Studie využití biometrických systémů v průmyslu komerční bezpečnosti

Study about application of biometric systems in the industry of commercial security

Hana Talandová

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Hana TALANDOVÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Studie využití biometrických systémů v PKB**

Zásady pro vypracování:

1. **Seznámení s problematikou biometrických systémů v průmyslu komerční bezpečnosti.**
2. **Členění biometrických systémů využívaných v PKB, princip činnosti a technická charakteristika.**
3. **Využití biometrických systémů v praxi.**
4. **Nové trendy v dané oblasti.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Laucký Vladimír. Technologie v komerční bezpečnosti I, Univerzita Tomáše Bati ve Zlíně 2004, ISBN 80-7318-194-0**
2. **Roman Rak, Václav Matyáš, Zdeněk Říha a kolektiv, Biometrie a identita člověka ve forenzních a komerčních aplikacích, Praha : Grada, 2008, ISBN 978-80-247-2365-5**
3. **Čandík, Marek,. Objektová bezpečnost II /. Vyd. 1. Zlín : Univerzita Tomáše Bati, 2004. 100 s. : ISBN 8073182173**
4. **Křeček, Stanislav. Příručka zabezpečovací techniky /. Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. : ISBN 80-902938-2-4**
5. **Ashbourn, J.: Practical Biometrics – From Aspiration to Implementation, Springer Verlag, 2004, ISBN 1-85233-774-5**
6. **Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W.: Guide to Biometrics, Springer Verlag, 2004, ISBN 0-387-40089-3**

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

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Bakalářská práce pojednává o využití biometrických metod k identifikaci/verifikaci osob v průmyslu komerční bezpečnosti. V teoretické části objasňuje pojem biometrie a uvádí metody biometrické identifikace. U každé metody uvádí princip činnosti a vhodnost použití. V praktické části je uvedena situace na českém a slovenském trhu s biometrickými technologiemi. Bakalářská práce je zakončena návrhem zabezpečení pomocí biometrické technologie.

Klíčová slova: biometrie, identifikace, verifikace, biometrické technologie

ABSTRACT

Bachelors work deals with using Biometric methods to dentification / verification people in the industry of commercial security. In theory it clarifies biometric concept and presents methods in biometric identification. Every method shows the principle of activities and advisable use. In the practice part there is a given situation in the Czech and Slovak market with biometric technologies. The Bachelors work is finished with a proposal of securing the need for biometric technology.

Keywords : biometry, identification, verification, biometric technology

Poděkování, motto

Tímto si dovoluji poděkovat své rodině za morální a finanční podporu během studia. Také bych ráda vyjádřila své poděkování Ing. Petru Navrátilovi, Ph.D. za kvalitní a odborné vedení, připomínky a poskytnuté konzultace při zpracování mé bakalářské práce. Dále bych chtěla poděkovat Ing. Petru Kováči za poskytnutí odborné konzultace.

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

Již několik tisíc let před naším letopočtem využívali lidé vlastností biometrické unikátnosti. Můžeme se setkat s otisky dlaní v jeskyních na nástěnných malbách, znamenající podpis autora.

V současné době je biometrickým systémům věnovaná zvýšená pozornost. S velice rychlým rozvojem výpočetní technologie, je umožněna automatizace biometrické identifikace a její následné využití v praxi. Současný rozvoj technologií a zároveň snížení cen a nákladů, napomohly k rozšíření biometrické technologie do komerční sféry. Nyní se můžeme setkat s biometrickými systémy zajišťující identifikaci osob vstupujících do střeženého objektu (banky, letiště, státní budovy apod.), rozpoznávání osob v davu umístěných v databázi hledaných osob nebo umožňující přístup k výpočetní technice. Můžeme se setkat s obavami a nedůvěrou uživatelů plynoucích z neznalosti principu funkčnosti biometrických systémů. Mezi jejich obavy patří strach o své zdraví (v případě snímání oční sítnice) nebo z nedostatečného zabezpečení. Proto je třeba podat uživateli dostatek informací, aby se případným obavám a nedůvěře předešlo. Při výběru biometrických systémů je nutné si vyjasnit, kde a který biometrický systém vybrat, aby byly minimalizovány jeho zápory a zároveň maximalizovány přednosti.

Hlavní výhodou biometrických systémů je automatizovaná, rychlá a spolehlivá identifikace. Oproti tradičním metodám identifikace je nelze odcizit, ztratit nebo zapomenout.

I. TEORETICKÁ ČÁST

1 BIOMETRIE

Využívá měřitelných charakteristik (obrazců, data apod.) živého organismu, které se snímají, zpracovávají, vyhodnocují a dále uchovávají. Předpokladem pro tyto charakteristiky je jejich jedinečnost, stálost, praktická měřitelnost a technologická možnost dalšího zpracování. Biometrie je často používána k zajištění vnitřní bezpečnosti, ochrany osob, majetku a různých objektů. Využívá se pro identifikaci nebo verifikaci osob.

Identifikace

Identifikace porovnává nasnímaný biometrický prvek se všemi referenčními šablonami, uloženými v databázi pro zjištění totožnosti osoby.

Verifikace

Verifikace porovnává šablonu vytvořenou z nasnímaného biometrického vzorku s referenční šablonou. Úkolem verifikace je potvrdit nebo vyvrátit identitu prověřované osoby.

Klasická biometrická identifikace se často spojuje s využitím výpočetní techniky. Automatizovaná realizace se stala jedním z hlavních atributů biometrické identifikace. Biometrické systémy snímají biometrické charakteristiky a následně je porovnávají s údaji v předem vytvořené databázi. Biometrické technologie jsou prostředkem k rychlé a pohodlné autentizaci s vysokým stupněm přesnosti.

Autentizace se provádí pomocí tří způsobů:

- **Heslem** – uživatel musí znát a zadat přístupové heslo pro povolení vstupu do chráněného objektu.
- **Předmětem** – aby byl uživatel vpuštěn do chráněného objektu, musí vlastnit určitý identifikační předmět (token), který mu umožní vstup do objektu.
- **Biometrika** – oprávněnému uživateli je povolen vstup na základě prokázáním se biometrickou charakteristikou.[1]

1.1 Komerčně bezpečnostní identifikace

Postupem času se z policejně soudní identifikace odvodila komerčně bezpečnostní identifikace. Kdy *bezpečnostní identifikace* představuje obecné bezpečnostní potřeby (počítačová identifikace, bankovní bezpečnost a ochrana citlivých osobních údajů). A slovo *komerční* vyjadřuje možnost získání biometrické technologie na specializovaném trhu.

Některé dříve používané metody byly buď podstatně zjednodušeny, nebo naopak hlouběji rozpracovány aby lépe vyhovovaly v širokém průmyslovém a komerčním nasazení. Důvodem jsou jiné uživatelské požadavky, zejména přijatelná chybovost a vyhodnocování biometrických identifikačních úloh v reálném čase (řádově sekundy). Komerčně bezpečnostní biometrická aplikace je zcela automatizovaná a převládá zde spíše verifikace nad identifikací. Pracuje na principu povolení nebo odmítnutí přístupu do chráněných „objektů“.

V současné době se používají v komerčně bezpečnostní biometrické identifikaci metody založené na poznatcích o daktyloskopii, o oční duhovce a sítnici, anatomických rozměrech a závislostech dlaně a prstů, tvarech obličeje, projevech hlasu a dovedností psaní (podpis a psaní na klávesnici). Díky svému plošnému nasazení jsou tyto technologie podstatně levnější než technologie policejně soudní.[1]

2 BIOMETRICKÉ SYSTÉMY

2.1 Daktyloskopie

Identifikace podle otisků prstů patří mezi nejstarší, nejznámější a nejrozšířenější biometrickou metodu. Jedná se o nejvíce používanou metodu identifikace nejen v kriminalistice, ale i v různých bezpečnostních systémech, bankách, bezpečnostních službách apod. Pomocí předem vytvořeného referenčního vzorku v databázi, poměrně rychle identifikují oprávněnou osobu a umožní přístup k systému, vstup do objektu apod. Tento způsob biometrické identifikace řadíme do skupiny daktyloskopické identifikace. Daktyloskopická identifikace je založena na obrazech papilárních linií, které se nachází na vnitřní straně článků prstů, dlaních a chodidlech.

Daktyloskopie vychází ze tří zákonitostí:

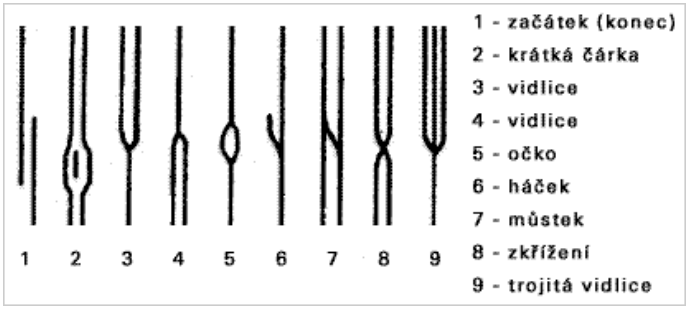
- Na světě nejsou dva lidé se stejnými obrazci papilárních linií
- Po celý život člověka zůstávají obrazce papilárních linií relativně neměnné
- Papilární linie nelze odstranit, pokud se neodstraní i zárodečná vrstva kůže

Na bříšcích prstů ruky nalezneme drobné prolákliny a vyvýšeniny. Vznikají vybíháním škáry proti pokožce v tzv. *kapilárách* – proto papilární linie. Obrazec papilární linie se vytváří již v průběhu embryonálního vývoje. Papilární linie dosahuje výšky 0,1 – 0,4 mm a šířky 0,2 – 0,7 mm.

Nevýhodou této metody je, že drobné poranění prstu může způsobit odmítnutí akceptace. Naopak při zhotovení kopie prstu ze silikonu nebo potravinářské želatiny může získat akceptaci.

U identifikace otisků prstů se zaměřujeme na daktyloskopické markanty. Individualita papilárních linií vzniká velkým počtem těchto markantů, které umožňují snadno od sebe jednotlivé obrazce rozlišit. Markanty rozlišujeme pomocí jejich geometrických tvarů, četností a rozmístěním v obrazcích papilárních linií, jde o nepravidelné a konkrétní tvary markantů, které vykazují rozdíly.

Na obrázku vidíme základní tvary daktyloskopických markantů:



Obr. 1. Daktyloskopické markanty [7]

Máme tři základní vzory seskupení papilárních linií.

Obr. 2 Hlavní vzory seskupení papilárních linií[1]

2.1.1 Snímání otisku prstu

Na kvalitě vstupních dat jsou závislá všechna zařízení, která provádí jakékoliv vyhodnocení. Je tomu tak i v případě automatizované identifikace daktyloskopických otisků. Podle časové posloupnosti a technologičnosti snímání rozdělujeme daktyloskopické snímání otisků do dvou základních skupin:

1. Klasické snímání daktyloskopických stop
2. Bezprostřední (interaktivní) snímání daktyloskopických otisků

Klasické snímání daktyloskopických stop

Jedná se o postupy používané převážně policejními (kriminálními), ale i bezpečnostními službami. Součástí tohoto procesu je vyhledávání, zviditelňování a fixace daktyloskopických stop, které se poté přenáší do daktyloskopických evidencí. S rozvojem prvních počítačových aplikací na vyhodnocování daktyloskopických otisků, vznikla otázka, jak kvalitně převést tyto data z papírových karet do elektronické podoby. Tento problém byl uspokojivě vyřešen až použitím klasických optických skenerů (obrazových snímačů),

které se staly běžnou součástí počítačových periférií pro přenos daktyloskopických otisků do digitální podoby.

