příklad postupu zpracování otisku

Pro zvětšení produktivity a kvality práce se zde nasazuje výpočetní technika. Člověk přejede prstem po čidle, kde je hlavní součástkou jeden mikročip, který je pokryt teplotně

citlivou vrstvou sestavenou ze 14 000 zobrazovacích prvků. Poté nám čip konvertuje nepatrné teplotní rozdíly, zaznamenané na 50-100 obrazových řezů. Následně speciální software přibližně za desetinu sekundy složí řezy do celkového snímku. Snímek lze uložit do databáze a zobrazit na monitoru.

Počítač zpracuje snímek pomocí složitého algoritmu a vytvoří se digitální identifikační kód. Přibližně pět procent lidí nemůže poskytnout věrohodné otisky z důvodu dočasných nebo trvalých (mozoly, ekzém, chybějící prsty, …). Přesnost současných přístrojů využívaných k rychlé kontrole je šest promile mylných odmítnutí a jedno promile mylných přijetí.



Obr. 4. Postup zpracování otisku prstu [12]

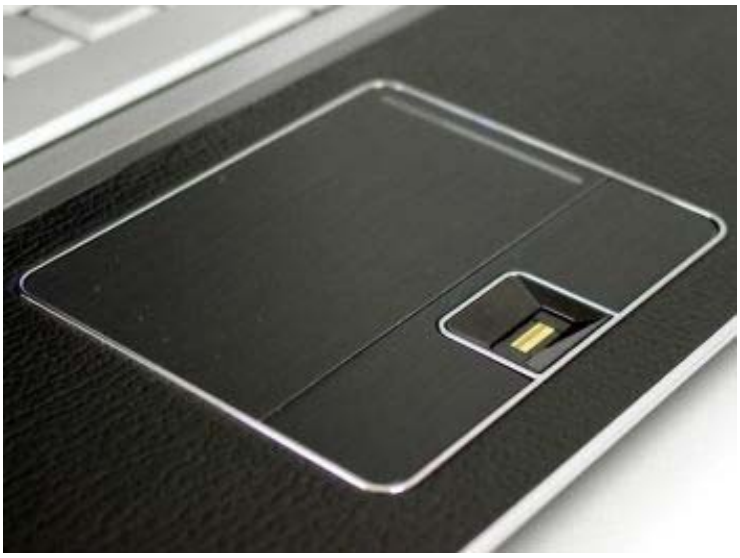
3.3 Využití daktyloskopie v praxi

Daktyloskopie má velký rozsah využití. S jedním z nejběžnějších využití se můžeme setkat u přihlašování k některým počítačům. V dnešní moderní době místo toho, abyste do systému psali uživatelské jméno a heslo, a nebo jste se identifikovali nějakou kartou, je možnost pouze přiložení prstu na čtečku. Stále větší počet počítačů, hlavně notebooků a jiných přenosných PC zařízení už obsahuje integrované čtečky otisků prstů. U zařízení, které neobsahují tuto čtečku je možnost připojit její externí USB provedení. Tyto čtečky otisků prstů lze používat k identifikaci a ověřování uživatelů.

Do nedávné doby neexistovala v systémech Windows žádná podpora pro biometrická zařízení nebo pro aplikace podporující biometriku. Z tohoto důvodu byli výrobci počítačů donuceni ke svým produktům dodávat software, který zajišťoval podporu biometrických zařízení. Tím bylo způsobeno poměrně složité používání a správa pro správce. Novinka posledního operačního sytému od firmy Microsoft systém Windows 7 obsahuje architekturu WBF (Windows Biometric Framework), která přímo podporuje čtečky otisků prstů a další biometrická zařízení. To umožňuje uživatelům řídit dostupnost biometrických zařízení a možnost jejich použití přihlašování k místnímu počítači nebo doméně přímo

v ovládacích panelech a dále využití v nastavení Zásad skupin a mnoho dalších možností. [7]

Tohle vše nám může umožnit snadnější přihlašování k počítačům a přidělovat zvýšená oprávnění prostřednictvím nástroje Řízení uživatelských účtů. Hlavní výhodou je následné rozsáhlé využití v sítích.



Obr. 5. Příklad čtečky otisku prstu u přenosného počítače [10]

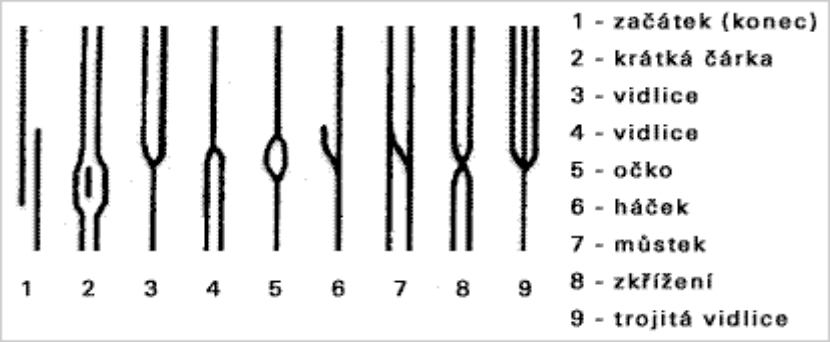
3.4 Papilární linie

Jsou základním prvkem pro daktyloskopii. Při důkladném pozorování kůže na vnitřní straně prstů, dlaních nebo prstech na nohou a chodidel uvidíme tzv. výstupky a prohlubně, které vytvářejí složité obrazce. Zobrazené obrazce (linie) bývají souvislé a vyvýšené, kde je jejich výška 0,1 mm až 0,4 mm a šířka 0,2 mm až 0,7 mm.

Papilární linie se vzájemně kříží, rozvětvují, mění směr, spojují apod. Takto vytvářené obrazce, se nazývají dermatoglyfy. Papilární linie nenalezneme pouze u lidí, ale také u primátů a to na všech čtyřech končetinách a u některých druhů opic i na vnitřní straně ocasu. [24]

3.4.1 Markant

Důležitou vlastností papilárních linií je tzv. markant, tím je myšlena jakákoliv změna v průběhu linií. Rozvržení markantů je pro každého člověka typické, nezaměnitelné a to dokonce i u dvojčat na rozdíl od DNA, která je u dvojčat stejná. Vyhledávání shodných otisků je založeno na tvaru, vzdálenosti a umístění markantů. [24]



Obr. 6. Ukázka základních typů markantů [24]

3.4.2 Vznik papilárních linií

Linie vznikají hned během vývoje plodu v děloze. Embryo je u matky vystaveno množství nejrůznějších tlaků a drobných nehod, které ho nijak neohrožují, ale formují mimo jiné i povrch jeho kůže. A díky tomu se upravuje vznik papilárních linií a již po šestém měsíci těhotenství už se dále nevyvíjejí. Posléze už nám zůstávají stejné po celý život. Změna je pak už jen možná díky hlubokému poranění. Linie nám zdrsní kůži a umožňují nám lepší zachycení a kvalitnější hmat.

4 OČNÍ DUHOVKY

Oční duhovka je pro nás stejně jedinečná jako otisk prstu. Jedná se o sval uvnitř oka, který reaguje na velikost čočky, neboli zaostření oka v závislosti intenzity světla dopadajícího přímo na oko. Jde o barevnou část oka, kde zabarvení odpovídá množství meletoninového pigmentu uvnitř svaloviny. Zbarvení i struktura oční duhovky je nám geneticky daná, ale její vlastní vzorkování nikoliv. Vývoj duhovky je dán během prenatálního růstu plodu a její vzorkování je náhodné a to znamená, že je pro každého člověka jedinečné a to i u dvojčat. Při porovnání obou duhovek jedné osoby bylo zjištěno, že má každá jiné vzorkování a to napomáhá přesnosti těchto identifikačních systémů. Metoda autentizace pomocí oční duhovky patří k těm nejpřesnějším vůbec, protože počet vzorů duhovky je vyšší než 400. [23]

Obr. 7. Lidské oko při skenování duhovky [8]

4.1 Vznik využití oční duhovky pro identifikaci osob

Rozpoznávání osob pomocí oční duhovky je poměrně nová metoda. Poprvé byl tenhle způsob oficiálně představen v roce 1994 a to díky americkému Úřadu pro jadernou bezpečnost pod vedením Dr. Johna Daugmana.

4.2 Analýza charakteristik oční duhovky

Pro snímání lidského oka je vyžadována velice kvalitní digitální kamera a infračervené osvětlení oka. Zařízení na první pohled podobné kameře nám zaznamená soubor několika snímků oka přibližně v intervalu několika sekund. Tato kamera obsahuje objektiv, který projektuje snímky na prvek s nábojovou vazbou neboli CCD. Údaje jsou následně

digitalizovány a odeslány k analýze do procesoru, kde jsou pomocí speciálního softwaru zpracovány.

