Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Biometrické autentizační metody

Martin Robausch

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Robausch

Informatika

Název práce

Biometrické autentizační metody

Název anglicky

Biometric authentication methods

Cíle práce

Přehled aktuálně používaných autentizačních metod založených na biometrice, technologie čteček, vyhodocování a chybovost. Případně i aplikace v praxi.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Pomocí této metodiky je vybráno vhodné řešení pro biometrický docházkový systém a srovnání s docházkovým systémem. Na základě teoretických poznatků a praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40

Klíčová slova

Biometrie, biometrické čtečky, docházkové systémy

Doporučené zdroje informací

BOLLE, R. Guide to Biometrics. Springer Science & Business Media, 2004. ISBN 0387400893, 9780387400891.

BOULGOURIS, N. – PLATANIOTIS, N.– MICHELI-TZANAKOU, E. Biometrics: Theory, Methods, and Applications. John Wiley & Sons, 2009. ISBN 0470522348, 9780470522349.

ČANDÍK, M. Objektová bezpečnost II, UTB ve Zlíně, 2004. ISBN 8073182173, 9788073182175.

JAIN, A. – FLYNN, P. – ROSS, A. Handbook of Biometrics. Springer Science & Business Media, 2007. ISBN 0387710418, 9780387710419.

ŘÍHA, Z. – RAK, R. – MATYÁŠ, V. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

ŠČUREK, R. Biometrické metody identifikace osob v bezpečnostní praxi. Ostrava: VŠB TU Ostrava, 2008 [online] <https://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf>.

WOODWARD, J. – ORLANS, N. – HIGGINS, P. Biometrics: Identity Assurance in the Information Age. Osborne, 2002. ISBN-13: 978-0072222272.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 10. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Biometrické autentizační metody" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Tomáši Vokounovi za cenné rady, ochotu a vedení práce. Dále by chtěl poděkovat firmě Kemmler Electronic za poskytnuté informace o docházkovém systému.

Biometrické autentizační metody

Souhrn

Práce se zabývá biometrickými autentizačními metodami. Obsahuje přiblížení do problematiky fungování biometrických metod. Dále se zaměřuje na výběr vhodného docházkového systému a implementaci tohoto systému do podniku.

Klíčová slova: Biometrie, Biometrické metody, Docházkové systémy.

Biometric authentication methods

Summary

This thesis deals with the biometric authentication methods. It involves problematics of using biometric methods. It aslo focuses on choosing an appropriate attendance system and it´s implementation into a company.

Keywords: Biometrics, Biometrics methods, Attendance systems

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1 Úvod

Biometrické systémy jsou v současné době velmi populární prostředky ke zvýšení bezpečnosti střežených prostor. Ve většině případů slouží jako kontrola vstupu. V této oblasti se setkáváme s několika základními systémy, které dominují na trhu. Jsou to především systémy pro rozpoznávání charakteristik obličeje a otisky prstů.

Cílem práce v teoretické části je představení a charakteristika aktuálně používaných biometrických metod. Nejprve se, ale seznámíme s tím co to vlastně biometrie je, její základní pojmy. V další části budou charakterizovány biometrické systémy, jak fungují, jak se vyhodnocuje výkonost systémů.

Praktická část bakalářské práce je zaměřena na srovnání klasického docházkového systému na docházková média a moderního biometrického systému. Nový biometrický systém je vybrán na základě teoretické části porovnáním biometrických metod na základě tří hlavních kritérií a určených požadavků, které mají mít za následek zvýšení efektivnosti zaměstnanců.

2 Cíl práce a metodika

2.1 Cíl práce

Přehled aktuálně používaných autentizačních metod založených na biometrice, technologie čteček, vyhodnocování a chybovost. Případně i aplikace v praxi.

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Pomocí této metodiky je vybráno vhodné řešení pro biometrický docházkový systém a srovnání s docházkovým systémem. Na základě teoretických poznatků a praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

Biometrie je vědní obor zabývající se studií a zkoumáním živých organismů, především člověka a měřením jeho anatomických a fyziologických vlastností a také podle jeho chování. Pojem biometrie je odvozen z řeckých slov „bios“ což je život a „metron“ což znamená měření. Biometrie se zabývá studií metod, které vedou k rozpoznávání člověka na základě jeho unikátních vlastností.

Biometrie se používala už před nástupem počítačů. Lidé se rozpoznávají pomocí vzhledu obličeje nebo jsou známy otisky dlaní rukou v jeskyních jako jakýsi podpis autora. S rozvojem počítačové technologie na konci 60. let se začalo stávat i rozpoznávání člověka automatizované.

V současné době jsou informační technologie jednou z nejrychleji se rozvíjejících oblastí. Každodenní transakce se stále častěji provádějí elektronicky místo standartních ručních zpracování. Rozvoj elektronických transakcí vyústil k rostoucí potřebě přesně identifikovat a autentizovat uživatele. (Koláček, 2009)

3.1 Základní pojmy biometrie

V problematice biometrie se setkáváme s několika základními, konkrétně se čtyřmi pojmy, které nejsou vždy správně překládány. Mezi tyto pojmy patří:

Recognition v překladu znamená rozpoznávání. Jedná se o rozpoznávání člověka použitím zvolené biometrické vlastnosti.

Verification znamená ověření. Je to proces, při kterém se systém snaží potvrdit totožnost jedince, který vkládá své údaje k ověření. Je proveden tak, že systém porovnává sejmutý vzorek jedince s již dříve zapsaným vzorkem tak zvanou šablonou.

Identification znamená identifikace. Je to proces, při kterém systém určuje totožnost uživatele. Biometrická vlastnost je sejmuta a porovnávaná se všemi uloženými šablonami.

Authentication znamená autentizace. Je to proces ověření proklamované identity subjektu. Po dokončení autentizace obvykle následuje autorizace, což je souhlas, umožnění přístupu či provedení konkrétní operace daným subjektem. (Flídr, 2009)

3.2 Elektronické biometrické rozpoznávací systémy

S neuvěřitelně rychlým rozvojem informačních technologií roste i zájem o nové techniky vzájemného působení člověka a stroje. Komunikace mezi lidmi, skládající se především z rozhovoru a poznávání osob podle obličeje zatím nebylo dostatečně upraveno pro interakci člověka a stroje. Stále se zde dominuje klávesnice a myš. Zatím ani dotykové obrazovky nejsou na takové vysoké úrovni, aby byli schopné konkurovat a komunikovat mezi sebou jako lidé mezi sebou.

Využití elektronických biometrických rozpoznávacích systému má v praxi široké uplatnění, ať už se jedná o soukromou nebo forenzní sféru. Ve forenzní sféře, mezi kterou patří soudní a kriminalistické se nejčastěji používají automatické rozpoznávací systémy otisků prstů a identifikaci pomocí DNA. Velký vliv na jejich implementaci v různých státech má i postoj odpovědných osob. Je nutno poznamenat i rychlý rozvoj biometrické identifikace u cestovních pasů, občanských průkazů a při bankovních transakcích.

Pořízení takovýchto systémů do soukromé sféry je zcela nepřijatelné z hlediska ceny. V případě uvažování o jejich implementaci do soukromé sféry je nutné zredukovat jejich cenu. Docílí se toho tak, že se využívá daleko menších databází. V databázích v soukromé sféře se používají biometrické vzorky osob, které pracují v daném podniku. Například v databázi otisků prstů v kriminalistické sféře je nutné ukládat vzorky všech deseti prstů, v soukromé sféře se ukládá například vzorek jen jednoho prstu. Z těchto důvodů si systém vystačí s mnohem menší kapacitou paměti a hlavně operačním výkonem, čím se také sníží cena celého systému. (Ščurek, 2008)

3.2.1 Princip řízení a kontroly vstupů

Hlavním předpokladem pro správné provedení biometrické autenfikace je odebrání a zápis určité vlastnosti osoby, které se dále uloží jako referenční šablona. Tato šablona může být uložena buď, centrálně nebo decentralizovaně. Když je šablona uložena centrálně znamená to, že je uložena do datové paměti systému nebo aplikace. Při decentralizovaném ukládání se referenční šablona ukládá na ID karty nebo počítače. Proces snímání musí být

prováděn v důvěryhodném prostředí, které musí splňovat právní úpravy v České republice. Většina biometrických systému pracuje s následujícím postupem:

Pořízení datového souboru, který může být uložen jako obrázek, zvuk nebo jakýkoliv jiný typ, podle biometrické vlastnosti. Tento datový soubor obsahuje hodnoty biometrické vlastnosti, které z tohoto souboru půjde použitím vhodné metody vyextrahovat pomocí vhodného snímače.

Dále se musí prověřit kvalita dat v souboru. V případě, že jejich kvalita nevyhovuje, jsou buď okamžitě odmítnuta, nebo se uživateli poskytne vhodná rada, které zvýší kvalitu odebrané biometrické vlastnosti.

Po těchto dvou předchozích bodů se provede zápis či uložení této referenční šablony do systému nebo aplikace.