Bezprostřední (interaktivní) snímání daktyloskopických otisků

Tato skupina je v současné době typická spíše pro aplikaci komerčně-bezpečnostního charakteru. Pro vstup do určitého objektu, musí osoba přiložit prst na snímací senzor, který sejme otisk a vzápětí následuje verifikace. Osoba není bezprostředně v kontaktu se snímacím zařízením. Toto snímací zařízení je mezičlánkem pro převod dat do počítače, k dalšímu automatizovanému zpracování získaných dat jiným, než klasickým kriminalistickým způsobem V praxi se setkáme u skupiny bezprostředně snímaných daktyloskopických otisků s anglickým termínem live-scanning. Tento pojem představuje všechny technologie snímání daktyloskopických otisků a následný automatický převod do digitální podoby. V nejbližší době nalezne bezprostřední snímání široké uplatnění i v policejně-soudních aplikacích, kde prozatím převážně používají klasické snímání. Bezprostřední snímání otisků prstů je realizování pomocí senzorů. Tyto senzory pracují na různých fyzikálních principech. Podle způsobu kontaktu snímaného povrchu tkáně s daktyloskopickou kresbou je můžeme rozdělit na senzory kontaktní a bezkontaktní.[1]

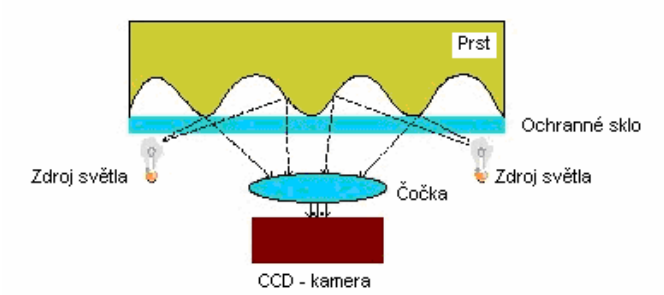
2.1.1.1 Senzory kontaktní

V této skupině senzorů nalezneme mnoho fyzikálních způsobů snímání otisků prstů. Jedná se o technologie používané před více než třiceti lety, ale i technologie mladšího data. Mezi kontaktní senzory patří:

- Optické
- Elektronické
- Opto-elektronické
- Kapacitní
- Tlakové
- Teplotní

Optické senzory

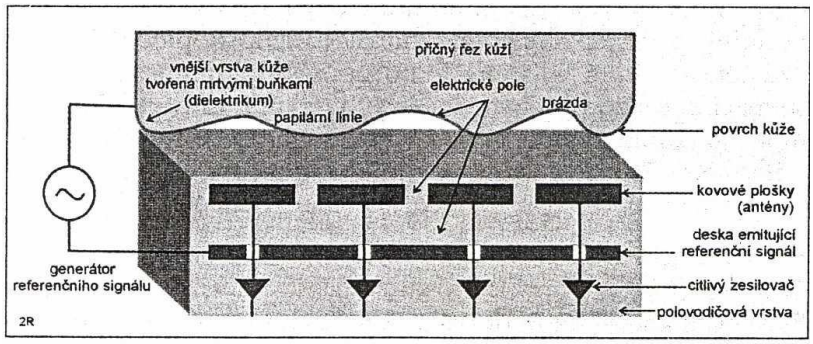
Optické senzory využívají technologie FTIR (Frustrated Total Internal Reflection). Tato technologie osvětluje zespod laserovým paprskem povrch prstu, který se dotýká průhledné desky senzoru, poté se odražený paprsek snímá CCD prvkem. Papilární linie odrážejí mnohem více světla než brázdy. Proto citlivost CCD prvku je nastavena tak, aby neregistrovala odraz od brázd.



Obr. 3. Princip optického snímání otisku prstu.
[8]

Elektronické senzory

Elektronické senzory používají ke snímání elektrické pole vytvořené mezi dvěma vodivými a elektricky nabitými deskami. Přiložený prst tvoří horní desku elektronického senzoru, jehož vlnitý profil změní tvar elektrického pole.



Obr. 4. Principiální schéma elektronického senzoru. [1]

Vrchní vrstvu tvoří odumřelé buňky, které jsou nevodivé. Pod ní nalezneme vysoce vodivou vrstvu slané tekutiny, která prostorově kopíruje profil vnější vrstvy kůže.

V okolí senzoru nalezneme vodivý prstenec. Ve chvíli kdy se dotkneme prstem tohoto prstence, se uzavře elektrický obvod. Nad základní deskou leží husté pole snímacích

antén, které vysílají referenční signál. Referenční signál bude mít deformovaný tvar podle tvaru papilárních linií a brázd. Následně je signál zesílen a transformován do elektronického obrazu daktyloskopického otisku.

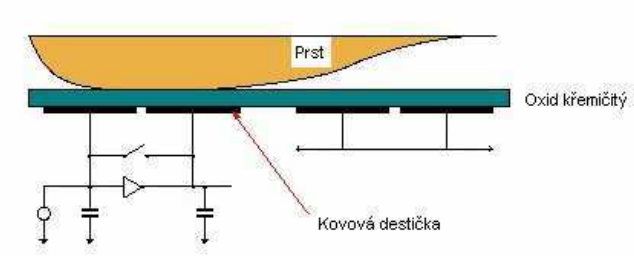
Výhodou tohoto senzoru je, že nereaguje na špínu a poškození povrchu kůže, ale proniká hlouběji pod povrch. Mezi další výhody patří i necitlivost na mokré a suché otisky.

Opto-elektronické senzory

Opto-elektronické senzory se skládají z horní vrstvy, na kterou přikládáme prst. Ta je vyrobena v polymeru TFT (je to průhledný film tvořený z miniaturních tranzistorů umožňující velmi efektivní metodu přepínání jednotlivých pixelů mezi stavy zapnuto/vypnuto), který po dotyku emituje světlo. Na dolní skleněné vrstvě jsou v hustém poli zataveny fotodiody. Ty mají za úkol převádět světelný impuls na impuls elektrický. Ze získaného elektrického impulzu je následně vytvořen daktyloskopický otisk.

Kapacitní senzory

Snímání otisku prstu provádíme pomocí měření kapacity. Na povrchu senzoru je velký počet (řádově 100 000) vodivých ploch, jež jsou od sebe odizolovány. Při dotyku papilární linie dojde k přemostění vodivých ploch v závislosti na její kresbě, kdež to brázdy zde fungují jako izolanty. Poté se mezi jednotlivými vodivými ploškami měří kapacitní úbytky a napětí. Pomocí tohoto měření získáme digitalizovaný obraz papilární kresby.

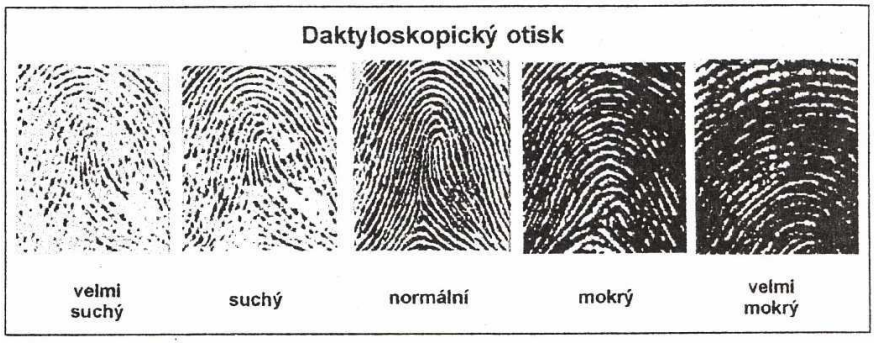


Obr. 5. Principiální schéma kapacitního senzoru. [8]

Otisk je zobrazen ve 256 odstínech šedi, kdy každý obrazový bod (pixel) je 8bitový. Kdy hodnota 0 představuje černou barvu a hodnota 255 barvu bílou.

Výhodou kapacitních senzorů je jejich malý rozměr a cena. Mezi nevýhody patří citlivost na znečištění pokožky prstu zbytky jídla, používání ochranných a léčivých krémů

na ruce. Další nevýhodou je snímání tzv. „suchých“ otisků, se kterými se můžeme setkat u některých osob.

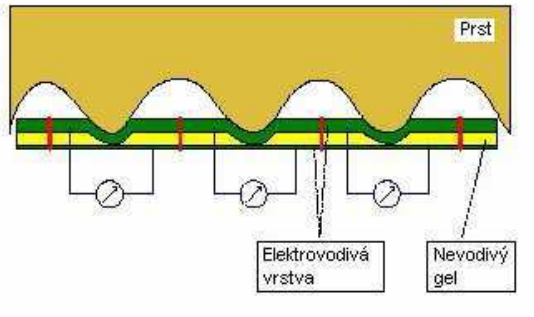


Obr. 6. Ukázka rozdílů různé „suchosti“ otisků prstů. [1]

Tlakové senzory

Na povrchu tlakového senzoru nalezneme elastický, piezoelektrický materiál (piezoelektrické krystaly). Přiložením papilární linie se vyvolá na ploše lokální tlakové působení, které se transformuje do elektrického signálu, brázdy vytváří menší tlak než papilární linie. Z elektrického signálu poté získáme daktyloskopický otisk.

Výhodou tlakového senzoru je, že není citlivý na „vlhké“ nebo „suché“ otisky prstů. Tyto senzory pracují dobře v suchém i vlhkém prostředí.



Obr. 7. Princip tlakového snímání otisku prstu. [8]

Teplotní senzory

U teplotních snímačů využíváme teplotních rozdílů mezi papilárními liniemi a brázdami. Tyto teplotní rozdíly snímáme pomocí miniaturního, velmi citlivého pyrodetektoru. Abychom získali obraz otisku prstu, musíme prstem přejíždět přes citlivou plochu (0,4 x 14 mm). Přejížděním prstu po citlivé ploše získáváme postupně digitální

pásky otisků, z kterých následně poskládáme výsledný obraz papilárních linií. Teplotní snímače používají k autentizaci teplotu povrchu prstu, proto lze rozpoznat, zda přiložený otisk patří živé osobě.

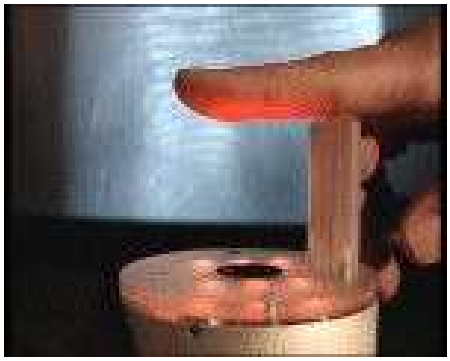
Nevýhodou těchto snímačů je možnost získání různých obrazů otisků při pohybu prstu přes citlivou vrstvu čipu. V databázi máme uloženou pouze určitou část prstu. Během snímání může být nasnímána jiná část prstu a poté dojde k odmítnutí i oprávněného uživatele.