Software nám v první řadě vyhledá údaje o očním víčku a odstraní jej, následně lokalizuje rozhraní duhovky, zornice a očního bělma. Jsou vyhodnocena a zachována pouze data týkající se duhovky. Duhovka je zmapována bod po bodu pomocí souřadnicového systému. Skenery si dokážou poradit, když se duhovka na světle stáhne, aby zúžila zornici a zaclonila oko, nebo když se ve tmě uvolní, aby rozšířená zornice pustila na sítnici více světla. Vygenerované údaje o jasnosti každého bodu jsou zaznamenány v 512-ti bitovém kódu. Díky výsledné analýze unikátních charakteristik duhovky jedince jsou získaná data uložena
v digitálním tvaru do databáze.

Následné identifikace osob jsou provedeny totožným způsobem jako při záznamu, je vytvořen digitální kód a ten je porovnáván s kódy v databázi. Jinými slovy je duhovka mapována do fázorových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Následně tyto informace slouží k vytvoření duhovkové mapy a šablony pro identifikaci. Celý tento proces trvá cca 2 s.

Výrobci skenerů v dnešní době garantují, že je zde možnost omylu jen v jednom z milionů případů a to v porovnání s identifikaci na základě otisků prstů je desetinásobné zvýšení spolehlivosti. [23]

4.3 Výhody a nevýhody použití identifikace pomocí oční duhovky

Hlavní velkou slabinou této metody jsou různé oční choroby, ale každá s jinak závažnými následky pro skenování. Onemocnění oka nám může duhovku výrazně změnit a to následně velmi komplikuje identifikaci.

Lékaři z Edinburgské oční kliniky Princess Alexandra Eye Pavilion otestovali čtyřiapadesát pacientů, kteří se podrobili léčbě různých druhů očních chorob. Byly zde porovnávány snímky duhovky před léčbou a po skončení léčby. Očekávala se četnost chybování přístrojů, ale dokonce i u pacientů se zeleným očním zákalem, u jehož léčby je v duhovce vytvořen laserem otvor, byly skenery úspěšné. Problém nastal pouze u pacientů se zánětem oční duhovky a to ze čtyřiadvaceti pacientů bylo špatně identifikováno pět. To

se může jevit do budoucna jako závažný problém z důvodu četnosti využívání při identifikaci na letištích. [19]

5 OČNÍ SÍTNICE

Sítnice je světlo-citlivý povrch na zadní straně oka a skládá se z velkého množství nervových buněk. K rozpoznávání osob pomocí sítnice slouží obraz struktury cév na pozadí oka v okolí slepé skvrny.

5.1 Princip použití

K získání obrazu se využívá zdroje světla s nízkou intenzitou záření a opto-elektrický systém složený z jedné LED diody. Naskenovaný obraz je následně převeden do podoby 40-ti bitového čísla.

Při použití této metody je po uživateli vyžadováno, aby se díval do přesně vymezeného prostoru, ale tento požadavek může být pro některé uživatele nepříjemný a někdy také nemožný např. při dlouhodobém nošení brýlí. Z těchto důvodů nemá tato metoda rozšířenou oblast využití. Jde o velice přesnou metodu a na zaznamenání poměrně náročnou. Tyto systémy se používají v oblasti toho nejvyššího stupně zabezpečení. Čas skenování je cca 1,5 až 4 sekundy. Velkou výhodou je spolehlivost a velmi obtížná napodobitelnost, nevýhodou je určitá nepříjemnost pro uživatele. [23]

Obr. 8. Oční sítnice [14]

6 OBLIČEJ – GEOMETRIE TVÁŘE

Geometrie tváře je v dnešní době asi nejvíce zkoumanou metodou, protože problematika identifikace osob dle tváří je velmi rozsáhlá. V laboratorních podmínkách má vynikající výsledky rozpoznávání obličeje, ale otázkou zůstává efektivita technologie v reálném světě.

6.1 Vznik a první využití

Rozpoznávání obličeje se prosadilo na veřejnosti díky Super Bowl 2001, když policie z Tampy skenovala obličeje fanoušků bez jakéhokoliv jejich vědomí a to za účely vypátrání skrytých teroristů v davu. Tento počin policie neměl mnoho kladných ohlasů, to se změnilo až po událostech 11. září 2001. Další použití ve světě je například v kasinech, která ji zavedla ke konci devadesátých let jako prostředek k určení vyloučených hráčů.

6.2 Výhody

Je nejspíše jednou z nejvíce kontroverzních biometrických technologií a to díky své nenápadnosti. Za dobrých podmínek jako je dobrá kamera a dobré světlo může systém zaměřit obličej i z velké vzdálenosti a to bez vědomí sledované osoby. Tato technologie má dobré výsledky i za podmínek maskování, změny váhy, stárnutí nebo změny účesu či vousů.

6.3 Využívané metody

Nejčastěji využívanou technologií pro rozpoznávání obličeje je metoda pomocí geometrie obličeje a to znamená, že systém vezme známý bod a to např. vzdálenost mezi očima a měří nám různé charakteristiky obličeje ve vzdálenosti a úhlu k tomuto známému bodu, nebo také pomocí oči, nosu, úst a obočí.

Další metoda je porovnávání obličeje (eigenface comparison), kde je využívaná paleta asi 150 obličejových abstrakcí a porovnávána s aktuálně skenovaným obličejem. Rozpoznávání funguje na principu srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. Obraz se může ukládat jako matice jasových úrovní, ale spíše se využívá diskriminování nějaké funkce, která nám sníží přebytek dat. To znamená,

že se neuchovává přesná poloha očí, nosu a rtů, ale ukládá se pouze vzdálenost očí a rtů od nosu a úhel mezi špičkou nosu a jedním okem. [23]

7 GEOMETRIE RUKY

Tvar a geometrie dlaně a prstů může sloužit díky tvrzení o své jedinečnosti k bezpečné identifikaci osob.

K rozlišení osob podle geometrie ruky se využívá informacích o délce, šířce, výšce prstů, lokální anomálie a zakřivení. Zařízení určená ke snímání geometrie ruky zaznamenávají pouze 2D siluetu a jiné informace jako např. papilární linie jsou ignorovány. Systémy všeobecně pracují spolehlivě u uživatelů od 8let, protože do tohoto věku dochází k velkým změnám geometrie ruky. Do budoucna lze předpokládat, že na trhu bude zařízení se schopností pracovat s 3D povrchem ruky. Prozatím je tato technologie ve složitém vývoji. V případě 3D snímání geometrie ruky by se zvýšila míra získaných informacích a tím i rozšíření této technologie pro více potencionálních uživatelů. Je zde také možnost kombinace s jinými zařízeními pro zúžení možnosti porovnávaných kombinací. [25]

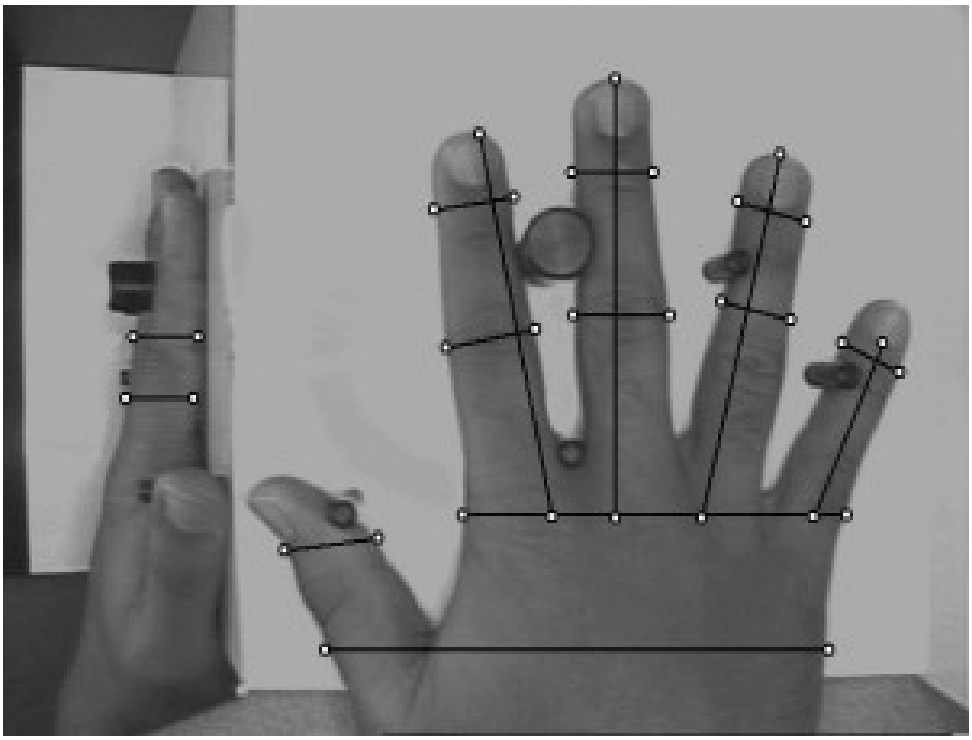
7.1 Technologie snímání geometrie ruky

Ke snímání se využívá dvou pohledů a to shora a zboku. Zřízení pro snímání ruky se skládá z digitální kamery, zrcadel a čtečky, která vymezuje rozmístění jednotlivých prstů a přesné posazení dlaně vůči snímacímu prvku.