Následuje ověřování referenční šablony. Znamená to, že se porovnává aktuální šablona s referenční šablonou užitím vhodného algoritmu pro určení shody a vygenerování hodnoty. Tato vygenerovaná hodnota se nazývá skóre, které je rozhodná pro determinování stupně shody.

Výsledkem ověřování je myšleno skóre, které je vygenerováno porovnáním vzorku s referenční šablonou. V daném systému se nadefinuje hranice, které určí jaké je možné nejvyšší skóre pro povolení přístupu. V případě, že se výsledné skóre nachází někde v této definované hranici, je přístup povolen. V případě, že výsledné skóre je vyšší, než předdefinovaná hranice je přístup odmítnut. (Ščurek, 2008)

3.2.2 Biometrické informace používané pro identifikaci

Hlavní kritéria pro výběr biologické nebo behaviorální vlastnosti člověka určené pro jeho další identifikaci jsou určena co nejširším a nejefektivnějším způsobem užití. Takováto vlastnost musí splňovat několik důležitých podmínek.

Mezi takovéto podmínky patří jedinečnost. Jedinečná vlastnost je taková vlastnost, které je co možná nejvíce výjimečná, to znamená, že se nesmí například objevit u dvou osob totožné otisky prstu.

Patří sem také kritérium univerzálnosti. Takováto podmínka znamená, že tato vlastnost musí být měřitelná u co možná největší množiny lidí.

Trvalost znamená, že daná vlastnost se nesmí měnit v čase. V průběhu stárnutí člověka musí být stále stejná.

Další podmínka je měřitelnost. Vlastnost musí být měřitelná shodnými technickými zařízeními.

Poslední podmínkou je uživatelská přijatelnost. Znamená to, že tato vlastnost by měla být měřitelná co nejsnadněji a pohodlně. (Ščurek, 2008)

3.2.3 Měření výkonosti biometrických systému

To, aby uživatel při autentizaci poskytl přesně stejný vzor, jako když se registroval, je téměř nemožné. Z toho důvodu je potřeba umožnit mezi porovnávanými vzorky určitou změnu. Jinak by mohlo docházet při rozhodování k chybám. Další chyby, způsobují hlavně neadekvátní vzorky od osob užívajících systém.

Efektivnost biometrických systémů lze měřit mnoha statistickými koeficienty. Mezi hlavní výkonnostní koeficienty jsou řazeny koeficient nesprávného přijetí a koeficient nesprávného odmítnutí. Existuje nespočet takovýchto koeficientů v závislosti na hloubce zkoumání daného problému. (Michálek, 2009)

Koeficient nesprávného přijetí z anglického překladu false acceptance rate ve zkratce FAR. Tento koeficient udává pravděpodobnost toho, že neoprávněná osoba může být přijata jako oprávněná. Nesprávné přijetí často může vést ke vzniku škody na majetku. FAR je tedy koeficient, který udává míru bezpečnosti. Jedná se o přijetí neregistrované osoby do systému, které nemá za standartních podmínek oprávněný přístup do systému. Jedná se tedy o kritickou chybu z bezpečnostního hlediska. Koeficient FAR se dá vypočítat pomocí následujícího vzorce. (Flídr, 2009) (Ščurek, 2008)

$$FAR = \frac{\text{Nesprávná přijetí (počet)}}{\text{Celkový počet pokusů}} * 100\ [\%]$$

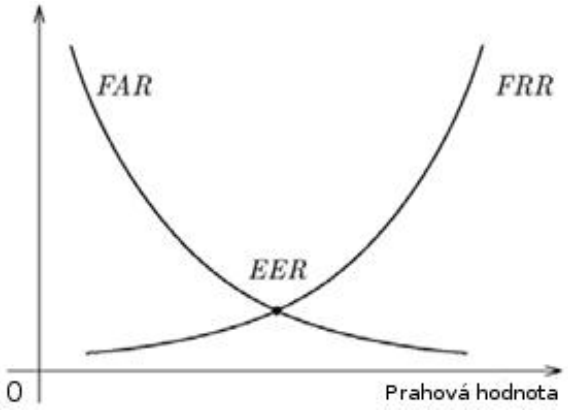
Obrázek 1 : Koeficient nesprávného přijetí (FAR) [8]

Koeficient nesprávného odmítnutí z anglického překladu false rejection rate používá se u něho zkratka FRR. Koeficient nesprávného odmítnutí udává pravděpodobnost, že je oprávněná osoba systémem odmítnutá. V případě koeficientu FRR se jedná hlavně o komfort, protože nesprávné odmítnutí je pro uživatele velice nepříjemné. Jedná se o odmítnutí či nerozpoznání osoby, která je v systému zaregistrována a má do něj za standartních podmínek oprávněný přístup. Tato chyba nemá z bezpečnostního hlediska velký význam, ale za to má vysoký význam z hlediska marketingového, protože nutí oprávněného uživatele k opakování pokusu o přístup a to má za následek jeho nespokojenost. Koeficient FRR se počítá podle následujícího vzorce. (Flídr, 2009) (Ščurek, 2008)

$$FRR = \frac{\text{Nesprávná odmítnutí (počet)}}{\text{Celkový počet pokusů}} * 100\ [\%]$$

Obrázek 2 : Koeficient nesprávného odmítnutí (FRR) [8]

Koeficient vyrovnané chyby z anglického překladu equal error rate, zkratka ERR. Tento koeficient se také nazývá jako křížový koeficient. Nachází se na pomezí koeficientů FAR a FRR. Čím se EER náchází níž, tím přesnější rozpoznávací systém je. Samotná hodnota koeficientu EER však nemá žádnou vypovídající hodnotu. To znamená, že je potřeba znát hodnoty koeficientů FAR a FRR, aby nám řekl jak je celý systém bezpečný. (Michálek, 2009)



Obrázek 3 : Závislost FAR a FRR na prahové hodnotě [8]

Dalším používaným koeficientem je Failure to Enroll Rate ve zkratce FER. Tento koeficient udává poměr osob, u kterých selhal proces sejmutí vlastností, pomocí některé biometrické metody. Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti. Pro získání spolehlivých statistických údajů, je nutné provést větší množství pokusů sejmutí biometrických vlastností. (Ščurek, 2008)

False Identification Rate udává pravděpodobnost, že při procesu identifikace je biometrická vlastnost nesprávně přiřazena. Tento koeficient závisí na principu, kterým se přiřazuje ke srovnávacímu vzorku. Stává se, že po identifikaci vyhovuje více než jeden srovnávací vzorek. Pro tento koeficient se používá zkratka FIR. (Ščurek, 2008)

3.2.4 Zvyšování bezpečnosti biometrických systému

Hlavním důvodem ke snaze o zvyšování bezpečnosti biometrických systémů, je že biometrické systémy pracují s určitou chybovostí. Dalším důvodem je zvyšování počtu pokusů o napadení biometrických systémů. V tomto případě se zde objevují pokusy o změny otisků prstů, odlívání otisků prstů nebo různé plastické operace, což je velice nebezpečné pro bezpečnostní aplikace.

Jednou z možností je vícenásobná biometrická identifikace. Jedná se o kombinaci více biometrických znaků v jednom systému. K nejčastěji využívaným kombinacím patří identifikace podle otisků prstů a geometrie obličeje. Další z možností jak zvýšit bezpečnost systémů je využití skrytých znaků, které je mnohem obtížnější změnit, v některých případech v podstatě nemožné změnit. (Ščurek, 2008)

3.3 Jednotlivé biometrické technologie

Biometrika, biometrická charakteristika je něco, co člověka téměř jednoznačně charakterizuje. Tyto charakteristiky mohou být různé. Liší se v principu, metodě a jistotě identifikace, kterou poskytují. V následujícím seznamu jsou uvedeny nejčastěji používané nebo vyvíjené metody.

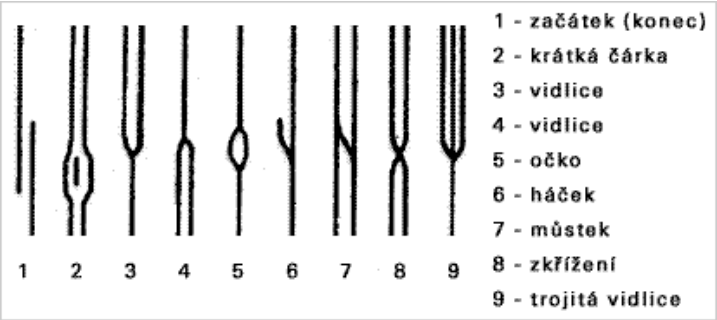
3.3.1 Identifikace pomocí otisku prstu

Identifikace na základě otisku prstu je nejznámější a jedna z nejpoužívanějších metod identifikace osob. Jedná se o velmi starou metodu, jejíž základy položil již Jan Evangelista Purkyně v roce 1823, když tohoto roku vydal spis a charakterizoval v něm základní vzory papilárních linií na koncových článcích prstů.

Jedná se o unikátní prostorovou kresbu vyvýšenin povrchové struktury prstu, tak zvané papilární linie. Tato kresba vznikla díky evolučním pochodům, kvůli zlepšení schopnosti úchopu a citů na všech končetinách. Informace o struktuře těchto útvarů je umístěna až v nejhlubších vrstvách zárodečné vrstvě kůže. To znamená, že jí není možné snadno odstranit bez násilných postupů. Informace odolá i mechanickému poškození. Po určité době se tato informace opět zregeneruje, pokud nedojde k poškození zárodečné vrstvy.