2.1.1.2 Senzory bezkontaktní

- Optické
- Ultrazvukové

Optické senzory

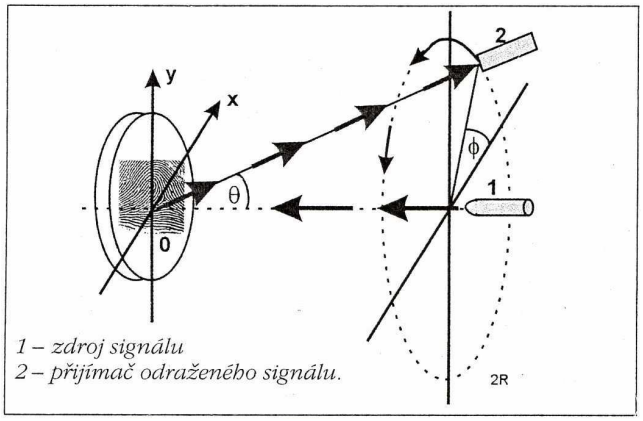
Optické senzory bezkontaktní pracují na podobném principu jako senzory kontaktní. Liší se schopností snímat světelným paprskem daktyloskopický otisk ve vzdálenosti 30 až 50 mm. Výhodou senzoru je eliminace znečištění snímacího senzoru znečištěnými prsty.



Obr. 8. Bezkontaktní optický snímač.
[3]

Ultrazvukové senzory

Ultrazvukové snímání provádíme vysíláním zvukových vln s vysokou frekvencí (4 až 25MHz) generovanou zdrojem směrem ke snímanému otisku. Odražené zvukové vlny jsou vyhodnocovány přijímačem, umístěným kolmě k vysílanému paprsku.



Obr. 9: Principiální schéma práce ultrazvukového snímání otisku prstu. [1]

Odražené a deformované vlny se snímají pomocí rotující hlavy (snímačem) nebo hustou sítí pevných snímacích čidel umístěných v rovině. Snímací čidla vyhodnocují funkční závislost mezi dopadajícími a odraženými zvukovými vlnami. Výsledný obraz otisku má vysoký kontrast, přesnost 0,1 mm a je trojrozměrný (3D).

Mezi výhody ultrazvukových senzorů patří inertnost k vlhkým otiskům prstů, špíně nebo obroušené slabé vrstvě kůže. Ultrazvukové senzory vytváří výsledný obraz v 3D, kdežto daktyloskopické podvrhy jsou zpravidla dvourozměrné, proto lze snadno rozpoznat falzifikát.

2.1.2 Předpoklady pro využití senzorů v praxi

Volba správného snímače je dána kriteriem, v jakém prostředí bude používán. Jednotlivé technologie snímání otisků prstů mají dané technické nároky, které ovlivňují výsledky a mohou do značné míry ovlivňovat kvalitu přístupového systému.

Pro využití senzorů v praxi jsou dány tři základní předpoklady:

- **Velikost zařízení** – při výběru zařízení pro přístup do místností a budov je požadavek velikosti zařízení snadno splnitelný. Pro přístup do počítačů a notebooků je však potřeba značná miniaturizace.
- **Cena zařízení –** cena zařízení závisí na kvalitě snímacího senzoru.
- **Rozlišovací schopnost –** mezi požadavky na rozlišovací schopnost patří nezkreslenost nasnímaného obrazu, dostatečný kontrast, a obsahování co nejširší

škály šedé barvy. Získání kvalitního obrazu závisí na konstrukci snímače, použitém fyzikálním principu a citlivosti na vlhký prst nebo prach.

Mezi další požadavky kladené na snímače otisků prstů patří:

- **Velikost snímací plochy –** pro snímání je potřeba dostatečně velká plocha pro sejmutí dostatečného počtu identifikačních znaků. Snímací plocha není nikdy menší než reálná plocha prstu, z něhož se provádí daktyloskopický obraz.
- **Opakovatelnost dosažené kvality obrazu otisku prstu –** pro dosažení dobrých výsledků je důležitá opakovatelnost kvality obrazu otisku. Posun obrazu otisků a natočení při opakovaném pokusu o autentizaci vzhledem k otisku musí být minimální a současně nesmí nadměrně zatěžovat autorizovaného uživatele.
- **Ochrana proti napodobeninám –** při znalosti obrazu otisku prstu autentizovaného uživatele nesmí být provedena autentizace ani nejdokonalejším padělkem. Nicméně ochrana vůči napodobeninám patří mezi slabá místa současných snímačů.
- **Odolnost proti elektrostatickému výboji –** elektrostatický náboj vznikající na osobách je pro většinu nejmodernějších součástek největším provozním problémem. Napětí vznikající na osobě proti zemi dosahuje 5 – 15 KV. Jedná se převážně o tepelné a kapacitní snímače.
- **Nároky na implementaci do zvoleného systému –** jedná se o požadavek možnosti připojit systém pro rozpoznávání jak do počítače (I/O), tak do distribuovaného systému.
- **Životnost snímačů –** požadavek se vztahuje na konstrukční prvky snímačů s omezenou životností. Jedná se především o materiály chránící snímací plochu proti poškození.

2.1.3 Využití daktyloskopické identifikace pro komerční účely

Pro široké komerční využití spotřebního charakteru přispěla miniaturizace snímacích prvků a speciálních procesorů, která umožnila daktyloskopické porovnání bezprostředně v místě snímání otisků prstů. Praktické rozšíření a snížení výrobní ceny nám umožnila dobře zvládnutá technologie výroby velkého množství autentizačních prostředků založených na biometrice.

Aplikace AFIS pro civilní využití má svá specifika oproti klasickým AFIS pro policejně soudní účely. Prvním specifikem je menší okruh lidí, se kterým musí sejmutý otisk prstu porovnat. Zjednodušováním algoritmů získáme větší výkonnost na běžném PC nebo samostatně stojících specializovaných procesorových jednotách.

Dalším specifikem je vyslovení závěrečného verdiktu výpočetním algoritmem, poté co sejme otisk, zda žadatele propustí nebo odmítne. V případě neúspěšného porovnání má žadatel možnost opakovat svůj pokus. Z důvodu minimalizace neúspěšných pokusů oprávněnými uživateli jsou snímací a vyhodnocovací zařízení neustále zdokonalovány.

Biometrická technologie otisků prstů se v praxi používá:

- Autentizace osob pro přístup k výpočetním a komunikačním prostředkům
- Zvýšení ochrany čipových identifikačních a platebních karet
- Autentizace vstupu do fyzických objektů
- Ochrana drahých nebo nebezpečných zařízení, technologií nebo majetku před neoprávněným použitím či zneužitím

2.1.3.1 Autentizace osob pro přístup k výpočetním a komunikačním prostředkům

Jedná se o nejrozšířenější a nejtypičtější oblast. Nejen na platformě běžných PC ale i pomocí jednoúčelových specializovaných procesorů je automatizované daktyloskopické porovnávání prováděno výpočetní technikou. Uživatelé počítačů při své práci používají klávesnici a myš, kterých se neustále dotýkají konečky prstů. Proto nemají většinou psychologické zábrany dotýkat se podobným způsobem snímacích daktyloskopických prvků, sloužících jako vstupní prvek pro bezpečné přihlášení uživatele do počítače.

Uživatelé počítačů pracují většinou v kancelářském nebo domácím prostředí, kde lze počítat s čistotou prstů, jež je základním předpokladem pro opakované daktyloskopické vyhodnocování. Povrch snímacího zařízení se musí udržovat čistý nebo musí být jednoduché uvést ho do čistého stavu.

Osoby pracující v prostředí počítačů mají mnohem větší pravděpodobnost přijatelné kvality otisků než osoby fyzicky pracující. Osoby fyzicky pracující mají kresbu papilárních linií často zjizvenou, mechanicky zbroušenou či jinak poškozenou. Z tohoto důvodu může být snímání a následné vyhodnocování pomocí automatizovaných technologických prvků

problematické. Další možnosti získání nevyhovujících otisků mohou způsobit léčivé a ochranné masti, případně stresová situace, při které se více potí ruce. Výsledkem je tzv. mokrý otisk.

Snímací prvky integrujeme do klávesnic stolních počítačů, do korpusu notebooků, myší. Vyrábějí se i jako samostatná zařízení, jež připojíme na port počítače. Podobným způsobem lze snímací prvky integrovat i do mobilních telefonů.

2.1.3.2 Čipové identifikační, platební a další karty s biometrickým prvkem

V čipu karty obvykle nalezneme uložené v elektronické podobně textové a grafické informace (jméno, příjmení, datum narození, fotografie držitele apod.). Mezi informacemi je uložena i biometrická šablona otisku prstu držitele karty.

Při verifikaci identity držitel vsouvá kartu do speciálního čtecího zařízení a také přikládá daný prst na snímací senzor. Proběhne porovnání vzoru uloženého na čipu a sejmutého otisku, a tím potvrzení identity. Výhodou uložení biometrické šablony v čipu karty je nepřenášení biometrických dat nikam po síti, ale vyhodnocení v lokálním zařízení. Data na čipu jsou šifrována.

V praxi se čipové karty s biometrickou identifikací používají nejen ve státním nebo finančním sektoru, ale i v nejrůznějších klubech zájmového sdružení. Čipové karty s biometrickou identifikací zaručují nepřenositelnost na jiné osoby. Některé letecké společnosti ve spolupráci s pasovými orgány vydávají čipové karty často cestujícím osobám. Karta nahrazuje standardní pas a urychluje odbavení pasažérů.

2.1.3.3 Autentizace vstupu osob do fyzických objektů

Autentizace vstupu osob do objektů je podobná jako v případě kontroly přístupu k počítačovým technologiím. Snímací zařízení a procesorové vyhodnocovací jednotky jsou připevněny na zeď v prostoru dveří nebo do dveřních klik.

Bezpečnost biometrické technologie zle zvýšit zavedení čipových karet (kombinace s vlastnictvím) nebo personálním kódem tzv. PIN (kombinace se znalostmi). V případě personálního kódu je vedle snímacího zařízení umístěna malá mechanická klávesnice, na které zadáme PIN.

Význam zadávání PIN:

- Bezpečnostní – jde o další doplňkový prvek k ověření při autentizaci
- Technologický – je-li procesorové jednotce znám PIN, probíhá pouze verifikace jediného vzoru otisku určeného pomocí PIN. Kontrolní proces je urychlen a realizován v reálném čase.

Vstupní zařízení do objektů jsou často spojována s prvky umožňujícími evidovat a vyhodnocovat docházku nebo dobu strávenou v chráněném prostoru.[1]

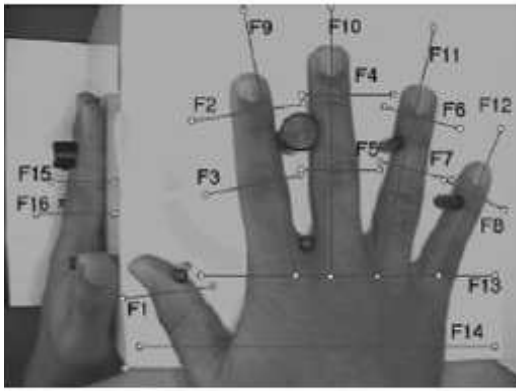
2.2 Geometrie ruky

S biometrickou metodou geometrie ruky se setkáme jen v komerčně-bezpečnostní sféře v režimu verifikace. Jelikož neposkytuje mnoho informací, nelze ji používat pro identifikační účely. Je převážně používána jako prostředek pro rychlou verifikaci v prostorech s omezeným počtem osob.

Lidská ruka je do určité míry jedinečná a lze na ni založit přesnou verifikaci osob. Na všech pěti prstech jedné ruky měříme jejich délky, šířky a tloušťky. Jejich tvar a rozměry jsou jedinečné a od dospělosti se identifikační charakteristiky ruky nemění. Avšak může dojít ke změně způsobené změnou tloušťky prstů a dlaně, úrazem nebo nemocí. Mezi měřené charakteristiky nepatří nehty, ty se v čase velmi rychle mění.