Nejprve vložíme ruku do čtečky, poté je digitální kamerou pomocí zrcadel sejmut obraz s informacemi o ploše dlaně, šířce, tloušťce a délce prstů. Následně jsou zjištěné informace porovnávány s informacemi v databázi.

Prvotní skenování a zaznamenání do databáze probíhá pomocí tří skenů, ze kterých je vytvořen průměr a následně je výsledek uložen do databáze. Určité čtečky nevyužívají k identifikaci celou dlaň, ale pouze dva prsty a to prostředníček a ukazováček.

Tato technologie je velmi rychlá celý proces trvá méně než 1 sekundu a je vhodný ke každodennímu používání. Výhodou je nepřetržitá aktualizace, což nám do budoucna eliminuje problémy, jako je změna velikosti ruky popřípadě další aspekty. [23]



Obr. 9. Proces snímání geometrie ruky shora a zboku [18]

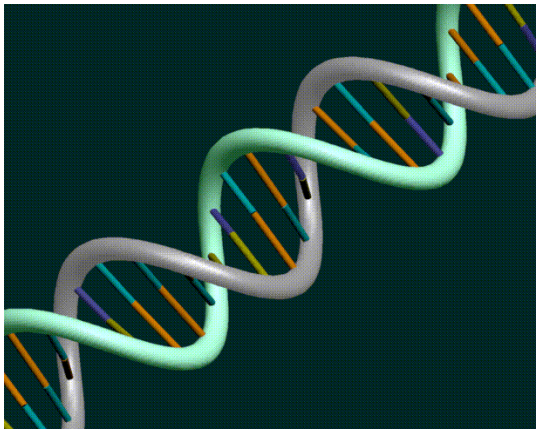
8 DNA

Struktura DNA je geneticky daná a odlišná u všech lidí pouze s výjimkou jednovaječných dvojčat. DNA je po celý život neměnná.

Důslednost a rozšířenost zkoumaní DNA je jedním z důvodu pro stále širší využití i přes to, že její získávání je poměrně technicky i časově náročné. Nevýhodou je, že pro kontrolu přístupu v reálném čase není tato technologie použitelná. [23]

8.1 Postup získání DNA

V prvním kroku je ze vzorku DNA vypreparována celá spirála a ta je štěpena enzymem EcoR1 a následně jsou fragmenty DNA prosévány, až je získán řetězec o využitelné velikosti. Získané fragmenty jsou přeneseny na nylonovou membránu a po přidání radioaktivních nebo obarvených genových sond je získán rentgenový snímek a ten je nazýván otisk DNA. Výsledný otisk vypadá jako čárový kód, a to nám usnadní převod do elektronické podoby.



Obr. 10. Příklad spirály DNA [21]

8.2 Použití v praxi

Přibližně od druhé poloviny osmdesátých let je jedním z hlavních prvků využívaných v policejní praxi. Uplatnění má velký rozsah a to od přiznání otcovství až po identifikaci těl. Již i některé státní organizace např. armáda vytvářejí databáze DNA svých zaměstnanců.

9 DYNAMIKA PODPISU

Tato metoda využívá kombinace behaviorálních a anatomických vlastností každé osoby. Tyto vlastnosti se projevují při ručním podpisu. Je zde možné zjistit tah, tvar a tlak při psaní a to vše elektronicky. Tyto poznatky lze využít k ověření osoby. Dynamika podpisu není to stejné jako elektronický podpis či snímání podpisu jako obrazu. Na rozdíl od statického podpisu se není možné dynamiku podpisu jen ze vzoru naučit. Velkou výhodou je snadná integrace s využitím vhodného softwaru do ostatních zařízení, naopak nevýhodou je, že se systém dokáže využít pouze k ověřování.

9.1 Technologie

Existuje mnoho výrobců zařízení pro zjištění dynamiky podpisu. Všechna zařízení používají stejné nebo podobné technologie, které mají schopnost využití zařízení citlivých na dotek. Nejčastěji jsou zde využívány digitalizační tabule a PDA záznamníky.

Zařízení bývají nejčastěji založené na dynamických vlastnostech, nebo je zde možnost kombinace se zařízeními sledující geometrické a statické vlastnosti podpisu.

Základními vlastnostmi dynamických zařízení je tlak, směr, rychlost, akcelerace a časování. Tyto vlastnosti jsou zaznamenány v trojrozměrném souřadnicovém systému. [23]

10 DYNAMIKY STISKU KLÁVES

Jde o veřejností dobře přijímanou a neinvazivní metodu identifikace osob. Při metodě dynamiky stisku kláves je sledována dynamika úhozů do klávesnice. U každého jedince je tato dynamika odlišná stejně jako u dynamiky podpisu.

Tato technologie spočívá ve sledování doby mezi jednotlivými úhozy a doby, kterou je klávesa zmáčknutá. Stejně jako u ostatních biometrických metod se zde získává otisk, ale doba pro jeho získání je delší než např. u vytváření otisku oční sítnice. [23]

10.1 Využití

Nejvhodnější využití je při kontrole a ochraně před nežádoucími přístupy k síťovým zařízení a osobním počítačům.

10.2 Výhody a nevýhody

Hlavní nevýhodou je vysoká šance nepřesností této technologie. Je zde vysoká možnost zaměnitelnosti sledovaných charakteristik psaní u více osob. Dalším nežádoucím aspektem je vývoj dynamiky stisku kláves u každého jedince.

Hlavní výhodou je, že sledování může běžet na pozadí a při zjištěných nesrovnalostech je vyžádána další kontrola.

11 CHARAKTERISTIKY HLASU

Jedná se o dlouhodobě využívanou neinvazivní metodu, ale s pokrokem ostatních technologiích se tato metoda začala prosazovat až nedávno. Jde o rozpoznávání hlasu, které závisí na okolí. Rozeznáváni hlasu v reálných podmínkách mezi ostatními hlasy je velmi náročné a zatím nebyl ani vyvinut takto přesný systém. Identita osoby je ověřena z uloženého vzoru hlasu. Každý hlas má své určité specifika a to je výhodou této metody, samozřejmě záleží na namluvené klíčové větě. Může se zdát, že tato metoda je z autentizačního hlediska slabá, ale pokud imitátor hlasu nezná předem namluvenou klíčovou větu, nelze při sebemenších schopnostech překonat systém.

Hlavní výhodou je bezesporu nízká pořizovací cena v poměru ke spolehlivosti a také široká možnost nasazení této technologie v praxi např. pro vzdálený přístup k informačním systémům nebo pro telefonické bankovnictví. [23]

12 DALŠÍ BIOMETRICKÉ METODY

Biometrických metod je spousta, ale ne každou je možno dostatečně využít v praxi. Osoby lze dále identifikovat také podle:

- mapy žil na dlani ruky,
- struktury žil na zápěstí,
- tvaru článku prstu a pěsti,
- vrásnění článků prstů,
- podélného rýhování nehtů,
- spektroskopie kůže,
- způsobu pohybu očí,
- povrchové topografie rohovky,
- dynamiky chůze,
- pachu,
- ušního boltce,
- odrazu zvuku v ušním kanálku,
- tvaru a pohybu rtů,
- dynamiky uchopení a stisku střelné zbraně,
- vlastností zubů,
- plantogramu neboli otisku bosé nohy.