Ani neustálým obnovováním odumřelých buněk pokožky novými a ani s věkem nedochází ke změně charakteristických bodů otisků, tak zvaných markatů. Tato kresba je teoreticky jedinečná pro každý prst. Vzhledem k počtu různých typů markantů a jejich množství v řádech desítek na každém prstu. To znamená, že pravděpodobnost shody

jediného otisku prstu u dvou lidí je velice nepravděpodobná. Základní typy markantů jsou zobrazeny na obrázku. (Ščurek, 2008) (Soška, 2002)



Obrázek 4 : Základní typy markantů [10]

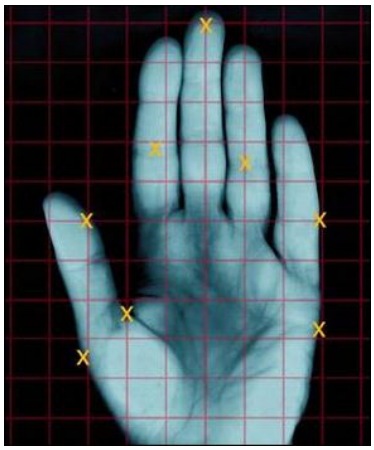
Za těchto podmínek je možno konstatovat, že hledané unikátní vlastnosti otisku prstu, které jej vynesly na mezi nejpoužívanější metody v identifikačních systémech. Jsou neměnné v čase, je velmi malá pravděpodobnost shody otisku a otisk prstu se nedá relativně odstranit. (Ščurek, 2008)

Pro zpracování otisku prstu je nutné převést otisk prstu do digitální podoby. Je nezbytné umožnit převod již získaných otisků prstů bez nutnosti jejich opětovného získávání. Jednou z možností jak dostat digitální otisk prstu je pomocí scanneru z inkoustového obrazu. Tento postup se využívá v kriminalistické praxi při převádění otisků do počítačové databáze. Pokud není možné skenovat z inkoustových obrazů, je potřeba spolupráce dané osoby a otisky se musí naskenovat pomocí elektronických snímačů. Senzory se rozdělují do dvou základních skupin kontaktní a bezkontaktní. (Flídr, 2009)

3.3.2 Identifikace podle geometrie ruky

Identifikace podle geometrie ruky je méně nepřesná oproti otisku prstu. Je to v podstatě pouze doplňková metoda, je určená spíš k verifikaci, nikoliv k identifikaci. Tato metoda se zabývá fyzikálními charakteristikami ruky a prstů z hlediska třídimensionální perspektivy. Při vývoji metody se začalo jednoduchým měřením délky prstu a nakonec se

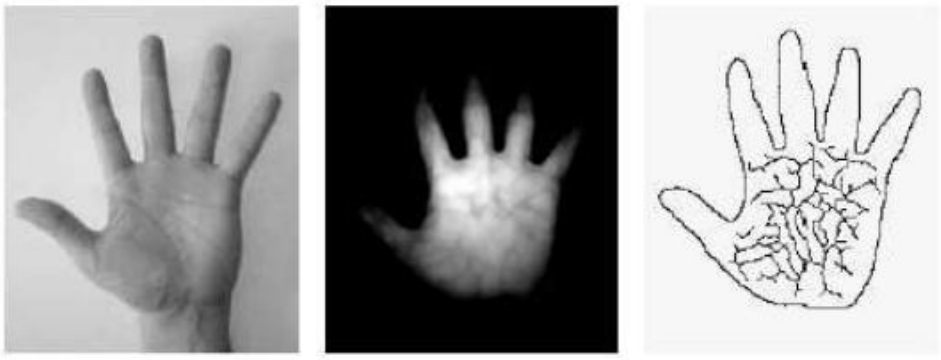
vyvinula do snímání tvaru ruky, to znamená, že se měří délka a šířka dlaně a jednotlivých prstů. Na snímaném obrazu ruky je možné najít přes 31 000 polohových a lze provést 90 různých měření vzdálenosti. Tvar ruky je snímán speciálním skenerem, který produkuje 3D fotografii (viz. Obrázek 5) a redukuje tato do 9 bitové hodnoty. Z toho vyplívá, že tato metoda není náročná na požadavky paměti systému. Tato metoda neřeší délku nehtů, povrchové poškození ruky nebo míru znečištění dlaně. (Soška, 2002) (Michálek, 2009)



Obrázek 5 : Snímek skenu geometrie ruky [7]

3.3.3 Identifikace podle tvaru krevního řečiště ruky

Identifikace podle tvaru krevního řečiště ruky je metoda s vysokou přesností, při níž není zapotřebí složitého zařízení. Algoritmy provádějící extrakci vzorků také nejsou příliš náročné. V této metodě se měří tvar krevního řečiště na dlani. Velkou výhodou této metody oproti geometrii ruky je, že do snímání nevstupují nečistoty, ani aktuální vlhkost kůže nebo drobná poranění. Při identifikaci se po přiložení ruky, pomocí infračerveného záření pořídí snímek s barevnou hloubkou 256 odstínů šedi. Žíly toto záření pohlcují a vytvářejí na snímku zřetelnou síť tmavých čar, které reprezentují jejich tvar. Takovýto obraz se poté převede na ekvivalentní černobílý obraz, který je v dalším kroku upraven tak, aby jednotlivé žíly byly na obrázku co nejtenčí. Na upraveném obrázku se poté provedou příslušná měření a výsledná data se porovnají s referenční šablonou. Na obrázku 6 vidíme jednotlivé fáze obrazu krevního řečiště lidské dlaně. (Michálek, 2009)



Obrázek 6 : Fáze získávání obrazu krevního řečiště [8]

3.3.4 Identifikace podle žil v zápěstí

Identifikace podle žil v zápěstí je metoda velice podobná metodě krevního řečiště. Tato metoda používá záznamy o podkožních žílách jako vzorku pro jednoznačnou identifikaci osoby. Technologie umožňuje vytvořit z takovýchto vzorků čárový kód pro každého jedince.

Obrázky žil jsou převedeny do binárního tvaru, zkomprimovány a uloženy ve srovnávací databázi 2D obrázku žil. Osoby jsou poté identifikovány pomocí odpovídajícího vzorku. Srovnání poté proběhne v čase kratším než 200 milisekund. Na obrázku 7 je zobrazena struktura žil v zápěstí. (Ščurek, 2008)

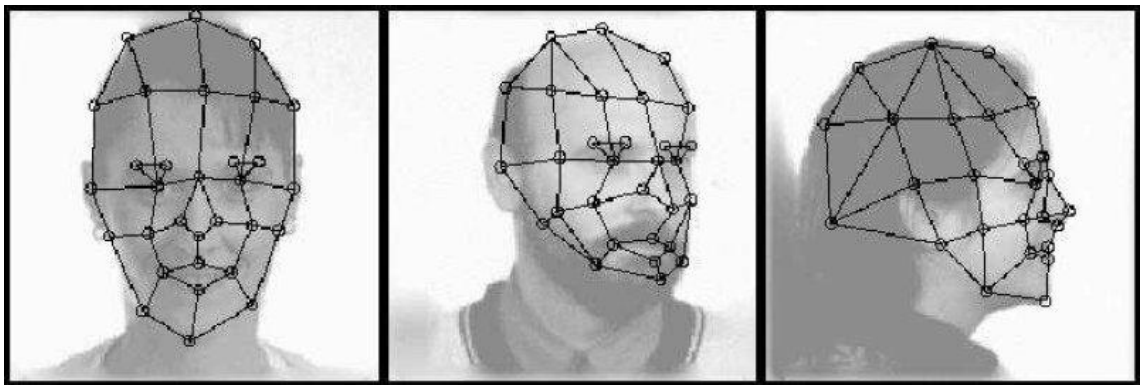
Obrázek 7 : Struktura žil v zápěstí [8]

3.3.5 Identifikace pomocí geometrie tváře

Identifikace podle obličeje dnes patří mezi nejvíce zkoumané metody, protože tato problematika je velmi rozsáhlá.

V identifikaci podle geometrie tváře se jedná o jednoznačné určení objektu. Identifikace je založena na porovnávacím procesu 1:N. Při identifikaci zde dochází k porovnávání hledaného obrazu obličeje s referenčními obličeji uloženými v databázi a hledají se podobnosti. Do databáze se nejčastěji ukládají obličeje pomocí vektorů. Tímto způsobem je zajištěna podobnost s odebraným vzorkem obličeje. Jedná se o proces, při němž jsou porovnávány jednotlivé vlastnosti obrazu, a je individuální téměř pro každou databázi. Nejprve je potřeba jednotlivé vlastnosti obrazu znormalizovat, to znamená pootočit je tak, aby byly srovnané podle os. Výsledky jsou následně seřazeny sestupně, podle nejvyššího počtu shod.