V dnešní době třírozměrné skenery snímají geometrické charakteristiky ruky v desítkách bodů během jediné sekundy. Uživatel položí ruku na horizontální plochu skeneru, která je opatřena speciálními fixačními kolíčky. Ty zajišťují, aby poloha ruky byla při každém snímání stejná. K osvitu ruky jsou použity infračervené LED diody. Následně soustava zrcadel umožní odraz obrazu do snímací CCD digitální kamery. Základová deska je vytvořena z leštěného materiálu s velkou optickou odrazivostí, která zajistí jasný a kontrastní odražený obraz.

Skener snímá černobíle pouze siluetu dlaně s prsty. Snímání obrazu ruky probíhá ze dvou stran. První obraz je snímán shora kolmo dolů na snímací desku a druhý pomocí postranního zrcadla vykresluje pohled na dlaň z boku.



Obr. 10: Snímání geometrie ruky s charakteristikami. [8]

Tab. 1: Tabulka charakteristik. [8]

CHARAKTERISTIKY PŘI SNÍMÁNÍ OTISKU RUKY			
Rys	Popis	Rys	Popis
F1	šířka palce ve druhém článku	F9	délka ukazováčku
F2	šířka ukazováčku ve třetím článku	F10	délka prostředníčku
F3	šířka ukazováčku ve druhém článku	F11	délka prsteníčku
F4	šířka prostředníčku ve třetím článku	F12	délka malíčku
F5	šířka prostředníčku ve druhém článku	F13	šířka dlaně u prstů
F6	šířka prsteníčku ve třetím článku	F14	šířka dlaně u palce
F7	šířka prsteníčku ve druhém článku	F15	tloušťka ruky u druhého článku
F8	šířka malíčku ve třetím článku	F16	tloušťka ruky u třetího článku

Uživateli je při vytváření referenční šablony přidělen i identifikační kód PIN. Při autentizaci zadává uživatel svůj kód a přikládá ruku do stanovené pozice mezi distanční kolíčky.

Referenční biometrická šablona se určuje pomocí identifikačního kódu PIN nebo hmotného nosiče (magnetický proužek ID karty, mikročip, čárový kód). Biometrické zařízení pak bude obsahovat skener geometrie ruky a místo klávesnice čtečku snímající charakteristiky biometrické šablony.

2.2.1.1 Přednosti metody geometrie ruky

Jedná se o velice jednoduchou a rychlou biometrickou metodu. Mezi přednosti patří odolnost na zašpiněné ruce a malá velikost referenční šablony. Referenční šablona má velikost pouhých 9bytů. Malá velikost referenční šablony nám umožňuje uchovávat několik desítek tisíc referenčních šablon v každém samostatně instalovaném skenovacím zařízení. Pro malou velikost referenční šablony ji lze ukládat do magnetických proužků nebo čipů identifikačních karet.

Verifikace osob založená na geometrii ruky je druhou nejrozšířenější verifikační metodou.

2.2.1.2 Nedostatky metody geometrie ruky

Skener geometrie ruky je citlivý na poranění či fyzické změny snímané charakteristiky. V případě amputovaného článku prstu nebo dokonce celého prstu mohou znesnadnit přesné polohování ruky v procesu snímání, ale i jakékoliv otoky prstů způsobí odmítnutí vstupu do objektu. Lidé trpící Parkinsonovou nemocí nedokážou položit správně ruku mezi polohovací kolíčky.

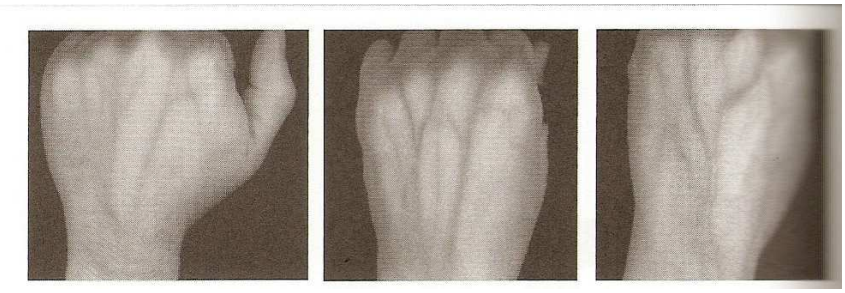
Záleží také na klimatických podmínkách, vnější teplotě a vlhkosti, ve kterých je zařízení instalováno. Ve chvíli, kdy přirozeně teplá ruka se dotýká chladné plochy, začne docházet ke kondenzaci vlhkosti na zrcadlových plochách a snímaný optický obraz může být zkreslen. Další potíže mohou nastat ve chvíli, kdy je zařízení instalováno na přímém slunečním světle. Snímání je prováděno v infračerveném pásmu a infračervená složka ze slunečního světla může negativně ovlivnit (oslepit) skener. Proto je zařízení vybaveno světelnou clonou.

Z důvodu předcházení negativních vlivů venkovních podmínek se proto se skenery geometrie ruky setkáme převážně ve vstupních halách. [1]

2.3 Krevní řečiště hřbetu ruky

Mezi jednu z nejnovějších metod identifikace člověka, patří identifikace pomocí síti cév na povrchu hřbetu ruky. Jedná se o technologii velice podobnou metodě geometrie ruky a nese její výhody.

Geometrické rozmístění krevního řečiště je jedinečné pro každou osobu. Obraz krevního řečiště se vytváří, již v prenatálním období. V průběhu života je dostatečně stabilní a lze na něm založit spolehlivou identifikaci. Obraz krevního řečiště tvořeného cévami je odlišný pro pravou a levou ruku. Vědecké studie prokázaly jedinečnost i u jednovaječných dvojčat.

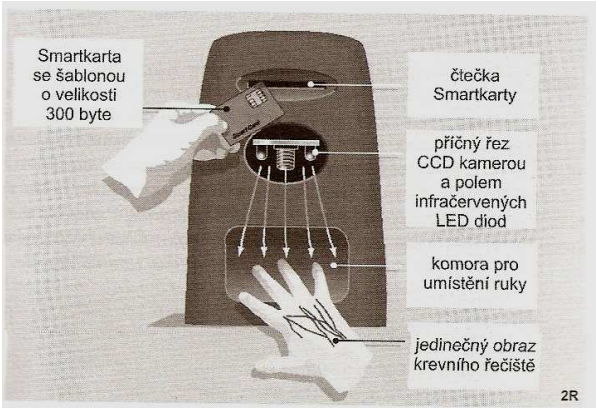


Obr. 11. Kresba krevního řečiště na hřbetu ruky. [1]

Uživatel pokládá ruku hřbetem nahoru na snímací plochu skeneru. Poté je hřbet ruky prosvícen polem infračervených diod a odraz světla je snímán černobílou CCD kamerou v 16 stupních šedi. Jde o infračervené snímkování, které je citlivé na teplo vyzařované cirkulací krve v těle. Infračervené záření proniká do hřbetu ruky přibližně jen 3mm, kdy okysličený hemoglobin pohlcuje světlo a tím se vytvoří síť černých čar, které vytvářejí obraz krevního řečiště.

Získaný obraz projde dalšími úpravami jako je segmentizace (rozdělení obrazu na dvě části- ruka a pozadí), vyhlazení a redukce šumu (potlačení vlivu tvaru hřbetu ruky a vyhlazení obrazu cév), prahování (oddělení vzoru žilní struktury od zbytku obrazu) a nakonec postprocesing (obraz struktury žil na hřbetu ruky používaný jako šablona).

Stejně jako metoda geometrie ruky má metoda obrazu krevního řečiště stejné základní využití. Nicméně pro svou lepší miniaturizaci najde uplatnění jako metoda pro přístup k počítačům, automobilovým dveřním zámkům nebo bankovním automatům.[12]



Obr. 12. Schematický řez skenerem, vybavený čtečkou Smartkarty, která obsahuje biometrickou šablonu jejího právoplatného držitele. [1]

2.4 Tvář

Problematika verifikace obličeje je velice obsáhlá a neustále se vyvíjí a zdokonaluje. Základní dělení systémů verifikace obličeje jsou statické a dynamické. Dále je pak dělíme na systémy řízené a neřízené.

Identifikace uživatele u statického, řízeného systému je vědomá. Snímání probíhá z čelního úhlu a výsledný obraz má předem stanovené pozadí, nasvícení a rozlišení snímku.

Obr. 13. Snímek obličeje s obličejovými rysy. [3]

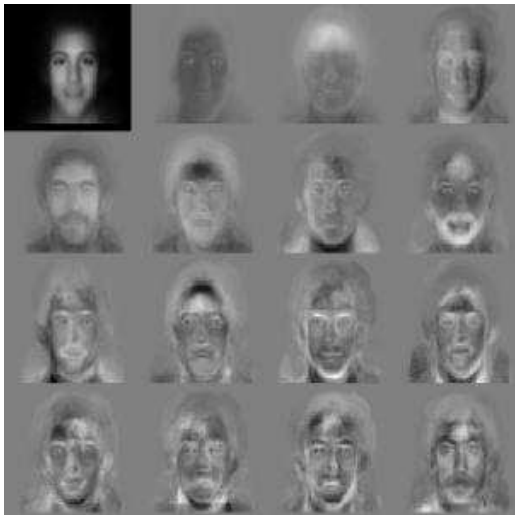
Principem dynamických neřízených systémů je zachytit a následně identifikovat osobu v davu lidí. Využití dynamických neřízených systémů je na frekventovaných

místech, např. letiště, obchodní centra a banky. Systémy mohou být propojeny s databází zájmových osob, jako jsou zločinci, teroristé, vytvářející vhodnou preventivní ochranu. Obličej uživatele lze identifikovat pomocí dvou způsobů.

Jeden způsob identifikace uživatele využívá k identifikaci tvar obličeje a polohu opticky významných míst na tváři. Jako první software vyhledá oči jako temné body v horní polovině obrazu a odtud pokračuje na další markantní body obličeje. Avšak systém neukládá přesnou polohu očí, nosu nebo rtů, ale zaobírá se vzdáleností očí, rtů od nosu nebo úhlem mezi štičkou nosu a jedním okem. V tomto způsobu mohou být využity tři algoritmy rozpoznávání tváře PCA, LDA, EBGM.

PCA (Principal Components Analysis) – analýza hlavních částí

Každou tvář je možné rozdělit do tvz. Eigenfaces (normalizovaná tvář). Normalizované tváře jsou výchozí množinou identifikačních charakteristik tváře jedné nebo více osob. Počítačová aplikace je poté používá k rozpoznávání osob. V databázi může mít jedna osoba uloženo více normalizačních tváří, vyjadřujících její momentální stavy v době pořizování snímku.



Obr. 14. Normalizované obrazy tváře.
V levém rohu je originální obraz tváře.
[4]

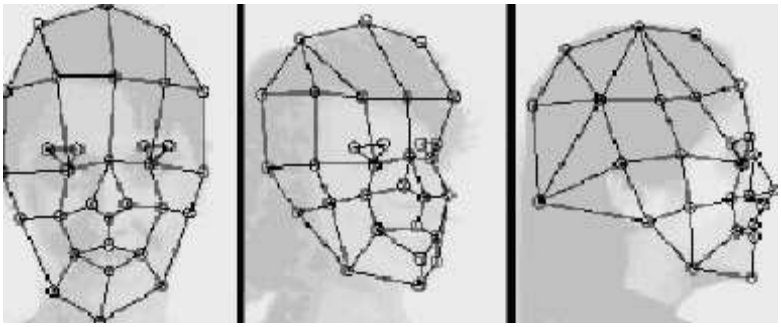
LDA (Linear Discriminant Analysis) – lineární diskriminační analýza

Pořizované obrazy tváří se třídí do skupin. Kdy hlavním cílem tohoto dělení je maximalizovat rozdíly mezi jednotlivými skupinami a zároveň minimalizovat rozdíly v dané skupině.