II. PRAKTICKÁ ČÁST

13 SOUČASNÝ STAV A PERSPEKTIVY POŽADAVKŮ NA VYUŽITÍ BIOMETRICKÝCH ÚDAJŮ

13.1 Požadavky kladené na biometrické systémy v praxi

Při výběru správného biometrického identifikačního zařízení pro praxi je v prvé řadě zapotřebí brát v potaz tato hlavní kritéria:

- rychlost,
- přesnost,
- velikost šablony,
- cenu,
- velikost snímacího zařízení,
- dotěrnost,
- režim činnosti,
- vliv na soukromí,
- provozní podmínky,
- kulturní a náboženské omezení.

Před vlastním návrhem si musíme ujasnit požadavky, které budeme vyžadovat po použitých biometrických systémech. Tím je myšleno hlavně bezpečnostní riziko, finanční a technické požadavky.

Mezi technickými požadavky nás zajímá splnění biometrických norem BS ISO/IEC 19794-X4, celková kvalita zpracování, záruka, složitost obsluhy, rychlost ověřování, FAR, FRR a v neposlední řadě technická a softwarová podpora dovozce nebo výrobce.

Mezi finančními požadavky nás zajímá v první řadě pořizovací cena v závislosti na rozsahu a podpoře dovozce či přímo výrobce, tím je myšlena aktualizace softwaru, kompatibilita, školení atd. Dále jde o náklady spojené s provozem systému.

Z bezpečnostního hlediska nás u zařízení zajímají podobné vlastnosti jako u technických parametrů a to používané kódování, šifrování, FAR, FRR a protokol pro přenos dat na síti.

Všeobecně u biometrických zařízení platí přímá úměra pro míru spolupráce a to znamená, že čím je potřebná větší míra spolupráce, tím je potřeba pro práci se zařízením zkušenější uživatel. Při výběru vhodného systému musíme brát ohled i na věk uživatelů. V případě využívání přístupového systému staršími osobami lze předpokládat, že může nastat problém při zapamatování hesla, dynamiky stisku kláves a do určité míry i při identifikaci pomocí sítnice či duhovky, v opačném případě by byla velká pravděpodobnost nárůstu koeficientu FRR. Existuje zde také možnost asistence pověřené osoby při identifikaci, ale to už ztrácí na „jednoduchosti“. V případě objektu s vysokým stupněm zabezpečení, jako jsou např. vojenské objekty nebo trezory bank, je vhodné sáhnout po jedné z náročnějších metod, popřípadě několikanásobné kombinaci biometrických systémů. Tyto technologie je díky své důvěryhodnosti a přesnosti velmi obtížné, ba skoro až nemožné neoprávněně překonat, a proto najdou své využití opravdu ve velmi důležitých místech, popřípadě v místech s dostatečnou obsluhou.

Při využití asi nejrozšířenější metody a to identifikace pomocí otisku prstu, která je založena na jedinečnosti každého otisku, je zapotřebí podle stupně zabezpečení dbát na správnou technologii, která již dokáže rozeznat falešný otisk či padělek prstu. Z tohoto důvodu nemůžeme používat ty nejlevnější zařízení se senzorem, který není schopen získat co nejvíce potřebných znaků pro snížení hodnoty chyby FAR. U těchto zařízení je hlavní výhodou velká možnost výběru na trhu za dostupnou cenu.

13.2 Klasifikace chyb

Žádné systémy nejsou bezchybné a to platí i pro biometrii. Můžeme se zde setkat se dvěma druhy chyb, které rozeznávají chybné přijetí anebo odmítnutí.

13.2.1 FAR (False Acceptation Rate)

Jedná se o pravděpodobnost chybné akceptace neboli koeficient bezpečnosti. To znamená, že otisky jsou rozdílné, ale i přesto jsou přijaty a je tak povolen neoprávněný přístup identifikované osobě a to je kritická chyba. [24]

$$FAR = \frac{počet\ shodných\ porovnání\ rozdílných\ vzorů}{celkový\ počet\ porovnání\ rozdílných\ vzorů}$$

Obr. 11. Klasifikace chyb FAR [24]

13.2.2 FRR (False Rejection Rate)

Jde o pravděpodobnost chybného zamítnutí, neboli koeficient "komfortu". To znamená, že otisky se shodují, ale i přesto je přístup zamítnut. Tato chyba nijak neovlivňuje bezpečnostní systém, ale snižuje komfort uživateli identifikace, protože je donucen k opakování identifikace. [24]

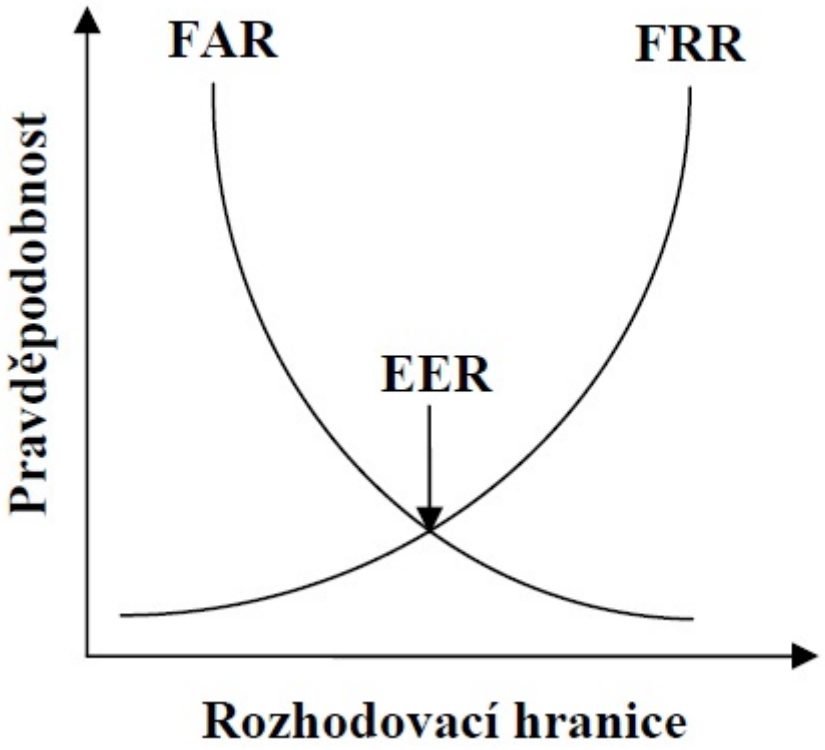
$$FRR = \frac{počet\ porovnání\ vzorů\ osoby\ A\ vedoucí\ k\ neshodě}{celkový\ počet\ porovnání\ vzorů\ osoby\ A}$$

Obr. 12. Klasifikace chyb FRR [24]

13.2.3 EER (Equal Error Rate)

Jde o křížový koeficient mezi FAR a FRR a určení nastavení pro jejich rovnost.

Platí zde, že čím je větší hodnota FRR, tím musí být nepřímou úměrou menší hodnota FAR a nebo také může dojít k opačnému případu, ale taková situace je pro nás nepřípustná. Z tohoto důvodu ideální systém vyžaduje jmenované hodnoty co nejnižší a sobě rovné.



Obr. 13. Závislost FAR a FRR na rozhodovací hranici [17]

Tab. 4. Porovnání jednotlivých biometrických metod FAR a FRR [Vlastní zpracování]

Biometrické metody	FRR[%]	FAR[%]	Rychlost [s]	Třída spolehlivosti
Sítnice oka	1	0,0001–0,00001	0,2-1	vysoká
Duhovky	0,00066	0,00078	2	vysoká
Ušního boltce	1	0,1	3	střední
Geometrie obličeje	1	1	3	střední
Geometrie ruky	0,1	1	1.2	střední
Struktury žil na dlani	0,01	0,00008	-	vysoká
Otisků prstů	1	0,0001–0,00001	0,2-1	vysoká
Spektroskopie kůže	3,9	1,2	-	-
Charakteristiky hlasu v ideálním případě	0,01	0,28	0,2-1	nízká
Pohybu očí	9,4	4,84	-	-
Dynamiky podpisu	0	0,1	-	-

13.3 Možnosti biometrických systémů na současném českém trhu

V této části jsem se zaměřil na biometrické systémy dostupné na českém trhu. Díky technologickému vývoji dnešní doby je velké množství firem, které nabízejí velkou škálu přístrojů a doplňkových služeb pro koncového uživatele.

13.3.1 Přístupové biometrické snímače otisku prstu

Mezi snímači otisků prstu je největší možnost výběru, jak podle použité technologie nebo jiných požadavků. Technologicky jsou nejvyužívanější kapacitní snímače otisku prstu, v menší míře již tepelné snímače a nejméně žádané jsou optické snímače.