Jestliže je identita hledaného vzorku již potvrzena, jedná se o hledání 1:1. V dnešní době existuje mnoho algoritmů pro verifikaci, které pracují s různými metodami. K vyhodnocení těchto metod nám slouží tak zvaný verifikační poměr. Pomocí tohoto poměru se určí poměr mezi správným počtem povolených přístupů proti chybnému poměru povolených přístupů. Správně fungující systémy se pohybují na hranici těchto dvou metod. Závislé je to pouze na konkrétním použití a bezpečnostním stupni. (Říha, Rak, & Matyáš, 2008) (Xiaoguang, 2010) (Michálek, 2009)

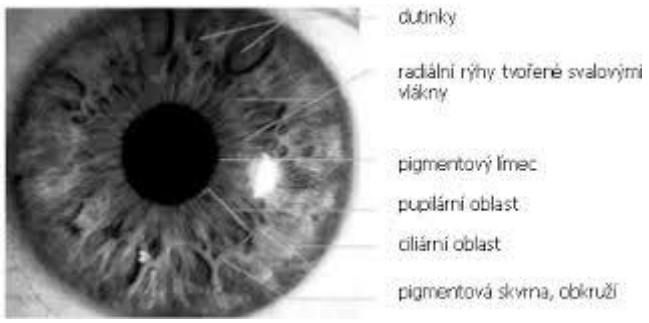


Obrázek 8 : Porovnávání obličeje pomocí vektorů [12]

3.3.6 Identifikace podle oční duhovky

Tato metoda identifikace využívá unikátnost oční duhovky. Duhovka je sval uvnitř oka, který reguluje velikost čočky na základě intenzity světla dopadajícího na oko. Oko je popsáno na obrázku 7. Duhovka je barevná část oka, jejíž zabarvení odpovídá množství melatoninového pigmentu uvnitř svaloviny. Zabarvení a struktura duhovky oka je geneticky závislá, ale její vzorkování není. Duhovka se vyvíjí během růstu plodu a její vzorkování je náhodné, tudíž je jedinečné pro každého člověka i pro dvojčata, dokonce i jeden člověk má každou duhovku jinou, což dělá tyto systémy nejpřesnějšími. Tyto systémy dosahují prakticky nulové pravděpodobnosti chybné identifikace osoby. Na oční duhovce se sledují čtyři hlavní rysy.

Sledují se krypty, to jsou tmavá místa a je zde duhovka poměrně tenká. Dále se sledují radiální rýhy, začínají poblíž zornice a paprskovitě vybíhají k okraji duhovky. Pigmentové skvrny jsou náhodné shluky pigmentových buněk na povrchu duhovky. A poslední rysem jsou pigmentové záhyby. (Soška, 2002)



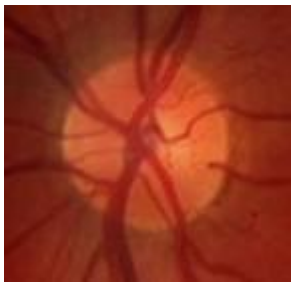
Obrázek 9 : Popis duhovky [8]

3.3.7 Identifikace podle sítnice oka

Sítnice je na světlo citlivý povrch zadní strany oka. Detail sítnice oka je vidět na obrázku 9. Skládá se z obrovského počtu specializovaných nervových buněk, které se nazývají tyčinky a čípky. Tyto buňky převádějí světelné paprsky na nervové signály. Čípky poskytují barevné vidění. Díky své husté koncentraci umožňují čípky nejostřejší vidění. Tyčinky jsou mnohem citlivější na světlo než čípky, ale poskytují pouze černobílé vidění. Každá tyčinka a čípek je spojen s nervy, jejichž signály vystupují z oka pomocí očního nervu. Oční nerv, společně s artérií sítnice, vystupují z oka v bodě, kde nejsou žádné cípky

ani tyčinky, jedná se o tzv. slepý bod na sítnici. Je možné prokázat tento slepý bod a lidé si ho jsou také obvykle vědomi.

Získání obrazu se provádí zaměřením infračerveného paprsku o nízké intenzitě skrz zornici na strukturu cév. Naskenovaný obraz je poté převeden do 40 bitového čísla. Tato metoda je velice přesná, ale bohužel má i spoustu nedostatků. Hlavní nedostatek je nutnost umístit identifikační zařízení na zeď, kde vzniká problém pro příliš vysoké nebo malé osoby. (Ščurek, 2008)



Obrázek 10 : Detail sítnice oka [15]

3.3.8 Identifikace podle ušního boltce

Jedná se o metodu, která využívá individuálního tvaru a stavby ušního boltce osoby. Existují tři metody identifikace podle ušního boltce:

- Podle morfometrického vztahu – geometrie ušního boltce, v 2D nebo 3D formě
- Podle otisku boltce – využívá se především ve forenzní oblasti, jinde se nepoužívá kvůli „nekomfortnosti“.
- Podle termogramu – využívá se termografického snímku, měří se rozložení tělesné teploty na boltci.

Pro komerční využití se využívá především metoda podle morfometrických vztahů. V tomto případě se je uživateli nasnímán ušní boltec speciálním optickým zařízením ze vzdálenosti do 1 metru. Data zanesená ve snímku jsou pak vyhodnocena a v závislosti na použitém typu algoritmu porovnána s příslušnou databází. U této metody je velkou

nevýhodou množství chyb vznikajících překrytím časti ušního boltce vlasy nebo pokrývkou hlavy. (Michálek, 2009)

3.3.9 Identifikace podle dynamiky podpisu

Základem je identifikace osoby na základě jejího podpisu s využitím velice spolehlivého biometrického zařízení. K tomu není potřeba nic více, než, aby se dotyčná osoba podepsala na speciální podložku pomocí speciálního pera. Systém ověřuje podpis osoby na základě srovnání s uloženým podpisovým vzorem, který charakterizuje jak, byl popis napsán. Není tedy důležitá podoba podpisu, i když o to jde samozřejmě také, nýbrž důraz je kladen na dynamiku podpisu, provedení tahu, síla, kterou tlačíme při psaní na podložku, rychlost psaní apod. To vše dohromady dává jednoznačnou charakterizaci našeho podpisu.

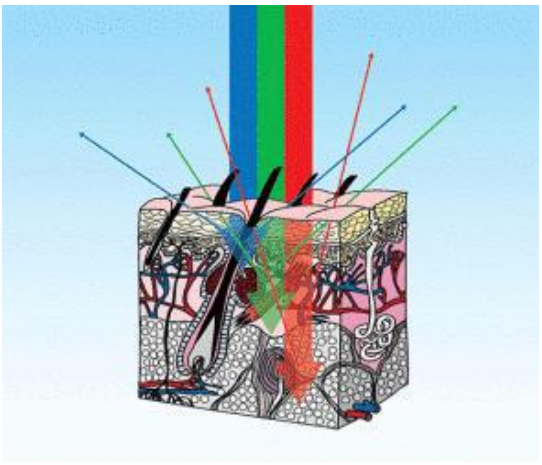
- tlak pera
- styl písma
- rychlost

Není stanoven limit pro styly a typy podpisu, jazyk podpisu. Každý podpis vyžaduje pouze 500 bitu, takže na větším serveru jich muže být uloženo až několik stovek tisíc, nebo data podpisu lze uložit na magnetickou kartu, do čipu apod. Používá se následující hardware: podložky citlivé na tlak, LCD, VGA displeje které snímají pozici v ose X a Y a tlak elektronického pera. (Woodward, Orlans, & Higgins, 2002) (Soška, 2002)

3.3.10 Identifikace podle spektroskopie kůže

Metoda identifikace podle spektroskopie kůže se zabývá lidskou kůží. Lidská kůže se skládá z několika vrstev. Tyto vrstvy jsou jedinečné pro každého člověka, mají různé tloušťky, jsou různě zvrásněné či zvlněné. Metoda je založena na ozáření části lidské pokožky světlem o více vlnových délkách. Více vlnových délek se zde používá z toho důvodu, že každé světlo se odráží či láme v jiné vrstvě pokožky. Odraz je poté zachycen a

porovnává se s již uloženým vzorkem. Na obrázku číslo 11 je vidět průnik světla pokožkou.(Ščurek, 2008)



Obrázek 11 : Průnik světla při spektroskopii [8]

3.3.11 Identifikace podle psaní na klávesnici

Dynamika stisku není tak úplně nová biometrická technologie, jak by se mohlo zdát. Dynamika úderů při vysílání v Morseovce pak byla specialistou porovnána s referenčním vzorkem k ověření pravosti zprávy.