Obr. 15. Příklad šesti tříd užití LDA. [4]

EBGM (Elastic Bunch Graph Matching) – elastický srovnávací diagram

Využívá souřadnicovou síť, která vznikne nadefinováním uzlových bodů a poté jejich propojením, jež definují linii tváře v prostoru. Pomocí filtru uzlových bodů reaguje systém na jednotlivé snímané tváře, které následně porovná a vyhodnotí.



Obr. 16. Síť vytvořená elastickým mapováním. [3]

Druhý způsob je založen na tepelném záření tváře uživatele. Snímání se provádí pomocí infračerveného optického snímače, který snímá teplo vyzařované žilním systémem a okolními tkáněmi. Jedná se o mnohem přesnější techniku oproti prvnímu systému.

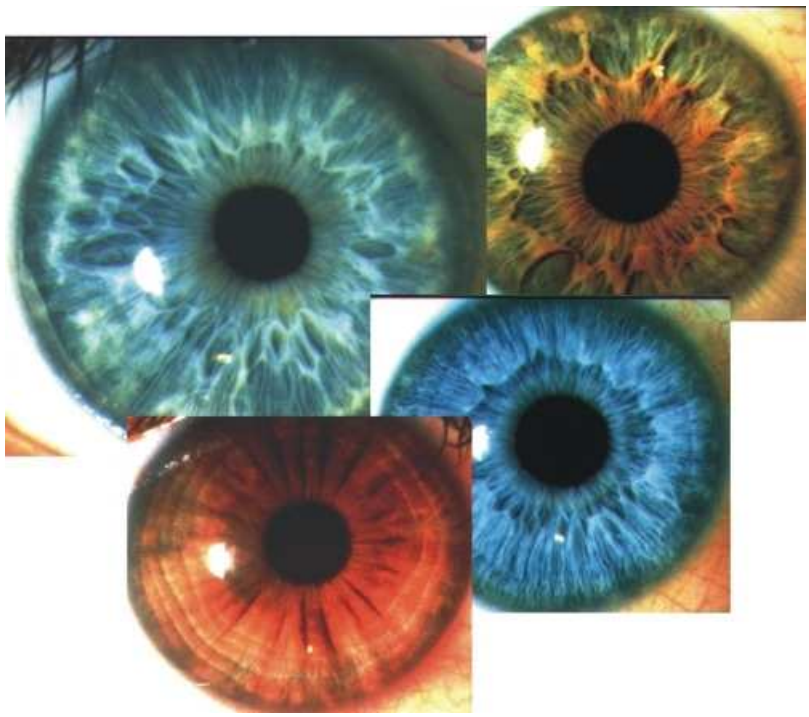
Obr. 17. Termografický snímek. [3]

Výhodou identifikace podle geometrie obličeje je, že nevyžaduje kontakt pro rozpoznání identifikované osoby.

Mezi nevýhody patří neschopnost rozeznat od sebe jednovaječná dvojčata. Nedokonalý kamerový systém, který nedokáže rozpoznat zobrazený obličej, protože na snímcích nesouhlasí světelné podmínky nebo je pokaždé jiná orientace hlavy.[4]

2.5 Oční duhovka

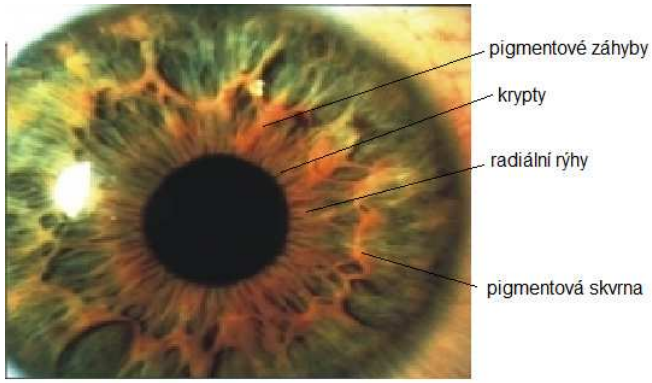
Jde o biometrickou identifikační metodu založenou na snímání oční duhovky, která je jedinečná pro každého člověka a ani identická dvojčata nemají stejné duhovky. Vyznačují se svou jedinečností i u jednoho člověka, jež má každou oční duhovku jinou. Identifikace pomocí oční duhovky se považuje za jednu z nejpřesnějších metod.



Obr. 18. Různé druhy očních duhovek. [11]

Oční duhovka se formuje od třetího měsíce těhotenství až do prvních postnatálních let. Oční duhovka je pigmentová membrána obklopující zřítelnici oka, která kontroluje úroveň světla vstupujícího do oka. Podle potřeby jemné svaly spojené s duhovkou ji rozšíří nebo naopak zúží. Její barva je ovlivněna hustotou melaninového pigmentu, kdy modrá

barva značí absenci pigmentu. Duhovka obsahuje složitý vzor mnoha charakteristických znaků, jako jsou krypty, rýhy, skvrny, klenuté vazy, korány, prstence.



Obr. 19. Popis oční duhovky.

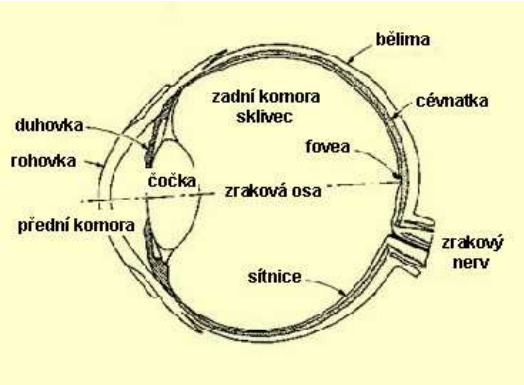
Charakteristické znaky duhovky jsou snímány CCD kamerou, která pořizuje černobílé snímky ve velkém rozlišení. Během snímání dochází k digitalizaci charakteristických znaků. Pro získání vhodných snímků jsou oči osvětlovány neviditelným infračerveným světlem.

K přednostem této metody patří bezkontaktní snímání, snímek může být pořízen do vzdálenosti jednoho metru. Jedná se o rychlou, pohodlnou a vysoce přesnou metodu. Brýle nebo oční čočky nepředstavují překážku pro snímání. Systém nelze přelstít fotografií oka nebo skleněným okem.

Mezi nevýhody patří vyšší pořizovací náklady a stále přetrvávající obavy uživatelů z poškození oka.

2.6 Oční sítnice

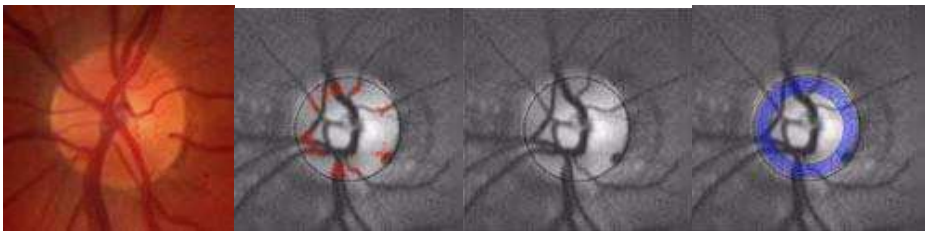
Biometrická metoda rozpoznávání pomocí oční sítnice provádí identifikaci osob prostřednictvím snímání a porovnávání obrazu sítnice (choroidu). Využívá se v oblasti s největším stupněm zabezpečení. Sítnici nalezneme na zadní straně oční bulvy. Snímáme sítnici a cévní obrazec nacházející se za sítnicí. Infračervený paprsek o nízké intenzitě je zaměřen skrz zornici na zadní stranu oka. Cévy sítnice reflektují a vytvářejí snímek sítnice používaný pro rozpoznávání osob, kdežto sítnice se jeví jako průhledná.



Obr. 20. Průřez lidského oka. [9]

Výhodou rozpoznávání pomocí oční sítnice je vysoká přesnost a rychlost doprovázená vysokou bezpečnostní.

Nevýhodou je malá uživatelská příjemnost, kdy je nutnost přiblížit oko k snímacímu zařízení a vydržet bez pohybu 10 až 15 sekund. Dále panují mezi uživateli obavy z možnosti poškození oční sítnice, i když se jedná o zdraví neškodnou metodu. Uživatel nosící brýle, musí je před použitím snímače odložit. V případě silného astigmatismu může způsobovat problém zaměřit tečku v kameře a tím fixaci cíle. Výsledkem je špatné nasnímání oční sítnice uživatele. Biometrická identifikace pomocí oční sítnice je relativně drahá.



Obr. 21. Snímky cév za oční sítnicí znázornění charakteristických parametrů. [3]

2.7 Podpis

Verifikace osoby založená na rozpoznávání podpisu patří k nejpraktičtějším způsobům ověřování lidské identity. Podpis nemůžeme ztratit, zapomenout nebo nám nemůže být odcizen. Podpis se stal přirozenou součástí běžného života. S ověřováním podpisu se můžeme setkat v oblastech, jako je kontrola přístupu, bezpečnost nebo finanční transakce. Verifikace osoby podle podpisu vychází z toho, že není nijak standardizovaný nebo stejný ale je pro každého člověka individuální.

Existují dva základní typy systémů, pomocí kterých rozpoznáme podpis osoby:

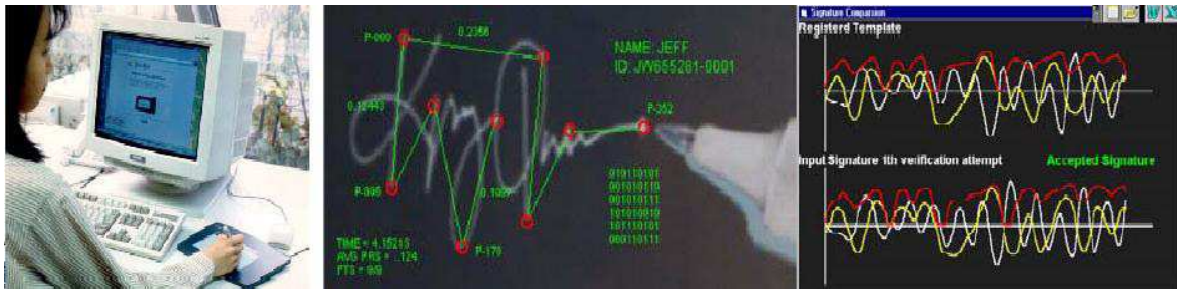
- On-line systémy
- Off-line systémy

Off-line systém

Podpis je napsán na papír a poté pro získání digitálních dat o obrazu je podpis naskenován nebo nasnímán kamerou. Verifikace pomocí off-line systému není dnes pro automatizované zpracování vhodné. Porovnávání dvou statických obrazů podpisu, předkládaného vzoru s referenční šablonou, je v dnešní době skenovacích zařízení náchylné k falzifikátům. Poněvadž se snadno pomocí skenování nebo vyfotografování získá podpis osoby a poté ho lze předložit snímacímu zařízení verifikační aplikace.