Kombinované biometrické kliky

Jedná se o kombinaci kliky a biometrického zámku v jednom. To zamezuje vstupu neoprávněných osob do určitých prostor. Jde o samostatné jednotky, které jsou součástí dveřního kování. Tyto jednotky mají vlastní paměť a tlačítka, která slouží k aktivaci a uložení uživatelů nebo možnosti nastavení průchozího režimu. Komunikace se zařízením

se uskutečňuje pomocí USB disků. Ceny biometrických klik se dle bezpečnostní úrovně pohybují cca od 9.500,- Kč.

Obr. 14. Biometrická klika [25]

Síťová kontrola přístupů

Jde o biometrické zařízení pro kontrolu vstupu identifikované osoby pomocí technologií otisku prstu. Existuje více druhů zařízení pro různé podmínky. Některé zařízení se skládají pouze ze snímače prstu nebo různých kombinací se čtečkami karet, klávesnicí, displeje atd. Tyto zařízení pracují na síťové platformě díky standardně dodávanému Ethernet rozhraní. Využití najdeme jak pro otevírání jednotlivých dveří, tak i pro monitorování docházky uživatelů. Ceny základních modelů se pohybují od 3.600,- Kč a kombinovaných od 12.000,- Kč.

Obr. 15. Přístupová čtečka otisku prstu s klávesnicí a v kombinaci s kartou [16]

13.3.2 Přístupové biometrické snímače podle 3D podoby obličeje

Jedná se o spolehlivou, přesnou a výkonnou metodu pro přístupový systém. 3D biometrický algoritmus dokáže v reálném čase rychlostí 30 snímků za sekundu vyhledat a zpracovat tvář ve video toku. Je zde dosáhnuto extrémně nízké míry chybných odmítnutí (FRR) a to i v případě, že je míra chybných vpuštění (FAR) nastavena na hodnoty blízké 0.

13.3.3 Přístupové biometrické snímače oční duhovky

V současné době je biometrická identifikace dle oční duhovky jedna z nejpřesnějších a nejbezpečnějších, ale četnost využití je především u specializovaných institucí např. armáda. Proces snímání je bezkontaktní a tím i vhodný do prostředí s vysokým hygienickým standardem. Jde o síťové zařízení a samotné porovnání snímku oční duhovky se provádí v hlavním PC.

Obr. 16. Bezkontaktní snímač oční duhovky [16]

13.4 Přístupové biometrické snímače geometrie ruky

Tento systém je vhodný pro maximální stupeň spolehlivosti. Jde o systémy schopné fungovat samostatně, ale také s možností připojení do sítě. Zařízení obsahuje obvody pro obsluhu zámku, monitorování stavu dveří, paměti pro uložení vzorů a transakcí a procesor vyhodnocující oprávněnost vstupu a to nám zabezpečí správnou funkci snímače i pokud selže spojení se síťovým PC. Cena kvalitního snímače geometrie ruky se pohybuje v řádech desítek tisíc korun.

Obr. 17. Zařízení na snímání geometrie ruky [22]

13.4.1 Možnosti přístupu k PC pomocí biometriky

USB zařízení se čtečkou otisku prstu

Jedná se o externí čtečku otisku prstů, která nám bezpečně identifikuje uživatele, pokud má oprávněný přístup k aplikacím. K většině zařízení je dodávaný software, který umožní správu všech přístupových hesel k různým aplikacím a webovým stránkám. Následně je z našeho otisku prstu pro všechny vytvořeno univerzální přístupové heslo. Cenově ji seženeme v základním provedení, ale s vysokou hodnotou FAR již cca za 400,- Kč.

Pro maximální bezpečnost našich dat jsou k dostání flash disky vybavené čtečkou otisků prstů.

Obr. 18. USB čtečka otisku prstu [15]

Přístup k PC pomocí technologie oční duhovky

Funguje na principu ověřování identity uživatele a to pomocí vysoce přesné a spolehlivé technologie oční duhovky. I přes velkou technologickou nákladnost tohoto zařízení jsou zachovány malé rozměry a nízké pořizovací náklady. Obrovskou výhodou je snadné ovládání. Doba verifikace je cca 3 vteřiny a pravděpodobnost chybného přijetí je 1:1200000. Cena takovéhoto zařízení se pohybuje od 5.000,- Kč.

Obr. 19. Přenosný snímač oční duhovky [15]

13.4.2 Biometrické trezory

Jde o trezory a úschovné zařízení např. s elektronickým biometrickým zámkem na otisk prstu a dodatečným způsobem otevření pomocí klíče. V dnešní době jsou k dostání trezory různých velikostí, od malých přenosných až po velké skříňové. Verifikační proces u nejběžnějších přenosných trezorů trvá cca méně než 1 s a je vybaven bezpečnostním kabelem k připevnění např. sedáku v autě. Ceny závisí na velikosti, přičemž cena základního přenosného trezoru s biometrickým zámkem se pohybuje od cca 4.000,- Kč.

Obr. 20. Přenosný biometrický trezor [25]

13.5 Možnost přelstít biometrické systémy

Biometrické systémy patří k těm nejpřesnějším mezi autentizačními metodami, ale vždy existuje nějaká možnost neautorizovaného překonání identifikačního systému. Je zde možnost chyby zařízení FAR a nebo pokusu o sabotáž.

Příkladem překonání otisků prstů je výzkum japonského vědce Cutomu Macumoto z Jokohamské národní univerzity, kde v roce 2002 dokázal jak snadné může být překonat biometrické systémy. Od té doby technologie k identifikaci osob udělaly velký krok kupředu. Bylo uvedeno, že jeho postup byl úspěšný až v 80 % pokusů. Spočívalo to v želatinovém odlitku prstu, který udělal pomocí plastické hmoty s potřebným otiskem. Tím byla vytvořena forma, ze které byl udělán odlitek a vznikl „umělý“ prst. Uskutečnit tuto metodu v praxi je téměř nereálné, jestliže oběť není zároveň útočníkem. S tím jsme se mohli setkat už i v České republice.

Další zjištěná varianta útoku je založena na získání otisku např. ze sklenice, kde už není potřeba spolupráce uživatele. Otisk se posype kriminalistickým aluminiovým práškem a následně otiskneme na průsvitnou folii, kterou přiložíme na fotocitlivou PCB desku. Zmíněná PCB deska se mimo jiné využívá i k výrobě tištěných obvodů. Pro získání plastického otisku je nutné desku osvítit a následně vyvolat. Poté nám stačí už jen postupovat jako u prvního příkladu a aplikovat na čtečce.

Existuje také možnost u rozpoznávání tváře, kde je porovnáván pomocí kamery digitální snímek. Překonání systému spočívá v získání uživatelovi fotografie a v editačním nástroji upravit nasvícení tváře. Tato metoda je v dnešní době už skoro nepoužitelná.

14 NÁVRH BIOMETRICKÉHO PŘÍSTUPOVÉHO SYSTÉMU PRO MALOU FIRMU

14.1 Bezpečnostní posouzení objektu

Uvažujme menší firmu se zaměřením na práci se šperky se sídlem v přízemním samostatném rodinném domě, který se nachází v hustě zastavěné oblasti sídlištního typu s adresou Nad Stráněmi 4511, Zlín. Jedná se o starší stavbu. Objekt je zabezpečen proti vloupání či vandalismu. Lokalitou Jižní Svahy Zlín pravidelně prochází policejní hlídky. Služebna okrsku městské policie Zlín Jižní Svahy se nachází v budově tzv. I. segmentu na ulici Okružní, č.p. 4699, nedaleko od objektu. Rychlost reakce zásahu po nahlášení bezpečnostního narušení se pohybuje v rozmezí 5-10 minut.

Objekt je zabezpečen bezpečnostním systémem od firmy Jablotron, kde je základem ústředna JA-83k rozšířená o rozšiřovací modul a GSM komunikátor připojený na PCO s možností komunikace přes mobilní telefon. Pro použití bezdrátových prvků je zde připojen radiový modul. Na ústřednu jsou připojeny PIR detektory s detekcí rozbití skla, bezdrátový detektor PIR s kamerou, klávesnice s RFID čtečkou, venkovní PIR detektory, magnetické kontakty a dvě akustické sirény.

Objekt není trvale obýván a jeho stěny jsou zděné, použitým materiálem jsou klasické pálené cihly. Střešní krytinu tvoří keramické tašky z pálené hlíny (jílu). Krytina chrání kvalitně proti extrémním klimatickým podmínkám. Na střeše je namontován bleskosvod. Lokalita Jižních Svahů ve Zlíně však přináší i další rizika, velmi často jimi jsou opilí výtržníci a vandalové. Objekt se nachází v přímé blízkosti studentského klubu s prodlouženou otevírací dobou, návštěvníci tohoto podniku mohou být rizikem vandalismu.