Využití této metody v dnešní době je používáno pomocí klávesnice a přídavného zařízení, které snímá určitá kritéria, při psaní na klávesnici. (Soška, 2002)

3.3.12 Identifikace podle DNA

„ *Z pohledu definice biometrické identifikace je identifikace prostřednictvím analýzy DNA poněkud odlišná od ostatních biometrických metod, neboť nepracuje s měřitelnými morfologickými nebo fyziologickými znaky člověka, ale objektem jejího zájmu je výhradně sám nosič genetické informace – molekula DNA.“* (Říha, Rak, & Matyáš, 2008)

DNA je jako identifikační prvek používáno opět v policejní praxi, a to od druhé poloviny osmdesátých let. Struktura DNA je odlišná u všech lidí s výjimkou jednovaječných dvojčat a s věkem se nemění. Přesnost zkoumání DNA je důvodem pro stále širší využití této technologie i přesto, že získávání otisků DNA představuje poměrně náročnou a zdlouhavou proceduru, která zahrnuje pět kroků:

1. Izolace DNA – DNA se získává z buněk nebo tkání těla, jako je krev, vlasy nebo kůže.

2. Rozštěpení a třídění - Speciální enzymy nazývané restrikční enzymy se používají na štěpení DNA na určitých místech. Kousky DNA jsou setříděny podle velikosti prosévací technikou zvanou elektroforéza. Kousky DNA se nechají projít gelem vyrobeným z agarosy.

3. Přenos DNA do nylonu - Části DNA se umístí na plochou desku gelu. Gelem prochází elektrický proud. Protože DNA je nabitá záporně, pohybuje se směrem ke kladné elektrodě. Čím menší fragment DNA, tím rychleji se pohybuje. V tomto procesu se vlákna každého segmentu DNA chemicky rozštěpí.

4. Sondování - Přidání radioaktivních nebo obarvených genových sond do nylonové membrány přinese vzorek, jehož rentgenový snímek se nazývá DNA-otisk. Každá sonda typicky ulpí jen na jednom nebo dvou specifických místech na nylonové membráně.

5. DNA otisk - Konečný DNA-otisk se vystaví užitím několika sond současně. To se podobá čárovým kódům, a proto je snadné jej převést do elektronické podoby.

Takto získaná informace slouží k řešení celé řady otázek od přiznání otcovství až po identifikaci těl. Mnohé armády či záchranářské sbory proto budují databáze DNA svých zaměstnanců. Pro kontrolu přístupu v reálném čase však zatím tato technologie není použitelná. (Soška, 2002)

3.3.13 Identifikace podle akustické charakteristiky hlasu

Při rozpoznávání hlasu uživatel vysloví slovo a systém určí, které slovo v databázi odpovídá této výslovnosti. Toto určení systém provede na základě porovnání vyřčené výslovnosti s množinou výslovností uloženou v databázi a výběrem té, která vzhledem k ostatním slovům v této množině vyhovuje vyřčenému nejlépe.

„ Podstatou této biometrické metody je elektronická analýza řeči identifikované osoby. Lidská řeč je charakteristická svým subjektivním vlivem osobnosti mluvčího (barva hlasu, rytmus atd.), akustickou a lingvistickou strukturou (gramatika a skladba řeči). Zdrojem řečových kmitů jsou řečové orgány, tzv. vokálový trakt, který je složen z hlasivek, ústní dutiny, jazyka a zubů, přičemž tvar těchto orgánů způsobuje, že rezonance vokálního traktu je u různých osob dostatečně odlišná.

K výhodám této identifikace patří rychlost, spolehlivost, jednoduchost na použití, nízká cena a také zde není zapotřebí žádné speciální hardwarové zařízení.

Nevýhodou je to, že verifikace může být za určitých okolností (nastydnutí, šum okolí, atd.) mnohem komplikovanější než u jiných biometrik“. (Ondrůšek, 2006)

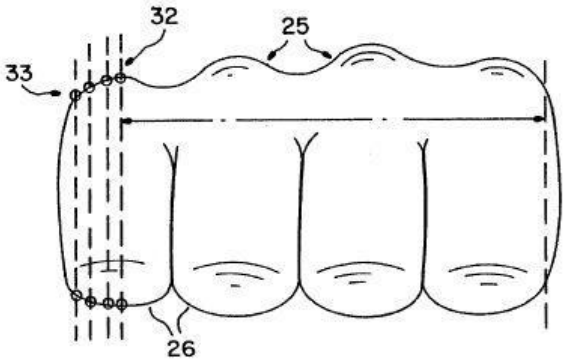
3.3.14 Identifikace podle podélného rýhování nehtů

Identifikace se provádí pomocí čárové nerovnosti na nehtu. Tato nerovnost je dána podle struktury lůžka na nehtu, kterou nerovovnost kopíruje. Pro každého jedince je struktura unikátní. Metoda funguje na principu nasvícení polarizovaného světla na nehet a jeho odrazu do speciálního čtecího zařízení. Odraz se poté zobrazí jako číselná sekvence, která se také nazývá jako „čárový kód“. (Soška, 2002)

3.3.15 Identifikace podle tvaru článků prstu v pěsti

Identifikace podle tvaru článků prstu v pěsti se provádí biometrická měření na sevřené dlani ve vnější části. Metoda využívá principu vyfocení cílové části, na které poté proběhne měření. Podle potřeby na přesnost je možné využít až 35 parametrů měření. U

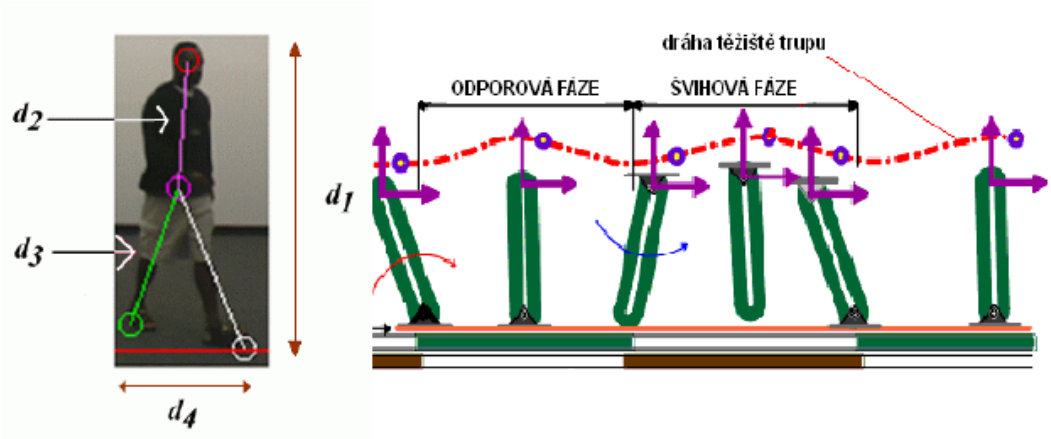
této metody se opět používá porovnávání s již uloženým vzorem v paměti počítače. Způsob měření je vidět na obrázku 11. (Ščurek, 2008)



Obrázek 12 : Způsob měření tvaru prstu v pěsti [8]

3.3.16 Identifikace podle dynamiky chůze

Dynamika chůze je prakticky u každého člověka jedinečná a svým způsobem v čase neměnná. Princip identifikace podle dynamiky chůze je podobný jako u identifikace podle podpisu. Metoda tedy funguje na základě porovnávání křivek drah pohybů, které opisují určité body na lidském těle, tedy hlavně jeho těžiště. Postup vytváření dráhy těžiště je vidět na obrázku 11. Tato metoda má obrovský potenciál a význam při identifikaci pachatelů při loupežných přepadení, jež nelze identifikovat pomocí žádné jiné metody, kvůli jejich převlečení a maskování. V současné době prozatím neexistuje databáze pro srovnávání získaných vzorků. (Ščurek, 2008)



Obrázek 13 : Postup vytváření dráhy těžiště trupu [9]

3.3.17 Identifikace pomocí bioelektrického pole

Bioelektrická pole jsou v podstatě neviditelná bioelektrická vlnění, která má každá osoba. Toto vlnění je jedinečné pro každou osobu stejně jako identifikace podle DNA. Tato pole lze zaznamenat detektorem pro toto určený, který zjistí bioelektrické pole osoby, které právě prochází kolem snímače. Nevýhodou tohoto snímače je, že nedokáže identifikovat více osob najednou. To znamená, že nejprve musí kolem snímače projít jedna osoba a až po identifikaci první osoby může projít další. (Ščurek, 2008)

3.3.18 Identifikace podle plantogramu

Jedná se o identifikace pomocí stopy bosé nohy. Tato identifikace se prozatím využívá v kriminalistice, kde jsou zajištěny otisky nohou na místě činu a ty jsou poté porovnávány s podezřelými ze spáchaného činu. Plantogram je unikátní pro každou osobu. Plantogramy v podstatě odrážejí vnitřní stavbu chodidla, jako jsou například různé záhyby kůže nebo se dá dokonce odhadnout i váha dané osoby. Na plantogramu se měří 5 základních měření. (Ščurek, 2008)

3.4 Rozhraní biometrických snímačů

V této kapitole se práce zabývá jednotlivými komunikačními, kterými jsou nejčastěji vybaveny biometrické snímače. Setkáváme se zde se 3 rozhraními, jsou to RS232, Wiegand a Ethernet.

RS232 – jedná se o standartní rozhraní pracující na fyzické vrstvě. Je určeno k obousměrné komunikaci dvou zařízení. Počet datových bitů je volitelný, ale obvykle se používá komunikace s 8 bity. Nevýhodou tohoto rozhraní je omezená délka, která bývá okolo 15 metrů.