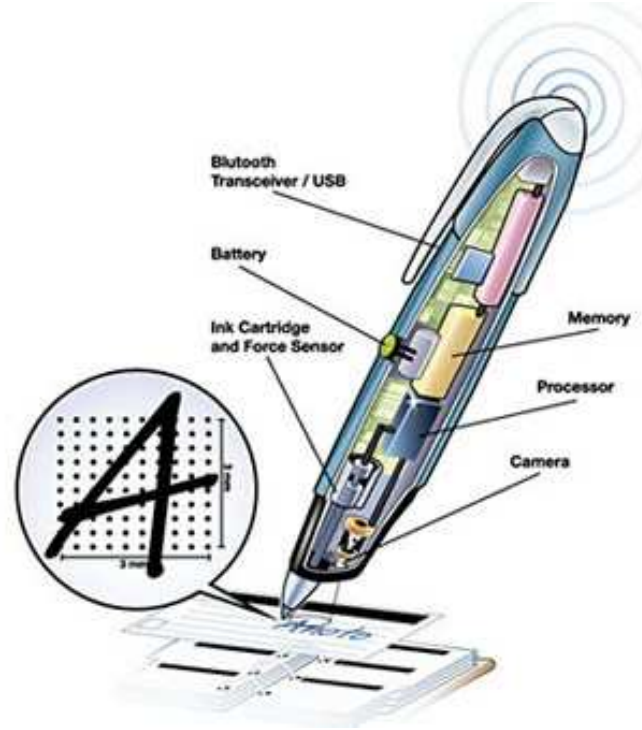
On-line systém

Data se získávají v reálném čase pomocí speciálního pera nebo digitalizačního tabletu. Dynamické on-line systémy získávají dynamické charakteristiky. Mezi dynamické vlastnosti patří rychlost psaní, tlak pera v jednotlivých bodech, pořadí psaní jednotlivých částí podpisu. Cílem využití dynamických charakteristik je detekce případných podvrhů a napodobenin podpisu.



Obr. 22. Princip dynamického podpisu; uživatel, měření a SW srovnání. [3]

Pro tyto účely se používaly klasické tablety, kdy pero bylo pevně spojeno s počítačem. Postupem času byla vyvinuta speciální pera, která umožnila přenášení získaných dat bezdrátově do vstupní jednotky a do počítače.



Obr. 23. Řez speciálním perem SmartPen, umožňující snímání dynamických charakteristik. [10]

2.8 Dynamika stisku počítačových kláves

Jedná se o metodu identifikace pomocí dynamiky psaní na klávesnici, kdy nezáleží na tom, co se píše, ale jak se píše. Dynamika psaní na klávesnici je zaměřena na dobu mezi stiskem jednotlivých kláves, dobu trvání stisku klávesy, celkovou rychlost psaní, sílu stisku klávesy, počet chyb a zvyk používat dodatečné klávesy (čísla na numerické klávesnici). Převážně se tato metoda používá jako sekundární autentizace vstupu, z důvodu malé bezpečnosti proti neoprávněnému uživateli.

V případě, že aplikace bude spuštěna na pozadí a zjistí odchylku od uloženého vzorku, může vyžádat od uživatele provedení primární identifikace.

Je možnost výskytu problému ve chvíli, kdy se zaregistruje uživatel „nováček“ a postupem času se naučí psát všemi deseti prsty. Pak je zapotřebí registraci opakovat.

2.9 Hlas

Identifikace hlasu se provádí pomocí elektronické analýzy řeči identifikované osoby. Hlas člověka se během života mění, relativně stálý a neměnný je ve stáří od 20-60 let. Hlas člověka je pro každého charakteristický a je ovlivňován osobností člověka (zabarvení hlasu, rytmus), amplitudové frekvenční spektrum měnící se v čase, lingvistickou strukturou (gramatika, skladba řeči) a rozměry vokálového traktu. Proděláním různých nemocí nebo pozměněním návyků může dojít ke změně hlasu. Vokálový trakt (řečové orgány) je zdrojem řečových kmitů. Hlasový trakt je složen z aktivních mluvních orgánů (čelisti, rty, jazyk, hlasivky, měkké patro) a vokálního traktu (dutina ústní, nosní, hrdelní, měkké patro).

Biometrický identifikační systém srovnává hlasový záznam s uloženým vzorem hlasu. Používají se dva přístupy. Jeden požaduje, aby identifikovaná osoba řekla předem danou frázi, kterou poté vyhodnotí. U druhého přístupu může identifikovaná osoba říct libovolnou frázi.

Systém nelze přelstít imitátorem hlasu, jelikož nezná potřebný klíčový význam věty. Metoda je rychlá, jednoduchá na použití, spolehlivá a jsou nízké pořizovací náklady.

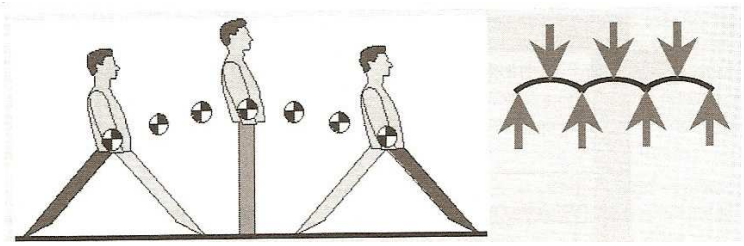
Avšak může nastat problém ve chvíli kdy uživatel je nachlazený, jelikož bude jeho intonace pozměněna.

2.10 Dynamika chůze

Jednou z nově vznikajících oblastí biometrických aplikací je rozpoznávání člověka podle stylu chůze. Jedná se o bezkontaktní rozpoznávání osob. Chůze člověka obsahuje mnoho individuálních specifik, jež lze využít pro identifikační účely, ale také individuální specifika dokážou znesnadnit technické, automatizované identifikování. Pomalá chůze nebo rychlý běh je pro člověka přirozeným pohybem, ale pro technické prostředky to znamená zcela odlišné podmínky pro jejich nasazení, volbu nebo kombinaci různých metod počítačového vidění a praktické vyhodnocení situace. Chůzi člověka může ovlivnit různé typy oblečení, těhotenství ženy, různé zdravotní problémy případně požití alkoholu, návykových látek apod.

2.10.1 Rozpoznávání chůze pomocí pohybu těžiště

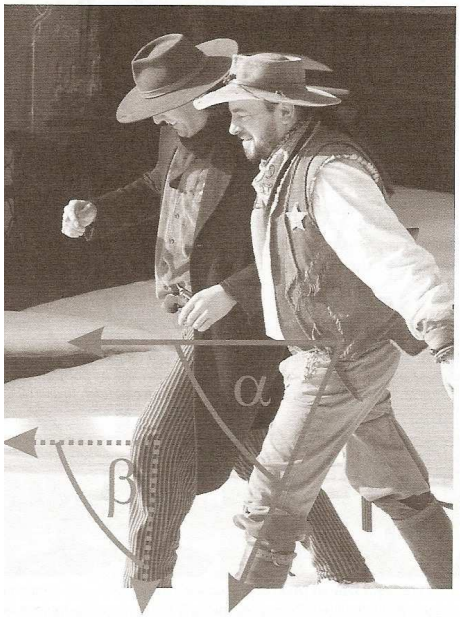
Člověk důsledkem anatomické konstrukce těla nedokáže během pohybu udržet těžiště v přímé linii. Při chůzi se těžiště lidského těla pohybuje nahoru a dolů. Postupně byly přidávány další aspekty jako je ohyb kloubů (kyčel, kolena, rotace pánve a hrudníku), což mělo za důsledek zjemňování výsledné křivky, která nakonec dosáhla sinusového průběhu.



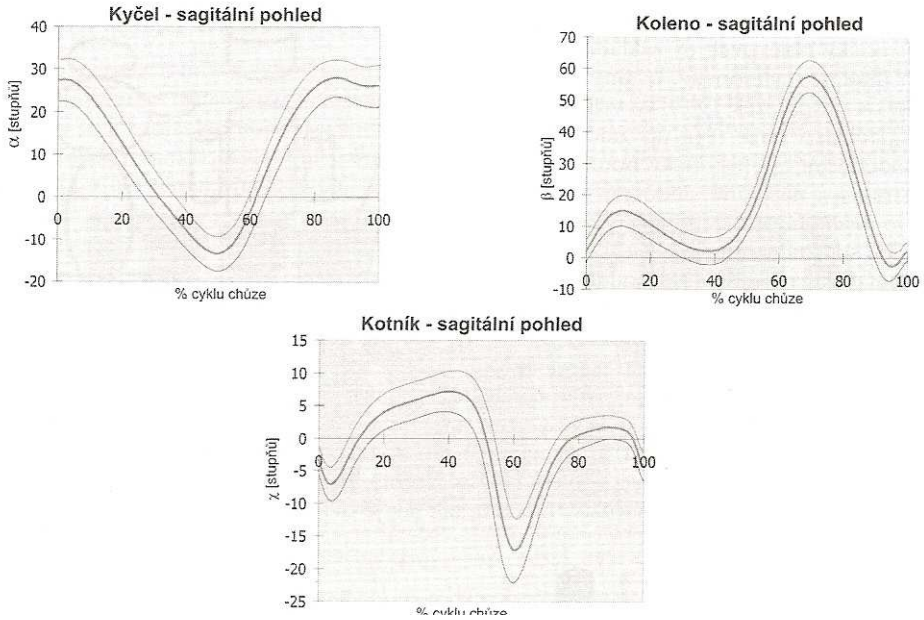
Obr. 24. Pohyb těžiště lidského těla. Nohy jsou přímé bez jakéhokoliv ohybu v kolenou či dalších kloubech. Trajektorie křivky zobrazena vpravo, šipky označují maxima a minima. [1]

2.10.2 Sagitální kinematika

Sledování těžiště těla neposkytovalo v minulosti uspokojivé množství informací, proto se zaměřili na pohyb jednotlivých částí člověka, hlavně kloubů. Měříme měnící se úhel odklonu dané části končetiny od kloubu směrem níže od předozadní osy procházející kloubem. Tento úhel se měří po dobu jednoho cyklu chůze a je poté zaznamenáván do grafů. Původně byla sagitální kinematika určena pro medicínské účely, ale časem se začala uplatňovat v oblasti počítačového vidění.



Obr. 25. Ukázka měření úhlu pohybu kyčle (α) a kolena (β) v sagitálním směru. [1]



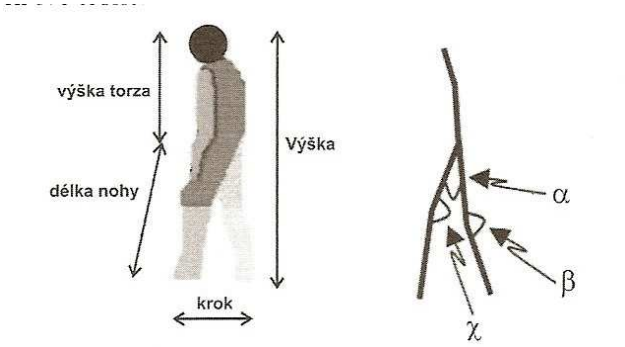
Obr. 26. Ukázka měření sagitálních úhlů kyčle, kolena a kotníku. Prostřední křivka je průměrná hodnota a horní a dolní křivky jsou standardní maximální a minimální odchylky od průměru. [1]

2.10.3 Principy automatizovaných technologií rozpoznávajících osoby dle chůze

U automatizovaných technologií se jedná převážně o sledování osoby v určitém prostoru, pokrytém kamerovým systémem. Biometrické rozpoznávání podle dynamiky chůze je v současnosti rozdělováno do dvou základních směrů.