Celková hodnota zabezpečovaných hodnot je cca 1.000.000,-Kč. V objektu se často uchovává zboží a materiál vyšší hodnoty. Převážně se jedná o speciální zařízení, které potřebuje firma ke své práci.

Do objektu je možno vstoupit předními vchodovými dveřmi a zadními prosklenými dveřmi z terasy, které jsou většinu dne chráněny bezpečnostní roletou. Přední vchod zabezpečují bezpečnostní dveře, které odpovídají střední, až vysoké úrovni bezpečnosti. Zadní terasové dveře jsou prosklené jednokřídlové plastové s jednostrannou klikou s venkovní

bezpečnostní roletou. Objekt má po obvodu rozmístěno devět plastových oken s venkovní roletou. Pozemek je oplocen dostatečně vysokým plotem ze svařovaného pletiva s jednou přístupovou bránou.

Objekt je rozčleněn do dvou hlavních částí, kde první je přístupová chodba se vzorkovou prodejnou a do druhé části mají přístup pouze oprávněné osoby.

Požární ochrana v objektu je zajištěna. Vznik požáru lze detekovat 5 detektory kouře a nacházejí se zde 3 hasicí přístroje.

14.2 Návrh poplachového zabezpečovacího systému

Stupeň zabezpečení:

3. střední až vysoké riziko (zbraně, ceniny, informace, narkotika).

Stupeň zabezpečení, pro které je zařízení určeno, deklaruje výrobce v technických údajích o zařízení. Požadované technické vlastnosti zařízení pro jednotlivé stupně určují normy řady ČSN EN 50131.

Třída prostředí:

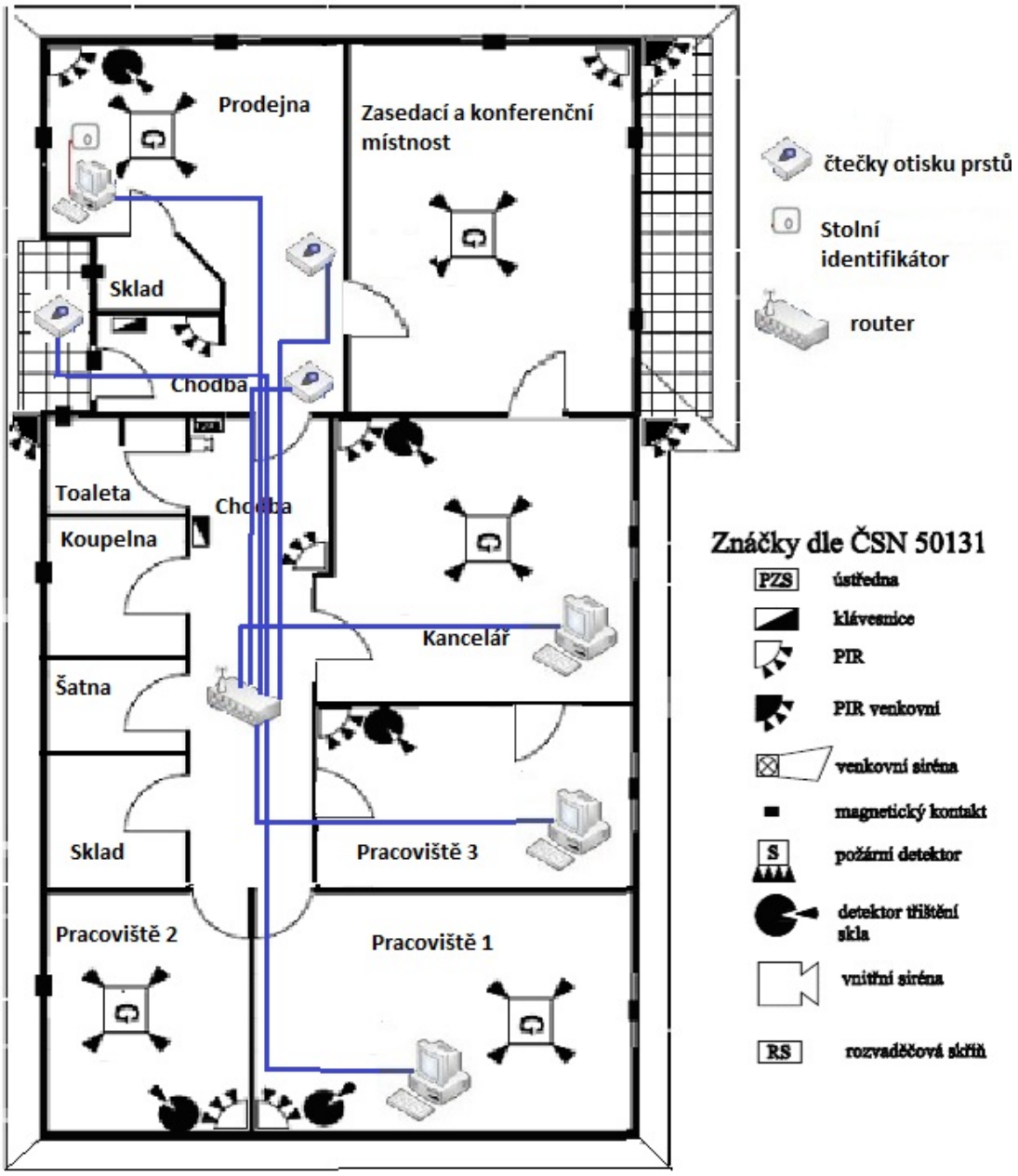
II - vnitřní všeobecné (- 10 °C až + 40 °C)

14.3 Přehled, popis a zdůvodnění použité techniky a materiálu

Varianta Alveno

Firma Alveo nabízí výhodné balíčky v různém rozsahu. Pro tento objekt jsem zvolil balíček Alveo Biometrix, který obsahuje vše potřebné v evidenci docházky ve firmě do 50 zaměstnanců. Obsahuje moderní čtečku otisků prstů DSi 200 s příslušenstvím, která byla použita u hlavního vstupu. Software byl zvolen do 25 zaměstnanců a pro jedno řídící PC.

K balíčku, který obsahoval hlavní venkovní čtečku byly přidány další dva terminály a stolní identifikátor.



Obr. 21. Návrh přístupového systému ALVENO [Vlastní zpracování]