Wiegand – je jednosměrné rozhraní. Používá se především pro docházkové systémy. Komunikační záznamy se zde přenáší s délkou 26 až 40 bitů. Délka rozhraní může být až 125 metrů.

Ethernet – jedná se o obousměrné síťové rozhraní, pracující na síťové vrstvě. Z těchto rozhraní využívá největší přenosovou rychlost dat. Délka tohoto rozhraní může být až 100 metrů. (Michálek, 2009)

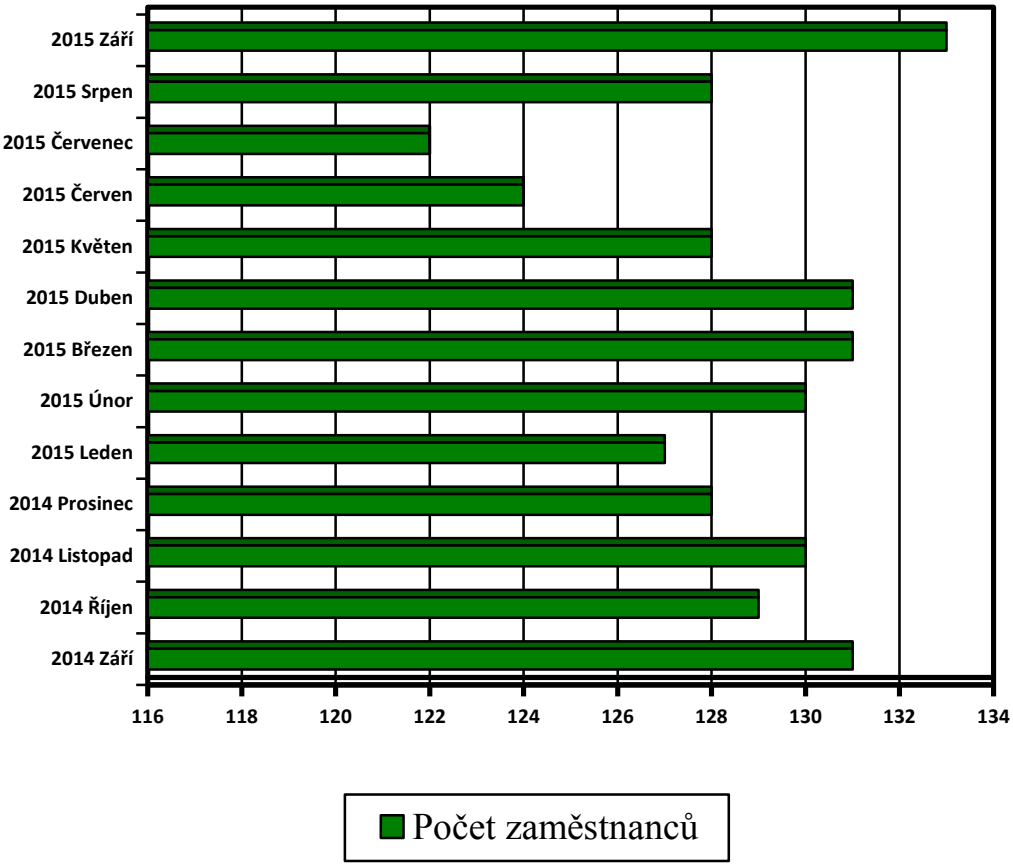
4 Praktická část

Cílem praktické části je návrh řešení biometrického terminálu pro středně velkou firmu a následná implementace a srovnání s předešlým docházkovým terminálem, jak z hlediska finančního, tak i z hlediska funkčního. V tomto případě bude prováděn návrh v konkrétní firmě Kemmler Electronic.

Pro první část jsou zjištěny údaje o počtech zaměstnanců a docházkovém terminálu z firmy Kemmler Electronic. Ve druhé části bude navrhnuto nové řešení pro docházku pomocí jedné biometrické vlastnosti. Nakonec budou tyto dva terminály porovnány mezi sebou.

Firma Kemmler Electronic byla založena v roce 1986 v Německu. Pobočka v Čechách v Rožmitále pod Třemšínem byla otevřena v roce 1996. Firma se zabývá výrobou kabelových souprav pro automobilový průmysl. Jedná se tedy o poměrně čisté pracovní prostředí. Ve firmě je aktuálně zaměstnáno 131 zaměstnanců.

Graf 1 : Počet zaměstnanců za poslední rok



4.1 Starý docházkový systém

Firma Kemmler Electronic využívá k docházce pouze jeden docházkový terminál kolem, kterého musí projít všichni zaměstnanci, než se vydají na určené pracoviště. Terminál je umístěn před příchodem do výrobní haly.

Firma používá bezkontaktní docházkový terminál od firmy Ron Software. Tento terminál je typu RT300-TPC. Cena tohoto terminálu je 11 900 Kč. Terminál je velice jednoduchý pro používání, stiskne se pouze daný požadavek a přiložíte kartu nebo čip a terminál zachytí a připíše k dané osobě. Což dělá tento terminál uživatelsky velice příjemným. Terminál pracuje i v off-line modu to znamená, že je schopen uchovávat data v interní paměti přístroje, které je poté možno přenést do počítače pomocí flash paměti.

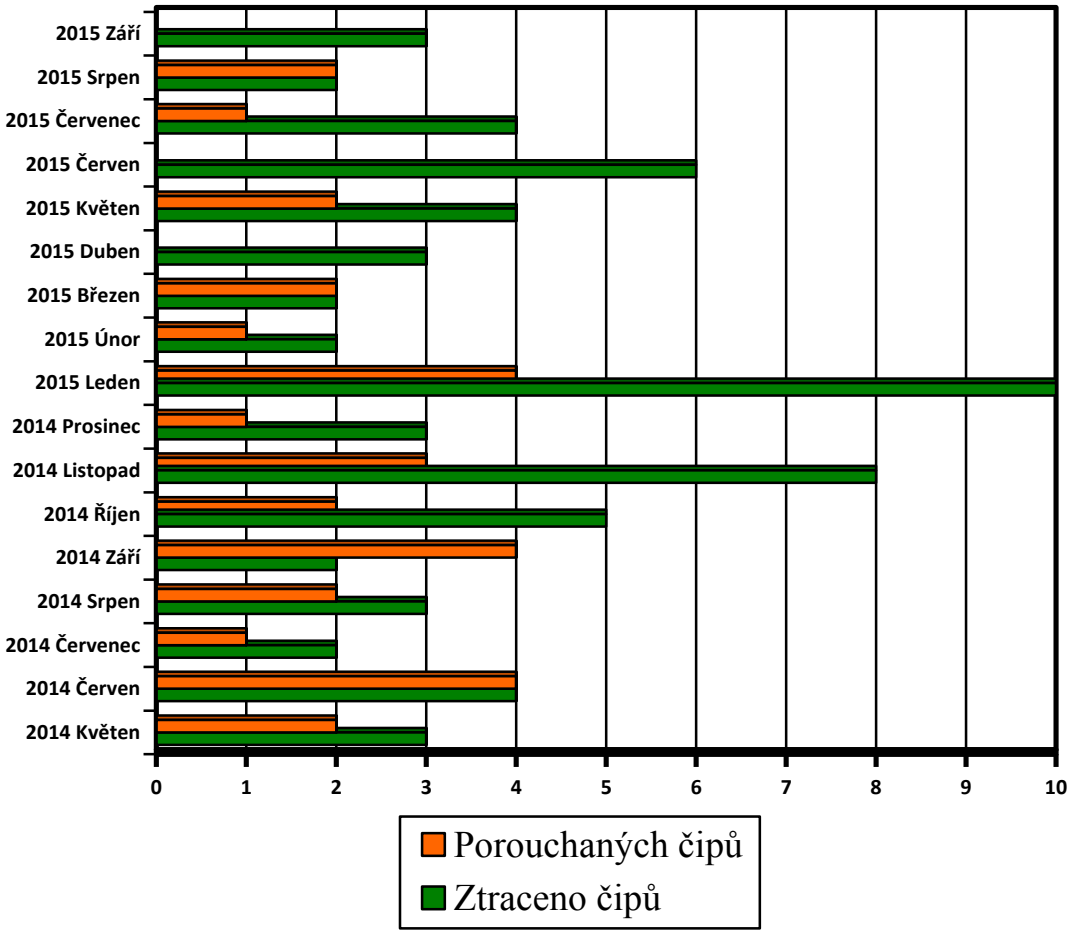
Nedostatky terminálu jsou, že si sám zaměstnanec nemůže pomocí něj podívat na stav své docházky, zůstatek dovolené a podobně. To znamená, že v případě když si zaměstnanec chce ověřit hodnoty své odpracované doby nebo stav dovolené musí se dojít zeptat na personální oddělení, kde mu předají tyto informace.

Obrázek 14 : Docházkový terminál RT300-TPC [13]

4.1.1 Docházkové karty/čipy

Při nákupu terminálu bylo spolu s ním nakoupeno 200 přístupových karet. Cena jednoho přístupové karty je 39,70 Kč. Do května roku 2014 byly používány pouze tyto přístupové karty. Do již zmíněného data se nezaznamenávaly počty ztracených docházkových médií. Nic méně bylo zaznamenáno větší množství porouchaných přístupových karet. To znamená, že se firma rozhodla pořídit dalších 100 přístupových médií. Ale už nebyly nakoupeny karty, ale čipy. Cena čipů a karet je totožná.