Modelování pohybu člověka

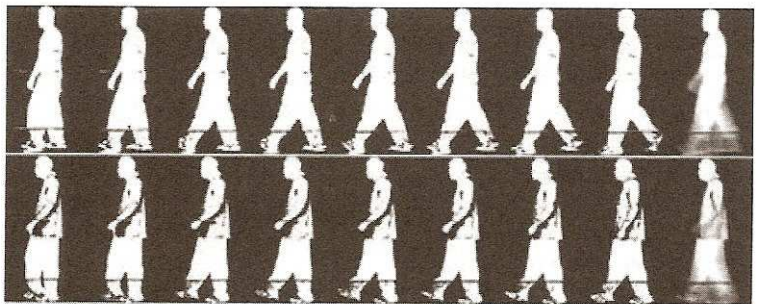
Metoda modelování pohybu analyzuje dynamiku pohybu torza (horní části těla) a nohou. Podobně jako u medicínských přístupů je věnována pozornost tělesným rozměrům (délkám) a úhlům při chůzi, u této metody není zohledňovaný vliv oblečení na chůzi člověka.



Obr. 27. Ukázka drátěného spoje se sledovanými a vyhodnocovanými parametry. [1]

Siluety pohybujícího se člověka

Z pozadí scény se vyčleňují siluety pohybujícího se člověka, které se sledují, vyhodnocují a zároveň se zaznamenává i její pohyb.



Obr. 28. Fázové pohyby siluety chodce snímané kamerou a počítačově zpracované. [1]

3 CHYBOVOST BIOMETRICKÝCH SYSTÉMŮ

Cílem identifikace či verifikace je bezchybně umožnit garantovaná práva oprávněné osobě. Kdežto neoprávněnou osobu bezchybně rozpoznat a odmítnout. Chybovost/spolehlivost systému popisují dva parametry:

FRR (False Rejection Rate, míra chybného odmítnutí) – jedná se o pravděpodobnost neautorizování oprávněného uživatele. Je dán podílem osob odmítnutých identifikačním přístrojem, ač měly být autorizovány, k celkovému počtu pokusů autorizovaných osob.

FAR (False Acceptance Rate, míra chybného přijetí) – charakterizuje pravděpodobnost autorizování neoprávněného uživatele. Popisuje podíl osob přijatých identifikačním přístrojem, když neměly být autorizovány, k celkovému počtu pokusů neoprávněných osob. [1]

Tab. 2. Spolehlivost nejobvyklejších biometrických prvků. [13]

Biometrická metoda	FRR	FAR	Rychlost verifikace	Míra spolehlivosti
Otisk prstu	< 1,0%	0,0001% - 0,00001%	0,2 až 1 sekunda	vysoká
Geometrie ruky	< 0,1%	0,1%	1 až 2 sekundy	střední
Tvář	1%	0,1%	3 sekundy	střední
Oční sítnice	< 0,4 %	0,001 %	1,5 až 4 sekundy	vysoká
Oční duhovka	0,00066 %	0,00078 %	2 sekundy	vysoká
Hlas	< 1,0%	> 1,0%	1,5 sekundy	nízká

II. PRAKTICKÁ ČÁST

4 PRODEJ BIOMETRICKÝCH SYSTÉMŮ V PRAXI

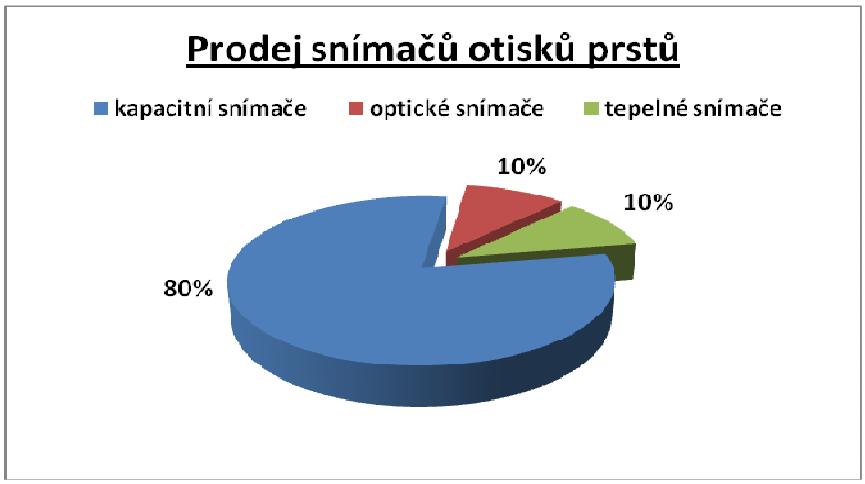
Biometrické systémy nabízejí bezpečnou a komfortní alternativu ke klíčům, heslům a PIN. Proto jsem se zaměřila na množství prodaných biometrických systémů v PKB. Bylo osloveno několik firem zabývajících se prodejem, ale povedlo se získat informace o prodeji jen ze dvou. Tyto firmy si nepřály být jmenovány, proto budou označeny jako firma 1a 2.

4.1 Firma 1

Snímače otisků prstů

Česká republika :

V české republice bylo prodáno průměrně 50ks/rok. Převážně se jednalo o kapacitní snímače otisků prstů, dále pak optické a tepelné protahovací snímače.



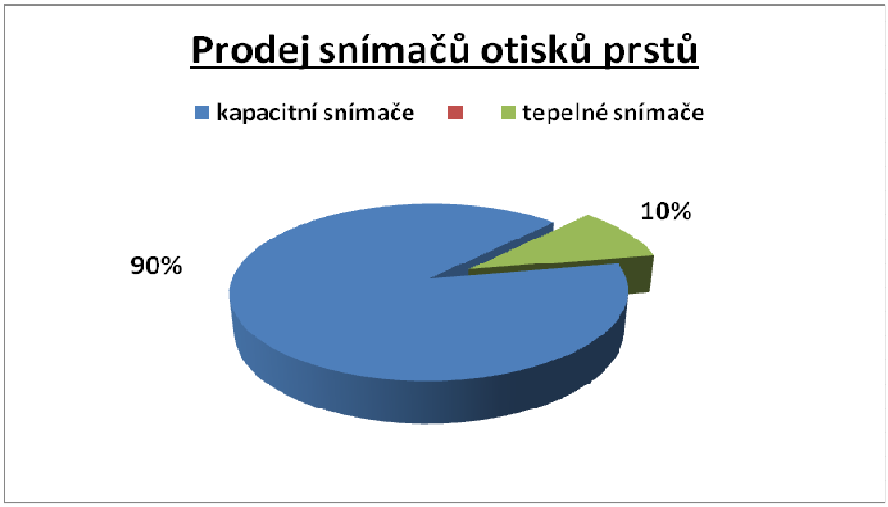
Obr. 29. Prodej snímačů otisků prstů v české republice.

Rozložení zákazníků:

- 40% bankovní sektor
- 45% soukromé společnosti, středně velké a administrativní objekty
- 15% rezidenční oblast

Slovensko:

I zde patří mezi nejvíce prodávané snímače kapacitní snímač otisku prstu, mezi méně prodávaný patří tepelný snímač.



Obr. 30. Projed snímačů otisků prstů na Slovensku.

Rozložení zákazníků:

- 70% soukromá sféra, menší a středně velké podniky
- 15% administrativní sféra
- 15% primárně privátní rezidenční sektor, ostatní

Oční duhovka

V české republice se prodalo 10ks, kdy snímače oční duhovky směřovaly do armádní sekce.

Systém pro vyhodnocení geometrie obličeje

Mezi nejméně prodávané patří systém pro vyhodnocování geometrie obličeje, kdy se v české republice prodal 1-2ks/rok do akademické sféry a velkých komerčních společností.

4.2 Firma 2

Všechny prodané produkty používají k identifikaci tepelný řádkový snímač otisku prstu. Bylo realizováno několik desítek až stovek zakázek směřujících do komerčního sektoru nebo soukromým investorům, kteří chtěli zabezpečit své rodinné domy.

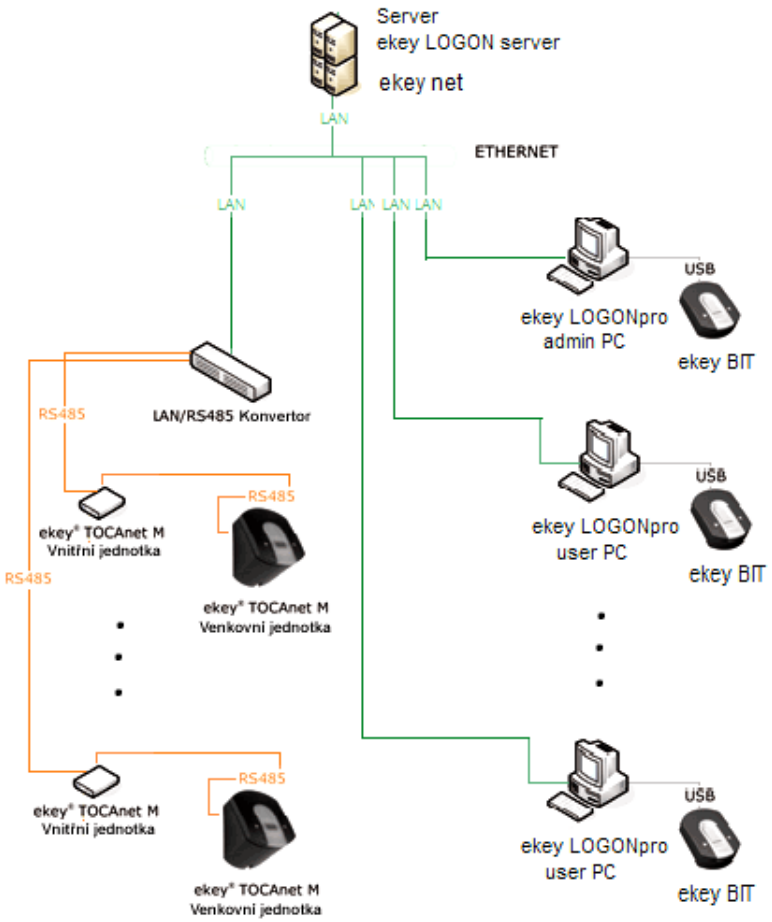
Z finanční stránky byly firmy větším zákazníkem, jelikož nakupovaly komplexnější a dražší verze produktů. Z pohledu prodaných kusů je mezi firmami a soukromými investoru poměr 50% na 50%.

Firmy nakupující tento systém z důvodu:

- Velkého počtu zaměstnanců
- Docházka zaměstnanců je pochybná
- Chtějí nadstandardně zabezpečit přístup některých místností
- Komfortu, který biometrické systémy poskytují

5 NÁVRH ZABEZPEČOVACÍHO SYSTÉMU

Jedná se o jednoduchý systém s uživatelskou přívětivostí. V návrhu je zajištěna kontrola vstupu a počítačové sítě. Pro návrh zabezpečení byly použity prvky od společnosti Ekey. Komplexní řešení od jednoho výrobce nám umožní předejít problémům s kompatibilitou a nastavováním systému. Administrátorský PC s jednou čtečkou a jedním uživatelským prostředím může spravovat databázi šablon a přístupové práva do objektu a počítačových sítí. Pro přístup k počítačové síti byl použit software Ekey LOGONserver, který používá jako přístupové čtečky Ekey BIT. Přístupový systém do objektu je realizován pomocí Ekey TOCAnet.



Obr. 31. Návrh zapojení systému.

5.1 Použité součástky

5.1.1 Ekey LOGONserver

Tento software umožňuje kontrolu přístupu k počítačové síti. K ekey LOGONserveru je na jednotlivých uživatelských terminálech nainstalovaná čtečka ekey BIT a software ekey LOGONpro.

Tab. 3. Parametry ekey LOGONserver. [2]

Parametr	Hodnota
Operační systém pro server	Windows 2000 server a 2003 server
Operační systém pro pracovní stanice	Windows 2000 SP 4 a XP Professional SP1 a vyšší
Čtečka	ekey BIT nebo Siemens ID myš

5.1.2 Ekey TOCAnet

Jedná se o produkt jednoduchý na použití, ale zároveň disponuje mnoha doplňky. Čtečka se skládá ze dvou jednotek. Vnitřní jednotka zpracovává informace, rozhoduje, ovládá zámek, a komunikuje jak se serverem, tak s vnější jednotkou. Vnější jednotka je snímací termický senzor firmy Atmel s označením FingerChip.

Ekey TOCAnet může v režimu online předkládat biometrický vzor k porovnávání s databází šablon uložených na ekey TOCAnet serveru (neomezený počet šablon). Avšak dojde-li k výpadku serveru je ekey TOCAnet schopný pracovat v offline režimu, kdy předkládaný biometrický vzor porovnává s databází šablon uložených ve vnitřní jednotce ekey TOCAnet M. Po opětovném uvedení čtečky do online režimu, odešle všechny informace na server. Vnitřní jednotkou lze díky 3relé výstupům ovládat najednou více prvků (dveře, vrata, apod.)

Tab. 4. Parametry Ekey TOCAnet. [2]

Parametr	Hodnota
Rozměry - vnitřní jednotka (š x v x h) - vnější jednotka	140 x 128 x 48 mm 60 x 95 x 55 mm
Typ senzoru	termický Atmel FingerPrint
Databáze otisků – offline (dle verze) - online	200 otisků verze M, 40 otisků u S a 2000 otisků u L "neomezeně"
Chybovost - FAR - FRR	0,00001 0,014
Napájení	z 220/110V na 9 nebo 12 V DC venkovní jednotka napájená z vnitřní
Příkon	2,2W
Relé	3x až 230V max. 5A
Komunikace	RS 485 přes konvertor LAN (Ethernet)
Pracovní teploty	-40 až +85 ℃
Relativní vlhkost	max. 95%
Krytí - vnitřní jednotka - vnější jednotka	IP 54 IP 43

5.1.3 Ekey BIT

Čtečka ekey BIT využívá ke snímání otisku prstu termický senzor firmy Atmel. Tato čtečka má více možností využití buď jako kontrolu přístupu do počítačové sítě obsahující program LOGONserver nebo jako přístup k autonomnímu PC a v neposlední řadě přidávání otisků prstů pro přístupový systém ekey TOCAnet přes admin server.[2]

Tab. 5. Parametry Ekey BIT. [2]

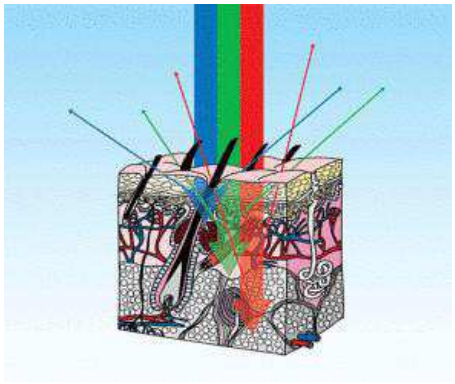
Parametr	Hodnota
Rozměry š x v x h	60 x 82 x 22 mm
Hmotnost	220g
Rozhraní	USB 1.1/2.0
Senzor	termický Atmel FingerChip
Chybovost - FAR - FRR	0,00001 0,014
Pracovní teploty	10℃ až +70℃
Ovladače	pro Windows 98 až XP (kromě NT)

6 NOVÉ TRENDY

6.1 Spektroskopie kůže

Jedná se o metodu využívající k identifikaci lidskou kůži. Lidská kůže je rozdělena do několika vrstev, přičemž každá vrstva má jinou tloušťku. Vyznačuje se svou jedinečností, je jedinečně zvlněná a obsahuje další jedinečné charakteristiky. U každého člověka se liší hustota a rozmístění kapilárního lůžka, velikost a hustota buněk uvnitř pleťových vrstev.

Vybraná část pokožky se ozáří světlem o více vlnových délkách (od viditelného až k blízkému infračervenému). V různých vrstvách pokožky se láme a odráží jiné vlnové délky světla. Poté je odraz zachycen přijímačem složeným z fotodiod a zaslán k dalšímu zpracování a analýze.[6]



Obr. 32. Princip spektroskopu. [3]

6.2 Identifikace podle nosu

Nově zkoumanou metodou je identifikace podle nosu. Každý člověk má jinak tvarovaný nos.

Podle určitého tvaru nosu, rozdělujeme do 6 skupin:

- Římský
- Řecký
- Núbijský
- Jestřábí

- Tupý
- Zatočený nahoru

Obr. 33. Rozdělení skupin podle tvaru nosu.

Obraz nosu zachycený CCTV kamerou nebo 2D fotografii je porovnáván s databází systému. Ani v případě menší plastické operace nosu by nemělo dojít ke znemožnění identifikovat osobu. Výzkum metody je prozatím v počátku, kdy zkoumají, zda je systém schopen rozlišit i osoby sobě velmi podobné např. pocházející ze stejné rodiny.

Bude-li výzkum úspěšný, může být tento systém běžně k vidění na letištích, bankách apod.[5]

ZÁVĚR

Vývoj biometrických systémů sebou přináší určitou pohodlnost a bezpečnost používání. Proto se stala biometrická identifikace dynamicky se rozšiřujícím oborem. Avšak s rychlým rozvojem biometrických technologií a jejich uplatňování v praxi vyvstávají obavy týkající se ochrany práv a svobod člověka. Daná problematika rozděluje názory lidí na dvě skupiny. Jedna se obává o zneužití prostředků k omezení svobody a druhá polovina plně podporuje zavedení biometrických systémů ke zvýšení bezpečnosti.

Cílem práce bylo seznámení s biometrickými metodami využívanými v praxi. Popsat jejich princip činnosti, stálost snímaných charakteristik, přesnost a vhodnost použití. Biometrické technologie jsou již dostupné k širokému používání, ale z důvodu neinformovanosti a nepopulárností ze strany uživatelů nejsou biometrické systémy moc rozšířené. V práci je model návrhu zabývající se řešením přístupového systému pomocí biometrických prvků a základní ochranou dat.

Ačkoliv je na trhu mnoho metod identifikace, stále patří mezi nejvíce rozšířenou metodu identifikace pomocí otisku prstu. Je to zapříčiněno nejlepším poměrem cena:výkon. Snímací zařízení otisků prstů je za mnohem přijatelnější cenu, při zachování stejné přesnosti, než snímací zařízení u jiných biometrických metod.

Výzkum biometrických metod stále pokračuje, přichází s novými metodami biometrické identifikace, některé přesnější a jiné méně přesné. V budoucnu se budu s velkou pravděpodobností biometrická identifikace rozšiřovat i nadále do běžných aplikací. Proto lze očekávat, že se s nimi budeme v nejbližších letech setkávat čím dál častěji.

ZÁVĚR V ANGLIČTINĚ

The advancement of biometric systems brings with it a certain comfort and security. For this reason the biometric identification system is valued in the growing industry. Even though the rapid advancement of biometric technologies has spread throughout the industry there are still concerns about the user's government rights and identity security. There are two common opinions about this issue. One is against the use of biometric systems because of their concern that there might be a misuse of the user's personal identification information which will compromise the person's identity. The other is fully supportive of biometric technology, saying it will benefit the entire countries security system.

The conclusion of my practice was to familiarize myself with the biometric methods used in the field. I had to document their principal activities, their current characteristics, their accuracy and proper use. Then we were given a scenario at work and had to solve it using biometric methods to establish a proper outcome. Biometric technologies have a wide range of use but without the right information and education provided to the user they are not desirable and wide spread.

Even though there are many identification methods on the market, this one is still wide spread throughout the market with the help of finger printing due to the cost/productivity. The cost of finger print imaging (even with the same image quality) is far more feasible then other biometrical methods.

The innovation of biometric systems is still growing. Some systems are more accurate than others but the development is on the rise. I believe that in the future biometric systems will spread into other applications and we as a human race will come in contact with biometric systems on a regular basis.

SEZNAM POUŽITÉ LITERATURY

[1] RAK, Roman, et al. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha : Grada Publishing, 2008. 664 s. ISBN 978-80-247-2365-5.

[2] Ekey [online]. [cit. 2010-05-16]. Dostupné z WWW: <http://www.ekey.cz/produkty/>.

[3] Biometrics [online]. 2007 [cit. 2010-05-16]. Dostupné z WWW: <http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm>.

[4] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. , 2008. 58 s. Dostupný z WWW: http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf

[5] University of Bath [online]. 2.března 2010 [cit. 2010-05-16]. Software sniffs out criminals by the shape of their nose. Dostupné z WWW: <http://www.bath.ac.uk/news/2010/03/02/nose-recognition/>.

[6] Center of Unifield Biometrics and sensors [online]. [cit. 2010-05-16]. Skin Spectroscopy. Dostupné z WWW: <http://www.cubs.buffalo.edu/skin.shtml>.

[7] Krimi [online]. 2009 [cit. 2010-05-16]. Obrazce a znaky kůže. Dostupné z WWW: <http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm>.

[8] KAZDEROVÁ, Jaroslava. Význam a charakteristika identifikačních biometrických systémů v PKB. Zlín, 2007. 75 s. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[9] Paladix [online]. 2003 [cit. 2010-05-17]. Barevné vidění: druhý pohled. Dostupné z WWW: <http://www.paladix.cz/clanky/barevne-videni-druhy-pohled.html>.

[10] Whiteqube [online]. 2010 [cit. 2010-05-17]. Destiny digital smart pen. Dostupné z WWW: <http://www.whiteqube.co.uk/skin/frontend/default/whiteqube/images/media/destinypen1.jpg>.

[11] Security ZONE [online]. 2004 [cit. 2010-05-17]. Medvídek. Dostupné z WWW: <http://www.jujitsu.cz/Listopadky/2004/Clanky/Img/03_Irismuster.jpg>.

[12] ČANDÍK, M., Objektová bezpečnost II, UTB ve Zlíně, 2004

[13] SKOUMAL, Miroslav. Identifikace člověka pomocí biometrických údajů. Ústí nad Labem, 2007. 50 s. Bakalářská práce. Univerzita Jana Evangelisty Purkyně v Ústí nad Labem.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PKB Průmysl komerční bezpečnosti.

CCTV Closed Circuit TV - Uzavřený televizní okruh.

PCA Principal Components Analysis - Analýza hlavních komponentů

LDA Linear Discriminant Analysis - Lineární diskriminační analýza

EBGM Elastic bunch graph matching - Elastický srovnávací diagram

FAR False Acceptance Rate - Koeficient nesprávného přijetí

FRR False Rejection Rate Koeficient nesprávného odmítnutí

AFIS Automated Fingerprint Identification System - Automatický systém identifikace dle otisku prstu

IR Infračervené záření

CMOS Complementary Metal Oxid Semiconductor - Polovodič s vrstvou kysličníku křemíku

SEZNAM OBRÁZKŮ

SEZNAM TABULEK