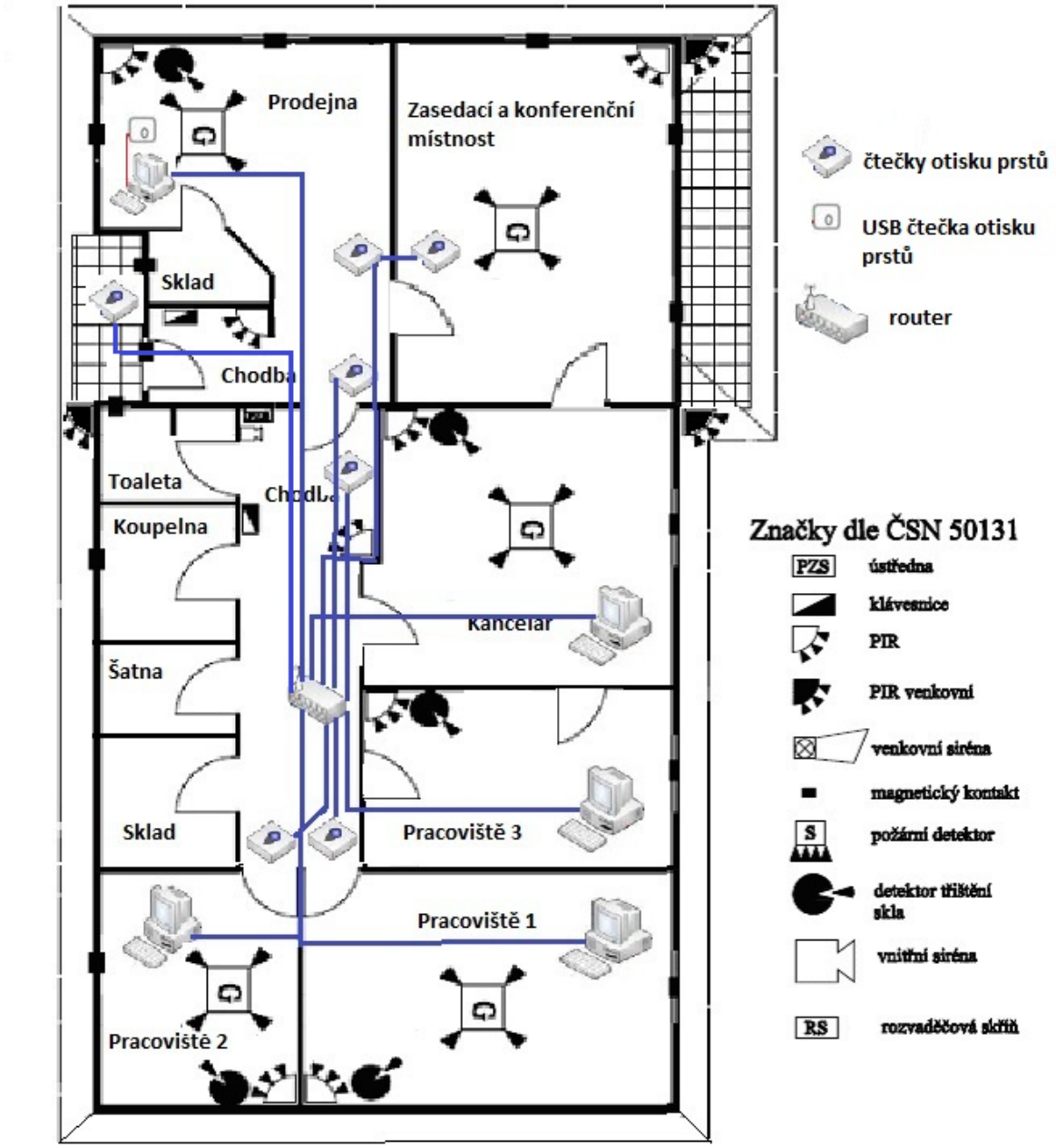
Varianta Comfis

Přístupový systém byl zvolen od firmy Comfis z důvodu velké škály biometrických prvků, softwarové podpoře pro výpočet mzdy a možnosti kompatibility s již nainstalovaným bezpečnostním systémem Jablotron.

Systém je navržen k monitorování pohybu uživatelů, evidenci a zaznamenání odpracované doby. Došlo k nahrazení doposud nedostačujícího způsobu docházky pomocí karty. Systém je propojen s hlavním PC a uživatel s dostatečnými právy může sledovat pohyb

zaměstnanců. Do systému jsou dodána všechna data o docházce potřebná pro zpracování mzdy. Systém byl připojen k dosavadní síti.

Pomocí tohoto přístupového systému chráníte hmotný i nehmotný majetek firmy, zároveň získáváme přehled o pohybu pracovníků po pracovištích a kontrolujeme přístup ke chráněným firemním informacím. Systém vyžaduje k plné funkci vzájemné propojení docházkového a přístupového systému.



Obr. 22. Návrh přístupového systému COMFIS [Vlastní zpracování]

14.4 Cenový rozpočet prvků

Varianta Alveno

Základem je čtečka DSi 200 určena menším firmám, které hledají levné řešení docházkového systému, ale za využití biometrických metod. U každého zaměstnance můžeme navolit, zda se bude identifikovat pouze otiskem prstu, čipem nebo kombinací otisku a čipu.

Obr. 23. čtečka DSi 200 [16]

Zvolené přístupové terminály Psi 50 jsou používány ke vstupu do soukromé pracovní části firmy. Jde o kombinovaný terminál, kde pro každého zaměstnance můžeme navolit práva.

Obr. 24. Terminál Psi 50 [16]

Objekt je dále vybaven čtyřmi přenosnými a kompaktními sejfy pro přenos a úschovu šperku, popřípadě jiných využívaných cenných materiálů a informací.

Tab. 5. Cenový rozpočet varianty od firmy ALVENO [Vlastní zpracování]

Balíček Alveno Biometrix	Čtečka	Dsi 200	
	Software	Alveno Business.25	**16.990,-**
+	Stolní identifikátor		**5.000,-**
+	Školení		**2 .000,-**
+	Terminál 2 ks	Psi 50	**24.682,-**
Celkem	bez DPH		**48.672,-**
	Trezor 4 ks	TRZ 01	**13.444,-**

Varianta Comfis

Hlavní jednotkou je terminál F702-MS od firmy Comfis, odolný proti venkovním nepříznivým vlivům. Kapacita otisků/záznamů je 1 500/50 000, doba verifikace: ≤ 2 s a hodnoty FAR: ≤ 0,0001 % a FRR: ≤ 1 %.

Obr. 25. Terminál Comfis F702-MS [25]

Podřazené čtečky otisku prstů SR100 jsou kompatibilní s terminálem. Veškeré informace o uživatelích včetně záznamů o transakcích jsou ukládány do nadřazeného zařízení.

Obr. 26. Čtečka otisku prstů SR100 [25]

Objekt je dále vybaven čtyřmi přenosnými a kompaktními sejfy pro přenos a úschovu šperku, popřípadě jiných využívaných cenných materiálů a informací.

Tab. 6. Cenový rozpočet varianty od firmy COMFIS [Vlastní zpracování]

	Typ	Počet	Cena /kus	Celkem
Terminál	F702-MS	1 ks	18.970,-	18.970,-
Čtečka	SR100	6 ks	3.076,-	18.456,-
Externí čtečka k PC		1 ks	796,-	796,-
Kabeláž	SYKY 6P CAT3	100 m	730,-	730,-
CELKEM bez DPH				38.959,-
Trezor	TRZ 01	4 ks	3.361,-	13.444,-

14.5 Postup instalace a konfigurace systému

Varianta Alveno

Velkou výhodou je jednoduchost montáže celého systému, kterou zvládne nainstalovat každý pracovník se schopností pracovat v síti. Čtečku připojíme k napájení a do nejbližšího switche, příp. strukturované kabeláže. Dále čtečce nastavíme IP adresu a na libovolný počítač nainstalujete program Alveno. Pro tento objekt byla zakoupena licence pro jeden PC. Po spuštění programu zadáme IP adresu čtečky a docházkový systém je nainstalovaný.

Varianta Comfis

Při instalaci a konfiguraci systému jsem postupoval podle následujících bodů:

- instalace terminálu a podřízených čteček,
- sejmutí otisku uživatele,
- nastavení komunikace s PC,
- instalace a nastavení softwaru,
- stažení uživatelských informací a otisků prstů,
- nastavení časového plánu a pracovních směn,
- přiřazení pracovních směn zaměstnancům,
- tisk a export dat.

14.6 Legislativa, normy a další předpisy

V oblasti zabezpečovací techniky je vydána řada norem (ČSN EN 5013x-x). Finální znění vydaných norem získáte v Českém normalizačním institutu.

14.7 Certifikace, prohlášení o shodě

Přístupový systém splňuje biometrické normy BS ISO/IEC 19794-X_4, bezpečnostní systém je certifikován podle ČSN EN 50131-1 do třetího stupně střední až vysoké riziko. Certifikace systému a certifikace montážní firmy je podmínkou pro uznání systému dle podmínek asociace pojišťoven. Podmiňuje výplatu pojistné náhrady v plné výši, případně se uplatňuje jako podmínka pro uznání slevy na pojistném (viz. podmínky konkrétní pojišťovny).

Návrh splňuje kvality dle ISO 9001 a ISO 13485, prohlášení o shodě – CE. Všechny prvky navržené v tomto návrhu jsou označeny CE.

Pokud se správně používá výrobek s platným označením CE, a pokud byl tento výrobek i správně nainstalován, je jeho používání v maximální míře bezpečné.

ZÁVĚR

V dnešní době je moderní technika všude kolem nás a je využívaná ve všech oblastech lidských aktivit. Informatika se zasloužila o zefektivnění a každopádně zrychlení biometrických systémů. Postupem času se biometrické zařízení, zejména snímače otisků prstů staly dostupným pro širší škálu zákazníků a již se s nimi můžeme setkat i několikrát denně v běžném životě. Doba jde dopředu a společně s ní i věda o biometrických systémech, které se zdokonalují a minimalizují. Do budoucnosti se dá počítat s velkým rozvojem všech biometrických metod a to, že se s nimi budeme setkávat častěji a „usnadní nám život". Biometrie se již využívá i v oblasti osobních dokladů nebo pro databáze pacientů v nemocnicích, ale díky své unikátnosti si myslím, že její největší uplatnění je spíše pro identifikaci osob v kriminalistice, kde jsou k této činnosti proškoleni pracovníci.

Biometrie nám přináší vysokou míru bezpečnosti a pohodlné používání. Rozvoj a vývoj neustále pokračuje a vznikají nové metody identifikace např. podle nosu nebo struktury kůže, ale identifikace pomocí otisku prstu zůstane nadále v případech kde nevadí při identifikaci kontakt nejspíše tou nejpoužívanější metodou. Rozvoj jde jasným směrem a to je uplatnění v každodenních lidských činnostech, proto lze očekávat v budoucnu častější styk s těmito technologiemi.