Graf 2 : Přehled ztracených a porouchaných médií



Z výše uvedeného grafu je patrné, že firma se potýká s velice velkou ztrátovostí docházkových médií. Je zde také vidět, že v některých obdobích v roce jsou tato čísla vyšší, než je obvyklé. Jsou zde tedy tendence ztrácet více čipů či karet v období letních dovolených a přes Vánoční svátky. Celkový počet ztracených médií za 16 měsíců je 66 kusů. Celkový počet porouchaných nebo nějakým způsobem znehodnocených karet je 31 kusů. V průměru to odpovídá 6 ztraceným médiím měsíčně, což je 238,20 Kč.

4.1.2 Celková cena starého docházkového systému

Při nákupu tohoto terminálu bylo potřeba ještě koupit programové vybavení pro docházku. Cena docházkového programu pro 200 zaměstnanců je 25 800 Kč. Dále byly nakoupeny docházková média v počtu 300 kusů. Cena jedno kusu tohoto média je 39,70 Kč. To znamená, že cena pořízených docházkových médií je 11 910 Kč.

Po součtu všech položek cena funkčního docházkového systému je 49 610 Kč. Do součtu nebude započítána cena za instalaci docházkového systému. Celková hodnota ztracených docházkových médií je 3 850,90 Kč.

4.2 Požadavky na nové řešení

Mezi hlavní požadavky na nové řešení patří:

- V terminálu bude možné přednastavit pracovní dobu pro jednosměnný, dvousměnný, třísměnný provoz a turnusový provoz.
- Dále bude možné na terminálu přednastavit základní operace pro snadné používání, například možnosti jako je lékař, nemoc a tak podobně.
- Terminál nebude používat žádná docházková média
- Terminál bude mít možnost, aby zaměstnanec možnost zkontrolovat svojí docházku, zůstatek dovolené a podobně.
- Terminál bude uživatelsky přívětivý.
- Terminál bude využívat ethernet rozhraní.
- Systém bude co možná nejlevnější.

4.3 Výběr nového řešení

Existuje velké množství terminálů pro zaznamenávání docházky pomocí desítek biometrických vlastností. Pro sestavení tabulky je použit model vícekriteriální analýzy variant. Model vícekriteriální analýzy potřebuje k výpočtu obodované varianty. Dále je

potřeba znát hodnoty vah kritérií. Jsou zvoleny 3 hlavní kritéria. Jsou to kritéria cena, komfortnost a přesnost. Největší váhu bude mít kritérium cena 0,4. Přesnosti a komfortnosti identifikace budou přiřazeny totožné váhy 0,3. Jednotlivá kritéria jsou ohodnocena od 1 do 5, přičemž 1 je nejlepší a 5 je nejhorší hodnota. Hodnocení jednotlivých kritérií probíhá tak, že v daném kritériu se najde nejlepší varianta a podle té jsou poté porovnány všechny ostatní varianty. Kritérium přesnost je založeno, na pravděpodobnosti nesprávného přijetí a nesprávného odmítnutí. Nejlepší hodnoty v tomto kritériu získali metody podle DNA, duhovky oka a sítnice oka. Ostatní varianty poté byly ohodnoceny podle toho, o kolik byli horší než tyto zmíněné metody. Kritérium komfortnost je ohodnoceno podle uživatelské přívětivosti, to znamená, že sledovanou veličinou v tomto případě je rychlost identifikace a podle toho jak je uživateli nepříjemná identifikace. V tomto případě je nejlepší varianta identifikace podle geometrie tváře, rychlost identifikace je v tomto případě o něco pomalejší než u ostatních metod, ale je to uživatelsky nejpříjemnější metoda identifikace. Nejhůře v tomto kritériu dopadla identifikace podle DNA. V kritériu cena hodnocení začíná až od hodnoty 2 je to z důvodů, že biometrické terminály jsou pořád cenově méně dostupné než klasické terminály. Nejlepší hodnoty zde získaly metody identifikace podle otisku prstu, geometrie prstu a podpisu. Ostatní varianty opět seřazeny podle toho, o kolik byly horší než tyto zmíněné.

Tabulka 1 : Porovnání jednotlivých biometrických metod

	Přesnost	Komfortnost	Cena	Výsledek
Podle DNA	1	5	5	3,8
Podle geometrie prstu	3	2	2	2,3
Podle struktury žil v zápěstí	2	2	4	2,8
Podle tvaru ucha	3	4	3	3,3
Podle geometrie ruky	2	2	3	2,4
Podle geometrie tváře	2	1	4	2,5
Podle podpisu	4	4	2	3,2
Podle duhovky oka	1	3	5	3,2
Podle sítnice oka	1	3	5	3,2
Podle otisku prstu	2	2	2	2
Váhy kritérií	0,3	0,3	0,4	

Další důležitá vlastnost u biometrických vlastností je stálost v čase, aby nemohlo dojít k její kompromitaci se stárnutím člověka. Je zde několik důvodů proč se může změnit. Je to například vliv růstu živé tkáně, biologické stárnutí, špína a nečistoty, zranění a následné hojící procesy.

Z výše uvedené tabulky vyplívá, že v úvahu připadají snímače, které snímají otisk prstu, geometrie tváře a geometrie ruky a prstu. Snímání geometrie tváře je sice pro uživatele nejkomfortnější, ale cena je příliš vysoká, když se zde jedná pouze o zaznamenávání docházky. Snímání podle geometrie ruky je taktéž příliš drahé. Dále je zde ještě geometrie prstu, cena je totožná s otiskem prstu, ale má menší přesnost, to znamená, že je zde větší riziko nastání chyby při identifikaci než u otisku prstu.

Je vybrán docházkový systém na otisky prstů. Hlavním důvodem pro toho řešení je, že patří aktuálně mezi nejdostupnější a nejlevnější systémy. Řešení docházkového systému otisky prstů je vyhovující díky komfortnosti, kdy zaměstnanec pouze přiloží prst a během pár vteřin je zaznamenáván příchod či jiná možnost na terminálu. Dále je toto řešení plně dostačující, co se týče bezpečnosti, který vyžadován ve firemním prostředí. Pracovní prostředí v této firmě je relativně čisté tudíž se nebude stávat, že se snímač zanese nějakou nečistotou a nebude správně snímat otisky prstu.

4.4 Nový terminál

Byl vybrán terminál FT500F-TPC, hlavním důvodem výběru tohoto terminálu je ten, že se zde dají použít stávající kabelové rozvody. Při výměně terminálu bude totiž nutné pouze vyměnit tyto terminály mezi sebou. Tento terminál má vlastní paměť a je možné zde uložit až 1 milion záznamů. Je zde možný export dat do externího mzdového programu, nastavení až 20 typů průchodů na čtečce. Zaměstnanec má zde možnost zjistit si svoji odpracovanou dobu nebo zůstatek dovolené. Tento terminál také využívá ethernet rozhraní.

Hlavní výhodou biometrického terminálu je, že prakticky pro běžného zaměstnance není možnost jak falšovat docházku a nemožnost předávat si přístupové údaje, čímž se zvýší pravdivost o odpracovaném čase. Tím se dá vyhnout rozepřemi mezi zaměstnanci, jelikož každý zaměstnanec odpracuje skutečnou pracovní dobu. Další výhodou tohoto

terminálu je, že nebude docházet nezapisování docházky z důvodů zapomenutí, ztráty nebo znehodnocení přístupové karty nebo čipu.

Obrázek 15 : Biometrický terminál FT500F-TPC [14]

4.4.1 Cenová bilance nového docházkového systému

Cena pořízení terminálu FT500F-TPC je 23 700 Kč. K zařízení je také nutné pořídit programové vybavení pro vedení docházky. Bude zvolena licence pro 200 zaměstnanců, které stojí 25 800 Kč. Do programového vybavení bude potřeba ještě dokoupit software pro správu otisků prstů, v hodnotě 3000 Kč. Celková hodnota nového docházkového řešení je 52 500 Kč.

4.4.2 Postup implementace nového terminálu

Postup implementace nového řešení terminálu bude následující:

1. Softwarová instalace nových čteček se zaškolením obsluhy – V tomto bodě implementace je nutné nainstalovat daný software, díky kterému bude spolupracovat terminál s počítačem. Nutné je ještě zaškolit personál, který se stará o docházku zaměstnanců. Tato část implementace zabere maximálně dva dny.

2. Načítání otisků prstů pracovníků a ověřování funkčnosti nového terminálu – Operace načítání otisků prstů bude z hlediska časového nejnáročnější. Časová náročnost se bude odvíjet od počtu zaměstnanců a počtu zvolených prstů. V tomto případě budou navrženy 2 prsty z každé ruky. Je to z důvodů manuální práce a může se stát, že se nějakému zaměstnanci při práci poškodí bříška prstů. Hlavní důvod je předejít nepříjemnému čekání pro zaměstnance, v případě že dojde k poškození prstu, zaměstnanec použije k autentizaci pouze jiný prst, který již bude zaregistrován.

3. Výměna stávajícího docházkového terminálu – Tato část implementace bude nejméně časově náročná, pouze se vymění mezi sebou na určeném místě.

4.5 Porovnání systémů

V této části jsou porovnány z finančního hlediska oba docházkové systémy. Ceny jsou uváděny bez DPH. Ceny porovnávaných systém jsou v aktuálních cenách, které firma uvádí ve svých cenících. Do ceny biometrických systémů nejsou zahrnuty náklady na instalaci software, implementace zařízení, školení zaměstnanců a ostatní náklady spojené se zprovozněním systému. Je to z toho důvodu, že ty náklady jsou individuální a nikdo není schopen reálně určit cenu těchto nákladů.

Tabulka 2 : Porovnání ceny starého a nového docházkového systému

	Starý systém	Nový systém
Cena terminálu	11 900 Kč	23 700 Kč
Cena software pro docházku	25 800 Kč	25 800 Kč
Docházkové karty/čipy	11 910 Kč	0 Kč
Celková cena systému	49 610 Kč	52 500 Kč
Cena ztracených karet/čipů	3850,90 Kč	0 Kč
Celková cena i se ztracenými docházkovými kartami/čipy	53 460,90 Kč	52 500 Kč

Z výše uvedené tabulky kde jsou uvedeny ceny obou docházkových systému, je patrné, že cena software pro docházku je totožná. Cenový rozdíl vzniká při rozdílných cenách terminálů. Cenový rozdíl mezi starým a novým docházkovým terminálem činí 11 800 Kč. V tomto případě se zde jedná o konkrétní podnik, ve kterém se terminál využíval už nějakou dobu. Proto je zde poměrně vysoká cena za docházková média, cena činí 11 910 Kč. To znamená, že rozdíl v celkové ceně těchto dvou docházkových systémů je 2 890 Kč. V případě, že k tomuto rozdílu je přičtena hodnota ztracených docházkových médií, která činí 3 850, 90 Kč. Je zjištěno, že nový docházkový systém se stává levnější o 960, 90 Kč. V případě, že bude pokračovat podobná ztrátovost docházkových médií i v budoucnu bude se nový systém stávat stále výhodnější.

Co se týče funkčního hlediska terminálu, tak biometrický terminál nám zaručí, že každý zaměstnanec setrvá na svém pracovišti až do skončení pracovní doby. Nebude se stávat, že zaměstnanec nechá svojí docházkovou identifikaci jinému spolupracovníkovi, který za něho potom zapíše odchod do terminálu. To znamená, že se zvýší pravdivost údajů o docházce zaměstnanců. Mezi další pozitiva pro zaměstnavatele patří, že díky tomu že zaměstnanci budou setrvat na svých pozicích, se bude zvyšovat produktivita práce. Zaměstnavatel i v tomto případě ušetří a platí reálně odpracované hodiny.

4.6 Výsledky praktické části

Výsledek práce je metodika pro vhodný výběr docházkového terminálu pro středně velký podnik. V tomto případě se jednalo o konkrétní podnik, který měl určité požadavky na nový docházkový terminál. Mezi tyto požadavky patřili hlavně nízká cena, přijatelná uživatelská přívětivost a přesnost. Proto byly stanoveny váhy jednotlivých kritérií, kde největší váhu měla hodnota cena, měla hodnotu 0,4. Ostatní váhy kritérií byly podle požadavků zvoleny 0,3. Díky takto zvoleným váhám kritérií, bylo vybráno právě řešení na otisky prstů. V případě, že by se jednalo o jiný podnik s jinými požadavky na docházkový terminál, změnily by se i váhy těchto kritérií a došlo by k výběru jiného docházkového terminálu, který využívá jinou biometrickou vlastnost.

V tomto konkrétním případě, při srovnávání cen docházkových systémů bylo zjištěno, že se ceny těchto systému po započítání ztracených docházkových médií liší o 960,90 Kč ve prospěch nového biometrického systému. Je to z důvodů vysoké ztrátovosti v tomto podniku.

5 Závěr

Začátek práce byl zaměřen na popis obecných postupů a fungování jednotlivých biometrických autentizačních metod, kde byla snaha o zachycení dnes nejvíce používaných biometrických metod. Některé z těchto biometrických metod se dnes nepoužívají, protože jsou stále ve fázi vývoje. Bylo zjištěno, že některé z těchto metod jsou používány spíše v komerční sféře především jako kontrola vstupu, je to například identifikace podle obličeje. Zatímco ve forenzní sféře se spíše používají metody, jako je identifikace podle DNA.

V praktické části byl řešen problém výběru biometrického terminálu pro středně velký podnik. Tento problém byl řešen na konkrétním podniku, který poskytl informace o docházkovém systému. Na základě zjištěných údajů byly stanoveny nároky konkrétního podniku na nový docházkový terminál a podle toho byly poté určeny váhy pro výběrovou tabulku. Výběrová tabulka byla zhotovena pomocí modelu vícekriteriální analýzy variant. Pomocí této výběrové tabulky bylo vybráno řešení, které používá k identifikaci otisk prstu. Byl vybrán terminál FT500F-TPC, který nejvíce odpovídal daným požadavkům konkrétního podniku. Na základě porovnání biometrického a starého docházkového systému po započítání ztracených médií vyšel cenově výhodněji biometrický systém. Biometrický terminál byl výhodnější i z hlediska funkčního.

Tuto práci by bylo možné dále rozšiřovat a zabývat se detailněji celým docházkovým systémem. Porovnávat jednotlivé programové vybavení pro vedení docházky. Dále by se práce mohla rozšiřovat i o programy pro vedení mzdového účetnictví. Programy pro vedení docházky by mohly být testovány z hlediska spolupráce s programy pro vedení mzdového účetnictví.

6 Seznam použitých zdrojů

[1] BOLLE, R. Guide to Biometrics. Springer Science & Business Media, 2004. ISBN 0387400893, 9780387400891.

[2] BOULGOURIS, N. -- PLATANIOTIS, N. -- MICHELI-TZANAKOU, E. Biometrics: Theory, Methods and Applications. John Wiley & Sons, 2009. ISBN 0470522348, 9780470522349.

[3] ČANDÍK, M. Objektová bezpečnost II, UTB ve Zlíně, 2004. ISBN 8073182173, 9788073182175.

[4] JAIN, A. -- FLYNN, P. -- ROSS, A. Handbook of Biometrics. Springer Science & Business Media, 2007. ISBN 0387710418, 9780387710419.

[5] ŘÍHA, Z. -- RAK, R. -- MATYÁŠ, V. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

[6] WOODWARD, J. -- ORLANS, N. -- HIGGINS, P. Biometrics: Identity Assurance in the Information Age. Osborne, 2002. ISBN-13: 978-0072222272.

[7] KOLÁČEK, J. Šifrování a biometrie pod drobnohledem [online]. [cit. 20. 02. 2009] dostupný z <http://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723-3>.

[8] ŠČUREK, R. Biometrické metody identifikace osob v bezpečnostní praxi. Ostrava: VŠB TU, 2008 [online]. Dostupný z <http://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf>.

[9] Server BIOMECH.FTVS.CZ, [online]. Dostupný z <http://www.biomech.ftsv.cuni.cz>.

[10] Web krimi-spk.sweb.cz, [online]. Dostupný z <http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm>.

[11] Adamec, Lukáš. Srovnávací testy vybraných biometrických zařízení [online]. Datum: 2009 [cit. 2010-03-25]. Dostupný z <http://is.muni.cz/th/208425/fi_b/Srovnavaci_testy_vybranych_biometrickych_zarizeni.pdf>.

[12] Xiaoguang, Lu. 3D tvar tváře pomocí uzlové sítě [online]. Michigan State University. Strana 17. Datum: 21. 7. 2005 [cit. 2010-03-14]. Dostupný z <http://www.face-rec.org/interesting-papers/General/ImAna4FacRcg_lu.pdf>.

[13] Terminál rt300, Ron.cz, [online]. Dostupný z < http://www.ron.cz/www/cz/terminal-rt300/>.

[14] terminal biostation, Ron.cz, [online]. Dostupný z < http://www.ron.cz/www/cz/terminal-biostation/>.

[15] VOLNÝ, O. Sítnice. [online]. Dostupný z < http://cs.medixa.org/nemoci/sitnice>.

[16] MICHÁLEK, L. Aplikace biometrických prvků v docházkových systémech. [online]. Dostupný z < https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=18526>.

[17] HöLL, K. Aplikace metod detekce a rozpoznávání obličeje. [online]. Dostupný z < https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=82657>.

[18] FLÍDR, J. Biometrické autentizační metody. [online]. Dostupný z < https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=17183>

[19] ONDRŮŠEK, R. Identifikační biometrické prostředky. [online]. Dostupný z <http://digilib.k.utb.cz/bitstream/handle/10563/743/ondr%C5%AF%C5%A1ek_2006_bp.pdf?sequence=1>

[20] SOŠKA, L. Biometrie. [online]. Dostupný z <Https://akela.mendelu.cz/~lidak/bif/soska.doc>