Nejrozšířenější a veřejností nejoblíbenější biometrickou metodou je bezesporu identifikace pomocí otisku prstu a to díky své jednoduchosti, spolehlivosti, jedinečnosti a dobrému poměru mezi cenou a výkonem. Při výběru snímačů otisků prstů je zapotřebí brát ohled na podmínky a osoby, které je využívají. Z praktického hlediska je myšleno zejména znečištění rukou, důležitost chráněných informací či přístupů a v neposlední řadě hygiena při snímání.

Stále více firem nabízí k přístupovým systémům kromě monitoringu pohybu zaměstnanců také rozsáhlejší software, který je nám schopen při dobrém přednastavením vypočítat mzdu každého zaměstnance.

Pro vhodný návrh přístupového systému si musíme ujasnit co je žádané, co může do budoucna firma nabídnout a jak dlouho se již na trhu pohybuje. Určitě je vhodné se kvůli kompatibilitě držet výrobků pouze od jedné firmy. Správná volba systému nám do budoucna ušetří spoustu práce a peněz.

ZÁVĚR V ANGLIČTINĚ

Nowadays modern technology is all around us and it is used in all areas of human activity. Informatics deserved to streamline and speed up biometric systems. Over time, the biometric devices, especially fingerprint sensors have become available for a wider range of customers and we can already meet them several times a day in a real life. As time moves forward, the biometrics systems are improved and minimized. In the future we can count on the great development of biometric methods. We will meet them more frequently in our lives and they will „make our live easier“. Biometrics is already being deployed in the area of personal documents or databases of patients in hospitals. Personally I think that because of its uniqueness the best application is for personal identification in forensics, because there is trained personnel for this activity.

Biometrics gives us a high degree of safety and comfort. Development and evolution continue and there are created new identification methods such as identification according to the nose or skin structures. But the fingerprint identification will continue to be the most used method in the situations where it does not matter whether you touch the things or not. The development is going in a clear direction. It is going in a direction of application in everyday human activities, therefore we can expect more frequent intercourse with these technologies in the future.

The most common and most popular public biometric method is certainly the fingerprint identification because of its simplicity, reliability, uniqueness and good relationship between price and performance. When selecting a fingerprint reader, it is required to take into consideration the conditions and people who use them. From a practical point of view it is particularly pollution of hands, the importance of protected information and approaches and, finally shooting hygiene.

More and more companies offer with the access systems in addition to the systems for monitoring the movement of workers also a more extensive software, which is able to calculate salary for each employee.

To design a suitable access system, we must clarify what is desired, what can offer a company and how long it is on the market. Surely, because of compatibility, it is the best to stick the products from only one company. The correct choice of the system will save us a lot of work and money in the future.

SEZNAM POUŽITÉ LITERATURY

Monografie

[1] ČANDÍK, Marek. *Objektová bezpečnost II.* Vyd. 1. Zlín : Univerzita Tomáše Bati, 2004. 100 s. ISBN 8073182173.

[2] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. ISBN 80-902938-2-4(brož.).

[3] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

[4] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[5] PORADA, Viktor. *Kriminalistika.* Brno : CERM, 2001. 746 s. ISBN 8072041940

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

Elektronické zdroje

[7] Biometrika - přehled. *TechNet* [online]. 2011, 1, [cit. 2011-05-15]. Dostupný z WWW: http://technet.microsoft.com/cs-cz/library/dd759228.aspx

[8] BIOMETRIKY. *COMFIS s.r.o.* [online]. 2008, [cit. 2011-04-19]. Dostupný z WWW: http://www.comfis.cz/biometrie

[9] Biometrické systémy v praxi. *Systemonline* [online]. 2004, [cit. 2011-04-19]. Dostupný z WWW: http://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[10] DOUPAL, František. Výběr notebooku v roce 2008 - 2. výkon a výbava. *Notebooky Ostatní* [online]. 2008, [cit. 2011-05-06]. Dostupný z WWW: http://www.notebook.cz/clanky/ostatni/2008/vyber-notebooku-v-roce2008-vykon-a-vybava

[11] ĎÁSEK, Milan. *Biometrika* [online]. 2003 [cit. 2009-05-15]. Dostupný z WWW: http://www.volny.cz/pretorian/biometrika.html#x81

[12] Ekey net. Ekey net [online]. 2010, [cit. 2011-04-19]. Dostupný z WWW: http://www.ekey.cz/produkty/ekey-net/

[13] JEDLIČKA, Miloslav . Kriminalistická daktyloskopie. *Kriminalistika* [online]. 2005, 1, [cit. 2011-05-15]. Dostupný z WWW: http://kriminalistika.eu/daktyl/daktyl.html

[14] JIRSOVÁ, Miroslava. Placení v budoucnu: místo PIN postačí oční sítnice. *Magazín Hospodářských novin* [online]. 2009, [cit. 2011-05-06]. Dostupný z WWW: http://in.ihned.cz/c1-32626600-placeni-v-budoucnu-pocitac-precte-ocni-sitnici-misto-pin

[15] Kontrola přístupu do PC [online]. 2009 [cit. 2011-05-12]. *Digitus*. Dostupné z WWW: http://www.digitus.cz/pristup_pc.php

[16] Kontrola vstupu a docházky [online]. 2009 [cit. 2011-05-21]. *Digitus*. Dostupné z WWW: http://www.digitus.cz/dochazka.php

[17] MIROSLAV, Skoumal. Identifikace člověka pomocí biometrické technologie. [s.8.], 2007. 50 s. Vedoucí bakalářské práce PaedDr. Zdeněk Pejsar Ph.D. Dostupný z WWW: http://minsky.ic.cz/veci/identifikace_cloveka_pomoci_biometrickych_udaju.pdf

[18] NOVÁČKOVÁ, Helena. Biometrické systémy. *Security info* [online]. 2010, [cit. 2011-05-06]. Dostupný z WWW: <http://www.securityinfo.cz/124/biometricke-systemy/>.

[19] PETR, Jaroslav. Zánět duhovky komplikuje identifikaci osob. *Člověk* [online]. 2009, [cit. 2011-05-21]. Dostupný z WWW: http://www.rozhlas.cz/leonardo/clovek/_zprava/561062

[20] POLÁČKOVÁ, Zuzana. Rešerše algoritmů pro snímání a zpracování otisku prstů [online]. 2008, [cit. 2009-02-15]. Dostupný z WWW:https://dip.felk.cvut.cz/browse/pdfcache/polacz1_2008bach.pdf

[21] Ribbons User Manual. Richards *Center at Yale University* [online]. 2009, [cit. 2011-05-06]. Dostupný z WWW: http://www.csb.yale.edu/userguides/graphics/ribbons/help/dna_rgb.html

[22] Snímání geometrie ruky. *Biometrie* [online]. 2010, [cit. 2011-05-21]. Dostupný z WWW: http://strade.fit.vutbr.cz/index.php?act=51&menu1=52&menu2=83

[23] ŠČUREK, Radomír . Biometrické metody identifikace osob v bezpečnostní prax [online] 58 s. Oborová práce. VŠB TU Ostrava. Dostupné z WWW: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf

[24] Technologie biometriky. *Technologie biometriky* [online]. 2008, [cit. 2011-05-06]. Dostupný z WWW: http://www.comfis.cz/biometrie?print

[25] Terminály. *Produkty - Terminály a Privaris* [online]. 2008, [cit. 2011-05-07]. Dostupný z WWW: http://www.comfis.cz/produkty/privaris-a-terminaly/terminaly

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCD Elektronická součástka pro snímaní obrazové informace (Charge-Coupled Device)

DNA Deoxyribonukleová kyselina

EER Křížový koeficient mezi FAR a FRR (Equal Error Rate)

FAR Poměr chybně akceptovaných osob (False Acceptance Rate)

FRR Poměr chybně odmítnutých osob (False Rejection Rate)

GSM Globální systém pro mobilní komunikace (Groupe Special Mobile)

IP Internetový protokol

LED Dioda emitující světlo (Light-Emitting Diode)

PC Osobní počítač (Personal Computer)

PCB Deska plošných spojů

PCO Pult centralizované ochran

PIN Číselný řetězec standardní délky (Personal Identification Number)

PIR Infrapasivní čidla

RFID Identifikace na rádiové frekvenci (Radio Frequency Identification)

USB Univerzální sériová sběrnice (Universal Serial Bus)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK