Biometrický snímač otisku prstů

Biometric Scanner of Fingerprint

Martin Končický

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Martin KONČICKÝ**
Osobní číslo:	**A10081**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Biometrický snímač otisků prstu**

Zásady pro vypracování:

1. **Uveďte základní terminologii a metody v oblasti biometrické identifikace.**
2. **Popište vlastnosti lidské pokožky.**
3. **Uveďte typy snímačů otisku prstů, jejich vlastnosti, vysvětlete principy.**
4. **Otestujte funkčnost konkrétního snímače otisků prstů.**
5. **Analyzujte funkce softwaru ke snímači otisků prstů a navrhněte jeho další funkce.**
6. **Navrhněte a vypracujte úlohu do laboratorního cvičení.**
7. **Odhadněte další vývoj.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**
2. **RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.**
3. **BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.**
4. **LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.**
5. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**

Vedoucí bakalářské práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

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

ABSTRAKT

Bakalářská práce se zabývá biometrickým snímačem otisku prstů. V teoretické části práce je uveden přehled biometrické terminologie, přehled metod biometrické autentizace, popis vlastností pokožky a souhrn typů snímačů otisků prstů. Praktická část obsahuje způsob testování funkčnosti snímače otisku prstů, analýzu dodávaného softwaru, navrhnutí a vytvoření laboratorní úlohy a odhad vývoje snímačů otisků prstů.

Klíčová slova: biometrie, biometrické metody, otisk prstu, snímače otisku prstů.

ABSTRACT

Presented bachelor`s thesis is focused on biometric fingerprints scanner. In theoretical part of the work, overview of biometric technology, methods of biometric authentication, properties of the skin and summary of the fingerprints scanner types are described. Practical part of the work is dealing with testing of the fingerprints scanner functions, supplied software analysis, specification of the solved task and estimation of the future development of the scanners.

Keywords: biometrics, biometrical methods, fingerprint, fingerprint scanners.

Tímto bych rád poděkoval vedoucímu mé bakalářské práce panu Ing. Rudolfovi Drgovi za odborné vedení, připomínky, náměty a poskytnuté konzultace při zpracování bakalářské práce.

Dále bych chtěl poděkovat své rodině a přátelům za jejich podporu.

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

Identifikace na základě otisků prstů má dlouhodobou historii. Už před pěti tisíci lety byly otisky prstů využívány k podpisu smluv, k uzavírání obchodních transakcí, apod. O rozmach v poznání papilárních linií se zasloužil český anatom Jan Evangelista Purkyně, který položil základní kámen pro vývoj daktyloskopie.

Autentizace pomocí biometrických vlastností člověka je v dnešní době považována za velmi bezpečnou metodu. Biometrické snímače jsou převážně využívány ve státních organizacích, ale postupně se začleňují do podniků a některých domácností. Je otázkou času, kdy se implementují do běžného života člověka.

Snímače otisku prstů jsou nejpoužívanějším biometrickým systémem. Jsou dostatečně přesné, uživatelský přívětivé a levné. Jejich zastoupení na trhu mluví za vše, kde mají 40% podíl na trhu s biometrickými systémy.

Bakalářská práce je rozdělena do dvou částí. Teoretická část objasňuje terminologii, uvádí jednotlivé biometrické metody, popisuje stavbu lidské kůže a v poslední kapitole se zabývá vysvětlením principů a popisu vlastností jednotlivých typů snímačů otisku prstů. Praktická část je založena na práci se snímačem otisku prstů, Veri-Pass FX MV1610. Praktická část se zabývá ověřením funkčnosti snímače, popisem dodávaného softwaru výrobcem a návrhem jeho dalších funkcí. Další kapitola praktické části předkládá návrh a zpracování laboratorní úlohy. Poslední kapitola se zabývá odhadem dalšího vývoje a využití snímačů otisků prstů.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE A METODY V OBLASTI BIOMETRICKÉ IDENTIFIKACE

1.1 Terminologie

1.1.1 Biometrie

Biometrie je vědní obor, který se zabývá metodami, které vedou k rozpoznání člověka na základě jeho biologických nebo behaviorálních vlastností. Slovo biometrie pochází z řečtiny. Skládá se ze slova „bios“, což znamená život a ze slova „metros“, které znamená měření. V technických oborech lze biometrii definovat jako automatizované rozpoznávání lidských jedinců na základě jejich charakteristických anatomických, fyziologických rysů (např. obličej, otisk prstu, duhovka, DNA, apod.) a behaviorálních rysů (jako např. hlas, písmo, dynamika psaní na klávesnici, atd.).

1.1.2 Identita

Identita (lat. identitas, odvozené od slova idem - stejný), neboli totožnost je charakteristika každého z nás. Rozlišujeme fyzickou a elektronickou identitu. Fyzickou identitu máme pouze jednu a je jedinečná. Na světě neexistují 2 lidi, kteří mají shodnou identitu. Fyzická identita je tvořena anatomickými, fyziologickými a behaviorálními rysy. Naopak elektronických identit můžeme mít několik (jedná se např. o účty na e-mailových portálech).

Identita je založena na:

- znalosti,
- vlastnictví,
- biometrii.

Znalost

Identita založená na hesle je vůbec nejpoužívanější metodou při ověřování totožnosti. Setkáváme se s ní takřka denně při přihlašování do elektronické pošty, při placení platebními kartami, při zadávání PIN kódu, apod. Výhoda hesla je v nízké pořizovací ceně. Nevýhodou je, že existuje riziko zjištění hesla druhou osobou, a to buď softwarovým lámáním hesel, nebo vysledováním při použití hesla. Protože heslo by mělo být bezpečné, to znamená dlouhé minimálně 8 znaků, s použitými znaky jako jsou velká

a malá písmena, číslice a speciální znaky, automaticky vzniká další nevýhoda, a to zapomenutí hesla.

Vlastnictví

Bezpečnější metodou autentizace je s použitím identifikačního předmětu, jako je čipová karta, apod. Při použití předmětu si uživatel nemusí pamatovat heslo. Nevýhodou je možnost odcizení identifikačního předmětu a neoprávněné jeho užívání.

Biometrie

Biometrická autentizace snímá biometrické vlastnosti uživatele. Protože je měřená biometrická vlastnost neodcizitelná, na rozdíl od čipové karty a na rozdíl od hesla, není možnost jejího ztracení, je biometrická autentizace považována za nejbezpečnější metodu. Biometrické vlastnosti lze rozdělit do dvou skupin, a to anatomicko-fyzikální vlastnosti a behaviorální vlastnosti.

1.1.3 Identifikační prvek

Identifikační prvky slouží k předložení systému pro ověření, nebo zjištění totožnosti.

Rozdělení identifikačních prvků:

- Manuální – např. kódové zámky.
- Čipové
    - kontaktní – např. SmartCard, iButton čipy,
    - bezkontaktní – např. RFID,
    - kombinované.
- Magnetické – karty s magnetickým proužkem.
- Optické – např. čárový kód.
- Radiofrekvenční – např. Bluetooth.
- Biometrické – např. DNA, papilární linie, oční duhovka. [1, str. 125]

1.1.4 Rozpoznávání (Recognition)

V oblasti biometrie znamená rozpoznávání člověka při zkoumání vhodné biometrické vlastnosti.

1.1.5 Autentizace (Authentication)

Stejně jako u rozpoznávání se jedná o rozpoznávání člověka. Rozdíl, kterým se tyto pojmy liší, je ten, že u autentizace získá uživatel informaci ohledně výsledku, jako např. identita nalezena/nenalezena, vstup oprávněn/ neoprávněn, apod.

1.1.5.1 Skóre (Score)

Skóre je hodnota, která vyjadřuje míru shody dvou porovnávaných biometrických vzorků. Ideální hodnota skóre je 100, ovšem v reálu není možné takového vysokého skóre nikdy dosáhnout.

1.1.5.2 Mez

Mez je hodnota, která je definována administrátorem. Biometrický vzorek, který má vyšší skóre než definovaná mez, je považován za vyhovující.

1.1.6 Identifikace (Identification)

Identifikace je proces zjišťování totožnosti. Uživatel předá svoji biometrickou vlastnost biometrickému systému a systém má za úkol zjistit identitu neznámé osoby. Výstupem systému je buď nalezení identity v databázi, nebo nenalezení identity. Tento proces může být zdlouhavý, protože se porovnává určitý biometrický vzorek se všemi biometrickými vzorky uložené v databázi systému.

1.1.7 Verifikace osoby (Verification)

Verifikace znamená ověřování pravdivosti výroku. Uživatel zadá svoji identitu a úkolem biometrického systému je identitu ověřit. Pokud je záznam nalezen, dojde k porovnání dat s výsledkem shody, je-li identita potvrzena, nebo nepotvrzena. Protože uživatel předal svoji identitu, tak systém porovnává určitý biometrický vzorek s určitým uloženým biometrickým vzorkem v databázi. Režim autentizování je 1:1. Proto je verifikace rychlejší a méně náročnější na výkonnost systému než identifikace.

1.1.8 FAR (False Acceptance Rate)

Míra nesprávných přijetí. FAR udává pravděpodobnost, kdy neoprávněný uživatel získá přístup. Neoprávněný uživatel je systémem rozpoznán jako některý z oprávněných uživatelů a je úspěšně autentizován.

$$FAR = \frac{počet\ nesprávných\ přijetí}{počet\ všech\ pokusů\ neoprávněných\ osob\ o\ autentizaci} \cdot 100\ [\%]$$

1.1.9 FRR (False Rejection Rate)

Míra nesprávných odmítnutí. FRR udává pravděpodobnost, kdy oprávněný uživatel nezíská přístup. Oprávněný uživatel není systémem rozpoznán a není úspěšně autentizován.

$$FRR = \frac{počet\ nesprávných\ odmítnutí}{počet\ všech\ pokusů\ oprávněných\ osob\ o\ autentizaci} \cdot 100\ [\%]$$

1.1.10 FER (Failure To Enroll Rate)

FER vyjadřuje pravděpodobnost, kdy registrace uživatele selhala z důvodu zranění, vlivem okolního prostředí, apod. FER je pohyblivá veličina, která má vztah nejen k uživateli, ale také ke konkrétní biometrické vlastnosti.

$$\text{FER} = \frac{počet\ neúspěšných\ pokusů\ o\ registraci\ uživatele\ (vlastnosti)}{počet\ všech\ pokusů\ uživatele\ (vlastnosti\ o\ registraci)} \cdot 100\ [\%]$$

1.1.11 FTA (Failure To Acquire Rate)

FTA vyjadřuje pravděpodobnost, kdy systém z důvodu vlivu okolního prostředí, nedodržení pokynů výrobce pro instalování systému, apod., není schopen sejmout biometrický vzorek v době, kdy uživatel svoji biometriku předkládá.

$$FTA = \frac{počet\ neúspěšně\ sejmutých\ biometrických\ vzorků}{počet\ všech\ pokusů\ o\ snímání} \cdot 100\ [\%]$$

1.2 Metody biometrické autentizace

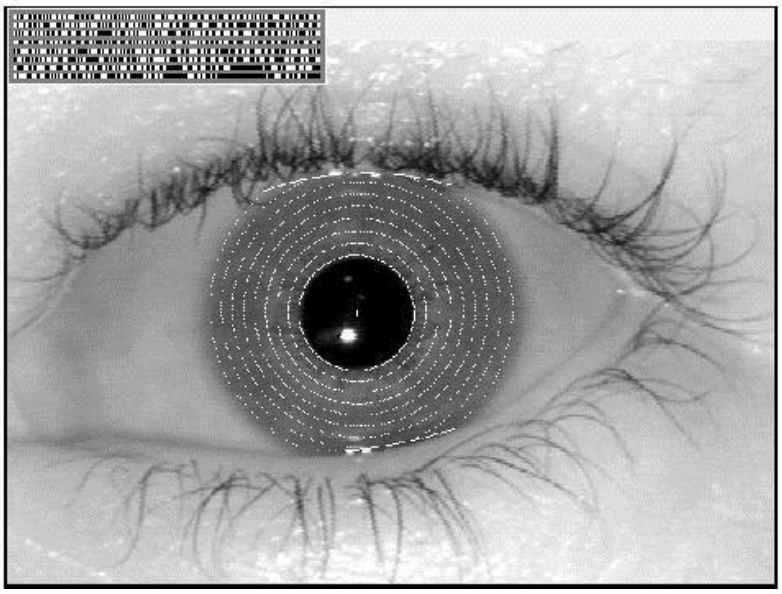
Kapitola uvádí souhrn rychle se vyvíjejících biometrických technologií. U každé technologie jsou uvedeny její výhody a nevýhody.

1.2.1 Autentizace na základě anatomicko-fyziologických charakteristik

Anatomicko-fyziologické vlastnosti jsou nejvhodnější pro biometrickou autentizaci. Jsou jedinečné, poměrně stabilní, neustále přítomny a obtížně ovlivnitelné. Tvoří vhodný předmět pro biometrickou autentizaci.

1.2.1.1 Oční duhovka

Duhovka je oční sval tvarem mezikruží, který na základě dopadajícího světla na oko, mění velikost zornice. Jako vnitřní orgán těla je duhovka odolná proti poškození vnějším prostředí, během života se nemění. Je velmi dobře viditelná, pro snímání oka postačí standardní videokamera. Duhovka má složitý vzor, k jejímu rozpoznání se využívá charakteristických znaků, jako jsou klenuté vazy, klikaté čáry, pigmentové okraje, pupilární oblasti, hřebeny, krypty, radiální rýhy, pihy, prstence, korány, atd. Těchto charakteristických znaků je přibližně 250. Pravděpodobnost nalezení dvou osob se stejnou duhovkou je mnohem menší než u otisků prstů, proto identifikace pomocí oční duhovky patří mezi nejspolehlivější biometrické metody.



Obrázek 1: Snímek oční duhovky [2]

Výhody:

- přesná, spolehlivá a rychlá metoda,
- bezkontaktní, hygienická metoda,

- nošení brýlí snímači nevadí.

Nevýhody:

- vyšší cena a malá nabídka zařízení,
- problémy s funkčností při očních chorobách a při nošení kontaktních čoček.

1.2.1.2 Oční sítnice

Méně rozšířenou metodou je rozpoznávání sítnice. Sítnice je tenká vrstva o síle 0,2 - 0,4 mm umístěna uvnitř, na zadní straně oka. Jejím hlavním úkolem je zpracování světelných signálů, přicházejících přes čočku oka. Pro identifikaci se snímá prostor v okolí tzv. slepé skvrny. Slepá skvrna (nebo také optický disk) je část sítnice, kudy vystupuje zrakový nerv s artérií sítnice. Sítnice je velmi dobře chráněna proti poškození a po dobu života se nemění. Pro svoji vysokou spolehlivost se používá v objektech s nejvyšším stupněm zabezpečení.

Obrázek 2: Snímek sítnice oka [3]

Výhody:

- vysoká přesnost při přijetí uživatele (FAR) a bezpečnost.

Nevýhody:

- nekomfortní, snímání trvá až 15 sekund, kdy uživatel musí mít oko ve vzdálenosti 2 cm od kamery,
- pravděpodobnost chybného odmítnutí (FRR) je vysoká,
- problémy při snímání oka s chorobami a s některými kontaktními čočkami,
- nepoužitelné ve venkovním prostředí nebo v prostorech s velkým množství světla.

1.2.1.3 Tvář

Jedná se o metodu, která je založena na poznatcích antropologie.

Antropologie je věda zabývající se člověkem, lidskými společnostmi a lidstvem vůbec. K popisu charakteristických znaků člověka využívá několik metod, které se navzájem doplňují, a to antropometrii, osteometrii a somatoskopii.

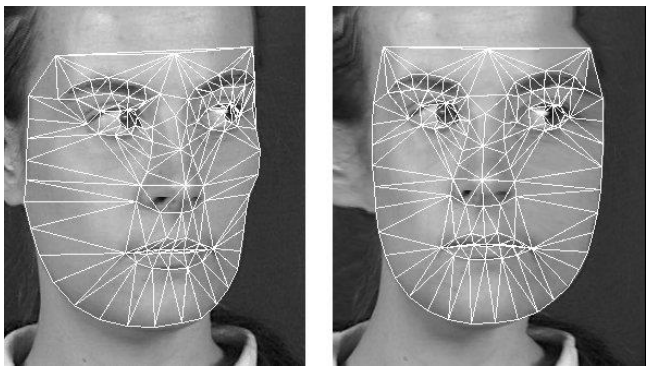
Antropometrie je soubor technik měření lidského těla pomocí délek, hmotností, obvodů, úhlů, apod. Byla založena roku 1883 francouzským policejním důstojníkem Alphonsem Bertillonem. Osteometrie je založena na stejném principu jako antropometrie, jen předmětem pro měření není lidské tělo, ale kosterní pozůstatky. Poslední metodou je somatoskopie, která se zabývá vývojem, velikostí nebo absencí charakteristického znaku člověka.

Pro identifikaci tváře je potřeba změřit vzdálenosti mezi 12 body, které se nachází na očích, uších, ústech a nosu. Patří sem přechod nosu do čela, špička nosu, vnitřní a vnější koutky očí, horizontální koutky rtů, spojení ušního lalůčku s tváří a body na chrupavce ucha chránící vnější zvukovod.

Existují 3 způsoby rozpoznávání obličeje:

- na základě 2D snímku,
- na základě 3D snímku,
- na základě termosnímku.

2D snímání



Obrázek 3: 2D snímek tváře [4]

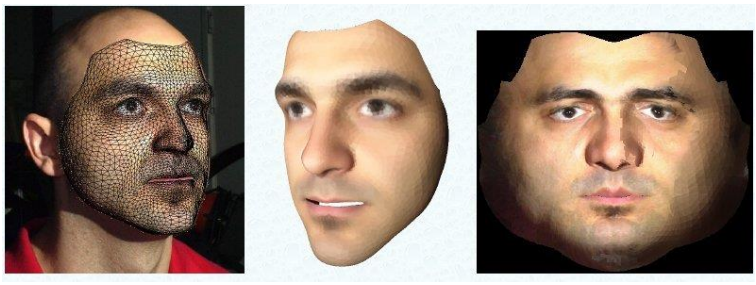
Výhody:

- možnost registrovat osobu ze záznamu nebo fotografie,
- systém používá běžné kamery.

Nevýhody:

- nízká přesnost a bezpečnost – lehce oklamatelné,
- možnost nevědomého získání identifikačního prvku,
- změna vizáže uživatele může být problematické pro identifikaci.

3D snímání



Obrázek 4: 3D snímek tváře [4]

Výhody:

- přesná a spolehlivá metoda,
- jednoduchá obsluha.

Nevýhody:

- citlivost na světlo,
- vyšší cena,

- omezení funkčnosti dosahem projektoru kamery,
- změna vizáže uživatele může být problematické pro identifikaci.

Termosnímek

Obrázek 5: Termosnímek tváře [5]

Výhody:

- nezávislost na vnějším osvětlení,
- obtížné vytvoření falzifikátu,
- vhodný pro kombinaci s předešlými metodami.

Nevýhody:

- nevhodný při samostatném použití,
- nestálá teplotní charakteristika člověka, může mít za důsledek špatného rozpoznání termokamerou.

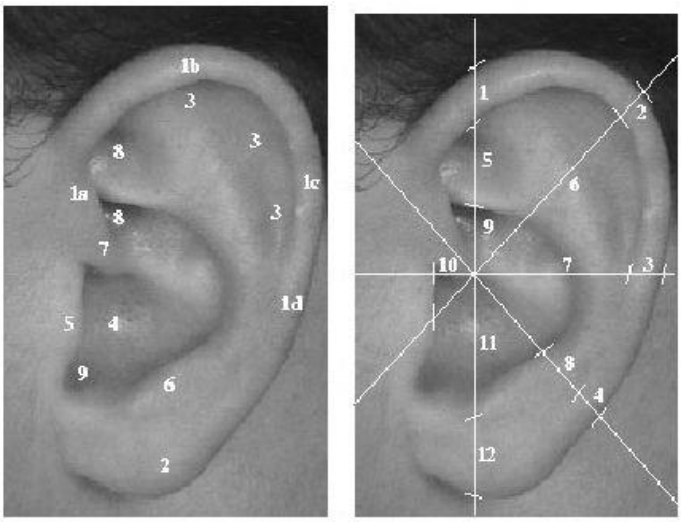
1.2.1.4 Tvar vnějšího ucha

Tvar vnějšího ucha lze snímat 3 způsoby:

- podle morfometrických vztahů,
- podle otisku ušního boltce,
- podle termografického snímku ušního boltce.

Způsob identifikace podle morfometrických vztahů využívá Iannarellisův systém, což je systém využívaný v antropometrii, který k popisu ucha používá 12 ušních rozměrů. Ucho se snímá do vzdálenosti jednoho metru speciálním optickým zařízením, které snímá v 2D, nebo v 3D formě. [6, str. 252-253]

Metoda založena na otisku ušního boltce není určena pro komerční využití. Pro uživatele je tato metoda velmi nekomfortní. Využívá se pro forenzní účely. Termograf ušního boltce mapuje tělesnou teplotu rozloženou na ušním boltci.



Obrázek 6: Snímek tvaru vnějšího ucha [7]

Výhody:

- metoda bez fyzického kontaktu.

Nevýhody

- malá rozlišovací schopnost.

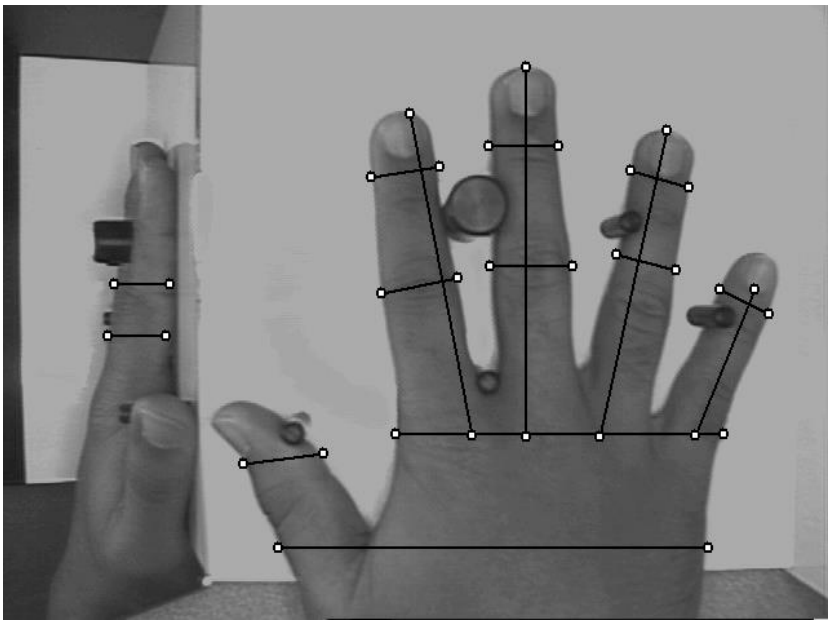
1.2.1.5 Geometrie ruky

Většina systémů snímá ruku ze seshora (hřbet ruky), nebo zezdola (dlaň ruky) po položení ruky na snímací plochu. Některé systémy využívají dalšího upraveného zrcadla, kterým lze snímat ještě ruku z boku. Snímací plocha obsahuje 5 distančních kolíčků, které udávají polohu pro správné položení ruky na snímací plochu. Pro snímání se používá standardní kamera, která může snímat černobíle s rozlišením od 100 dpi.

Pro rozpoznání uživatele používají systémy následující parametry ruky:

- délka prstů,
- šířka prstů,
- výška prstů,

- zakřivení a lokální anomálie.



Obrázek 7: Snímání geometrie ruky [8]

Výhody:

- přesnost při využití 3D snímání,
- komfortní pro uživatele,
- vhodná pro nevidomé uživatele,
- odolnost proti nečistotám,
- malá náročnost na paměťovou kapacitu, šablona má pouze přibližně 9 bytů.

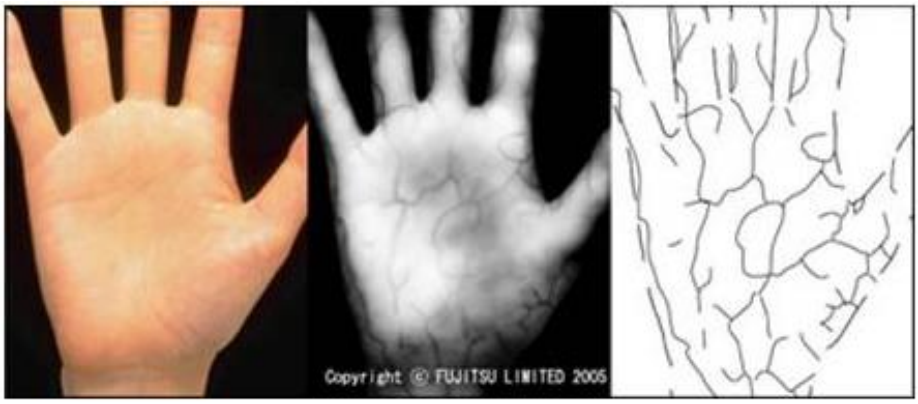
Nevýhody:

- nízká variabilita identifikačního prvku a přesnost,
- nerozpozná živou tkáň,
- lze použít jen pro verifikaci,
- lidé trpící Parkinsonovou chorobou nedokážou správně položit ruku mezi distanční kolíčky,
- nutnost sundávání prstenů,
- nelze použít ve venkovním prostředí.

1.2.1.6 Krevní řečiště ruky

Další biometrickou identifikační metodou podle ruky je rozpoznávání uživatelů podle snímků cévního stromu ruky. Snímač snímá cévy ruky, které jsou u každého

uživatele unikátní a během celého života uživatele stabilní. Pod pojmem cévy rozumíme žíly, které vedou krev směrem k srdci, tepny, které vedou krev směrem od srdce a vlásečnice, které propojují žíly a tepny. Systém zjišťuje geometrické rozmístění cév, jejich tvar, velikost a orientaci. Cévy jsou pouhým okem neviditelné, k pořízení snímků se používá monochromatická CCD kamera v kombinaci s nasvícením pole infračervených diod.



Obrázek 8: Krevní řečiště ruky [9]

Výhody:

- přesná a spolehlivá metoda,
- bezkontaktní, hygienická metoda,
- vysoká obtížnost falšování, obtížné napodobení cévní sítě.

Nevýhody:

- malá nabídka zařízení,
- vyšší cena.

1.2.1.7 Otisk prstu

Technologie rozpoznávání otisku prstu má bohatou minulost. Mezi první civilizace, které používaly otisky prstů byli Babylóňané, asi 3000 let př. n. l. Otiskovali palec do hliněných tabulek jako potvrzení uzavření obchodní transakce. Kolem roku 500 př. n. l. v Číně, zanechávali autoři listin otisky prstu na svých listinách. Řečtí umělci často nechávali otisky prstů na keramice, protože používali prsty ke zdobení svých výrobků. Čínský zákoník, který byl platný od 7. století, až do 10. století, přímo nařizoval připojení

otisku prstu do dokumentu, ve kterém muž uvádí své důvody k rozvodu. Daktyloskopie, nauka o kožních papilárních liniích, se dočkala svého rozmachu v 19. století.

V roce 1823, český anatom, fyziolog, biolog, básník a filozof, Jan Evangelista Purkyně jako první popsal kresby na bříškách prstů. Zjistil, že jsou pro člověka jedinečné a během života jsou stabilní. Bříška prstů popisoval čistě z lékařského hlediska. I když ve svém 54 stránkovém spisu, týkající se o 9 třídách otisků prstů, „Comentatio de examine pbysologico organi visus et systematis cuntanei“, neuvádí přínos jeho objevů pro kriminalistiku, tak nepřímo ovlivnil vývoj daktyloskopie.

V roce 1858 William James Herschel, britský koloniální úředník, vyžadoval po indickém dodavateli materiálu pro stavbu silnic otisk prstu místo podpisu pro potvrzení smlouvy. Tímto způsobem získal jistotu, že dodavatel dohodu splní. Místní obyvatelé totiž považovali takto podepsanou smlouvu za něco závažnějšího, než smlouvu podepsanou ručně. Tuto formu podpisu použil při mnoho dalších listin. Až byla jeho sbírka otisků prstů dostatečně velká, došel k závěru, že otisky prstů jsou jedinečné. Po návratu do Anglie sepsal svoje poznatky do knihy „The Origin of Fingerprinting“. William James Herschel je považován za jednoho z průkopníků v oblasti daktyloskopie, i když jeho poznatky chtěl využívat pouze v administrativě při dokazování identit osob.

V roce 1880 Henry Faulds, skotský vědec, jako první navrhl, že poznatky ohledně otisků prstů by mohly být využity, ke zjištění identity pachatele z místa trestného činu. Aby bylo možné identifikovat sériové zločince, navrhl vytvoření sbírky otisků prstů těchto zločinců.

V roce 1894 Francis Galton, anglický vědec a bratranec Charlese Darwina, vydal na základě prostudování Herschelových materiálů, svých měření a poznatků, práci „Fingerprints“. Vědecky prokázal, že na světě neexistují 2 stejné otisky prstů a jejich neměnnost. Vypočítal, že pravděpodobnost nalezení stejných otisků prstů je přibližně 1:64 miliardám. Zjistil, že praktický každý otisk prstu obsahuje oblast, ve které se sbíhají linie. Po jeho pojmenování se dodnes této oblasti říká delta. Na základě delty určil 4 typy otisků prstů: otisky s deltou doleva, otisky s deltou doprava, otisky s několika deltami a otisky bez delty.

Rok 1896 se považuje za období, kdy se konečně začaly daktyloskopické poznatky široce využívat v praxi. Za zakladatele kriminalistické daktyloskopie můžeme považovat 2 kriminalisty. Argentinský policejní úředník Juan Vucetich a londýnský policejní prezident

Edward Richard Henry, kteří si osvojili daktyloskopické poznatky a dokázali je využít v praxi.

Metoda identifikace pomocí otisků prstů má dnes jinou formu, než před více než 100 lety, kdy se otisky prstů nanášely na identifikační karty. Tato „papírová“ forma je velmi zdlouhavá, neefektivní, v dnešní době nepoužitelná. Pomocí počítačové techniky se metoda rozpoznávání podle otisků prstu stala plně automatizovanou.

Technologie rozpoznávání otisků prstu je nejznámější a nejpoužívanější metodou vůbec. Snímač snímá obrazce papilárních linií, které obsahují tzv. markanty. Markanty jsou jakékoliv změny v papilárních liniích. Různým počtem markantů, jejich umístěním a jejich vzájemnou kombinací je dána unikátnost každého otisku prstu. Pro vyhodnocení, jestli jsou otisky stejné, je potřeba nalézt několik podobných markantů. Záleží na nastavení meze snímače.

Výhody:

- široká nabídka snímačů,
- nízká cena,
- energeticky málo náročné, malé rozměry – možnost mobilního použití.

Nevýhody:

- bez kontroly živosti lehce oklamatelné,
- otisk lze snadno získat bez vědomí uživatele,
- problém při snímání prstu s kožními chorobami.

1.2.1.8 Struktura nehtu

I nehet obsahuje potřebné informace k rozpoznávání osob. Nehet se skládá celkem ze šesti částí. Pro rozpoznávání osob je nejdůležitější nehtové lůžko, které je umístěno pod nehtovou ploténkou. V nehtovém lůžku vybíhají ze škáry podélné lišty, které tvoří nehet jedinečným. Pro snímání struktury nehtu se používá bílé světlo nebo odražené světlo z interferometru.

Výhody:

- neinvazivní, společensky přijatelná metoda,
- vhodná jako doplněk pro snímání otisku prstů.

Nevýhody:

- náchylnost na mechanické poškození nehtu,
- metoda se zatím na světě neprosadila.

Další, poměrně novou technologií, je ukládání informací na nehet. Technologie pochází z Japonska, která umožňuje na nehet zapsat bity, pomocí pulsů laseru o vlnové délce 800 nm. Mikroskop s UV osvětlením je schopen přečíst fosforeskující bity. Všechny nehty člověka jsou schopné nést informaci o velikosti 12,5 MB.

Výhody:

- vhodné úložiště informací, jako jsou klíče, hesla, osobní informace (krevní skupina), apod.

Nevýhody:

- identifikace jen těch osob, které byly označeny.

1.2.1.9 DNA

Kyselina deoxyribonukleová (DNA) je považována za nejlepší identifikátor osob. Její struktura definuje každého jedince na světě. DNA je považována jako přímý důkaz před soudem, proto zaujímá nezastupitelnou roli ve forenzní medicíně. Pro autentizaci v oblasti elektronické kontroly vstupu je ovšem tato metoda nepoužitelná.

Výhody:

- vysoká přesnost,
- DNA lze lehce získat, např. z oblečení, nedopalku od cigarety,
- z DNA lze zjistit mnoho informací, jako rasa, pohlaví, zdravotní stav, apod.

Nevýhody:

- příliš drahé,
- nevhodný pro elektronickou kontrolu vstupu, možnost obelhání cizím vzorkem.

1.2.2 Autentizace na základě behaviorálních charakteristik

Behaviorální charakteristiky nejsou neustále přítomny, objevují se až v souvislosti s nějakou činností člověka. Zkoumají se rysy lidského chování, které jsou ovšem snadno

ovlivnitelné momentálním fyzickým či psychickým stavem člověka. Proto jsou v praxi používány méně často.

1.2.2.1 Podpis a písmo

Rozpoznávání podle rukopisu využívá z pohledu biometrie část statických vlastností a část dynamických vlastností. Klasické rozpoznávání podle písma patří do statických vlastností. Určuje se podle velikosti písma, sklonu písma, grafických návyků při psaní, apod. Statické vlastnosti písma jsou považovány za vlastnosti nedostatečné pro rozpoznávání, nesou málo informací a jsou lehce zfalšovatelné. Dynamické vlastnosti nesou dostatečné množství informací. Vyhodnocuje se rychlost psaní podpisu, akcelerace, tlak hrotu pera při jednotlivých fázích rukopisu, směr a posloupnost psaní diakritiky, apod. Rukopis je ovlivňován také vnějšími faktory, jako je poloha těla při psaní, pootočení papíru, tabletu, apod.

Výhody:

- levná a rychlá metoda,
- přijatelná u uživatelů, možnost využití v místech, kde se používá klasický podpis.

Nevýhody:

- pro člověka může být obtížné se podepsat stejně,
- zatím málo rozšířené,
- náchylnost při poranění ruky.

1.2.2.2 Hlas

Biometrická technologie rozpoznávání podle hlasu je méně používaná. Využívá se hlavně v kriminalistické metodě tzv. fonoskopie. I když se hlas během života vyvíjí, lze říct, že v období od 20 let do 60 let člověka je hlas poměrně stabilní. Části těla, jako hlasivky, čelisti, měkké patro, jazyk, rty, zuby, dýchací ústrojí, ústní a nosní dutina, definují rezonanci vokálního traktu. Systém autentizuje uživatele na základě analýzy množiny slov, které zná jen uživatel.

Výhody:

- přijatelné pro uživatele,
- možnost rozpoznání na dálku.

Nevýhody:

- nepoužitelné v hlučném prostředí,
- autentizace systému může být ovlivněna momentálním fyzickým nebo psychickým stavem uživatele.

1.2.2.3 Lokomoce

Lokomoce je schopnost se přemísťovat z místa na místo pomocí svalové činnosti. Pro člověka je typická tzv. bipedální lokomoce, což znamená schopnost se přemísťovat pomocí dolních končetin. Formy bipedální lokomoce jsou chůze, běh, skákání, lezení, plavání a volný pád. Pouze běh a chůze se v praxi využívají jako vhodné identifikátory pro biometrickou identifikaci.

Styl lokomoce je podmíněn několika faktory, a to anatomickými a psychofyziologickými vlastnostmi, tělesnou výškou a hmotností, zdravotním stavem a anatomickými diferencemi (ploché nohy, zakřivení páteře, rozdílné délky končetin, pohyblivost kyčelních kloubů, apod.), profesními a sportovními návyky, atd. Dále je lokomoce ovlivňována vnějšími faktory, jako je např. stav cesty, typ oblečení nebo tíže břemene, kterou uživatel nese. I když je rozpoznávání člověka pomocí lokomoce poměrně nová metoda, vkládají se do ní velké naděje pro použití v monitorovacích systémech s automatizovaným vyhodnocením lidské identity. Zejména jako doplňující metoda k technologii rozpoznávání podle tváře.

Výhody:

- bezkontaktní, automatizované rozpoznávání na větší vzdálenost.

Nevýhody:

- zatím neznámá rozlišovací schopnost.

2 LIDSKÁ POKOŽKA

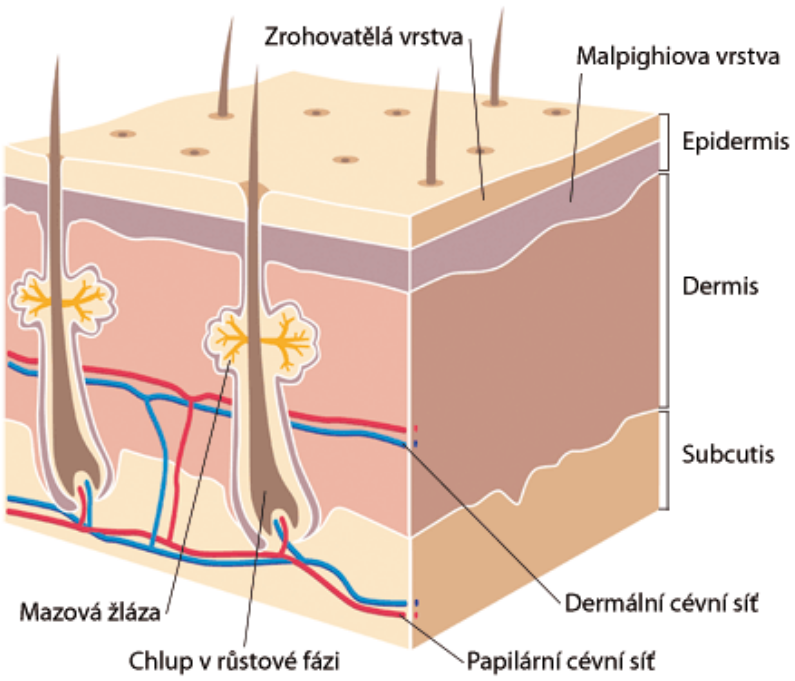
Kůže, s povrchem do 2 m^2, je největší orgán lidského těla. Její šířka se pohybuje v rozmezí od 0,4 mm do 4 mm a tvoří až 12 % tělesné hmotnosti. Nejtenčí kůže je na očních víčkách a nejtlustší na dlaních a chodidlech.

Funkce kůže:

- krycí funkce – ochrana před UV zářením, mikroorganismy, apod.,
- smyslová funkce – sídlo receptorů, reagujících na teplo, chlad, tlak a bolest,
- zásobní funkce – sklad tuku a vitamínů,
- vylučovací funkce – vylučování chemických látek z těla,
- resorpční funkce – možnost absorpce dýchacích plynů a dalších látek,
- termoregulační funkce – udržování stálé teploty těla.

Kůže se skládá z 3 hlavních částí:

- pokožka (epidermis),
- škára (corium, dermis),
- podkožní vazivo (tela subcutanea, subcutis).



Obrázek 9: Stavba kůže [10]

2.1 Epidermis

Epidermis je nejsvrchnější část lidské kůže. Je tvořen mnohovrstevným dlaždicovým epitelem. Jeho šířka může nabývat až 1,5 mm. Epidermis obsahuje kožní deriváty, jakou jsou vlasy, chlupy, nehty, mazové a potní žlázy, atd. Neobsahuje, ale žádné cévy, proto musí být vyživován ze škáry. V epidermisu se provádí obnova kůže. Staré buňky odumírají v důsledku toho, že buňky v nejspodnějších vrstvách neustálým dělením vytlačují buňky ve vyšších vrstvách. Tím se buňky dostanou do nejvyšších vrstev, kde přijdou o dodávání potřebných živin k životu a odumřou. Celá pokožka se obmění přibližně během tří týdnů. Během celého lidského života odumře až 18 kg buněk.

2.2 Corium

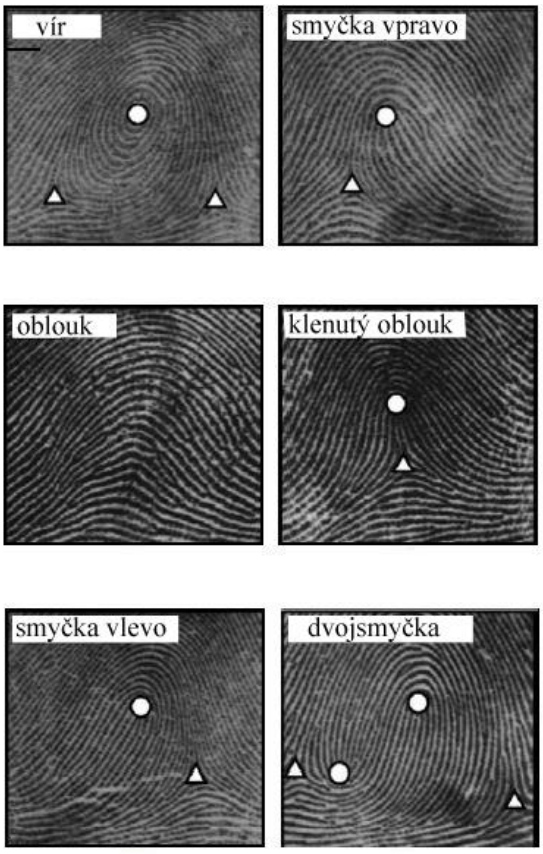
Škára je pružná, pevná, vazivová část kůže. Je nejširší a zároveň nejdůležitější vrstvou kůže. Je pevně spojena k pokožce a obsahuje množství cév a nervových vláken. Její šířka nabývá hodnot asi 0,5 mm – 2,5 mm. Škára obsahuje nervová zakončení, která detekují bolest, chlad, teplo a tlak. Dále obsahuje žlázy, a to potní, mazové a mléčné. Škára působí na pokožku svými kuželovitými útvary (tzv. papily), které tvoří na povrchu těla papilární linie, čehož využívá daktyloskopie.

2.3 Tela subcutanea

Podkožní vazivo je nejspodnější část kůže. Je tvořeno hustým kolagenním vazivem. Obsahuje tuk, tudíž šířka podkožního vaziva je dána převážně výživou. Nejtenčí je na očních víčkách, naopak nejtlustší je na hýždích, břichu a stehnech.

2.3.1 Papilární linie

Papilární linie jsou hlavním předmětem zkoumání daktyloskopie. Jsou to kožní lišty, které se tvoří na rukou a nohou a tvoří obrazce, které jsou u každého člověka jedinečné. Papilární linie dosahují šířky 0,2 mm – 0,7 mm a výšky 0,1 mm – 0,4 mm. Vznikají už během embryonálního vývoje mezi čtvrtým a pátým měsícem. Od té doby žádným způsobem nezmění svoji podobu, jen se zdokonalí svým vyvýšením a prohloubením brázd. Papilární linie jsou definovány papilami, které vyrůstají ze škáry. Na obrázku (Obrázek 10) jsou zobrazeny základní typy obrazců papilárních linií.



Obrázek 10: Papilární linie, (upraveno)
[11]

Následující tabulka (Tabulka 1) klasifikuje základní papilární linie vzhledem k umístění jedinečných bodů.

Tabulka 1: Kategorizace papilárních linií vzhledem k umístění jedinečných bodů, (upraveno) [12, str. 197]

Typ obrazu papilární linie	**Jádra**	**Delty**	**Umístění jader vzhledem k deltám**
Vír	1	2	–
Smyčka vpravo	1	1	Vlevo
Smyčka vlevo	1	1	Vpravo
Klenutý oblouk	1	1	Pod
Oblouk	0	0	–

Jádro je bod, který označuje střed dané kategorie otisků prstů. Delta je místo, kde se papilární linie rozbíhají do tří směrů.

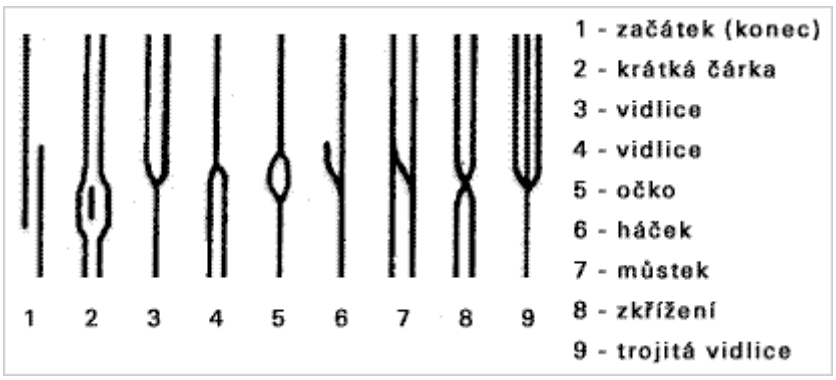
2.3.1.1 Zákonitosti papilárních linií

Podstata papilárních linií spočívá ve třech zákonitostech:

- na světě neexistují dva jedinci, kteří by měli totožné obrazce papilárních linií. Je dokázané, že na světě existuje asi 64 miliard různých variant obrazců prstu. Nalezení dvou různých osob se stejnými obrazci je vysoce nepravděpodobné, proto se daktyloskopický obrazec v kriminalistice považuje za dostatečně jedinečný.
- Obrazce papilárních linií zůstávají po celý život relativně neměnné. Papilární linie se vytváří od čtvrtého měsíce embryonálního života. Během života mění pouze svoji velikost. Jen u lidí s vysokým věkem jsou papilární linie občas ovlivněny vráskami stárnoucí kůže.
- Papilární linie jsou relativně neodstranitelné, pokud není odstraněna i zárodečná vrstva kůže. Běžné mechanické poškození na povrchu kůže sice má vliv na papilární linie, ale po zahojení kůže se papilární linie opět obnoví. Papilární linie lze odstranit drastickým zásahem do zárodečné vrstvy kůže. Člověk se sice zbaví papilárních linií, ale kvůli zásahu do kůže vzniknou specifické jizvy, které jsou opět pro každého člověka individuální.

2.3.2 Markanty

Markanty jsou drobné nepravidelnosti papilárních linií, které se svou četností, polohou a směrem vytváří jedinečný obraz papilárních linií. Existuje celkem 52 typů markantů, z toho celkem 7 typů využívá k rozpoznávání kriminalistika a pouze 2 typy využívá obor informačních technologií. Na obrázku (Obrázek 11) jsou tyto 2 typy markantů zobrazeny. Jedná se o markanty pojmenované jako začátek (konec) a vidlice.



Obrázek 11: Markanty [13]

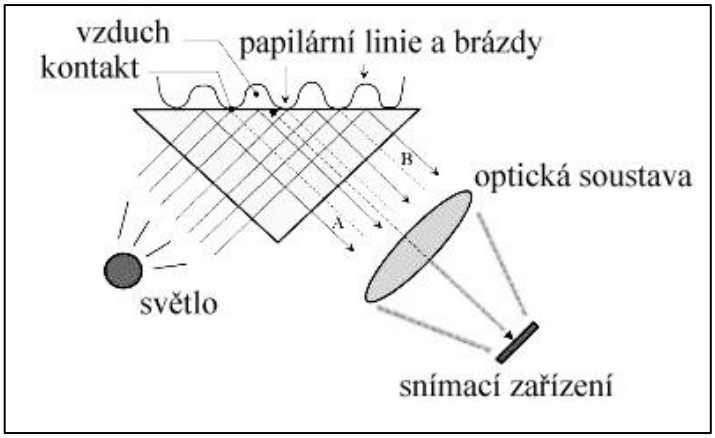
3 TYPY SNÍMAČŮ OTISKŮ PRSTU

3.1 Kontaktní snímače

3.1.1 Optický snímač

Optický snímač je vůbec nejstarší a dodnes nejpoužívanější technikou pro snímání otisku prstů. Princip spočívá na vlastnostech světla, které dopadá na předěl dvou látek.

Optický snímač obsahuje skleněnou, nebo plastovou průhlednou dotykovou plochu. Soustava LED diod emituje difuzní světlo, které dopadá na dotykovou plochu. V případě, že světlo dopadá na místo, kde se papilární linie dotýká dotykové plochy, dochází k rozptylu světla. V opačném případě, když světlo dopadá na místo, kde je brázda (vzdálenější místo od dotykové plochy), dochází k odrazu světla. Takové odrážené světlo je odráženo do optické čočky, která světlo usměrní na CCD, nebo CMOS senzor. Ve finálním obraze jsou tmavá místa, která znázorňují papilární linie a světlá místa, kterými jsou znázorněné brázdy.



Obrázek 12: Princip optického kontaktního snímače, (upraveno) [14]

Výhody:

- velmi vysoká kvalita obrazu,
- rychlost získání obrazu.

Nevýhody:

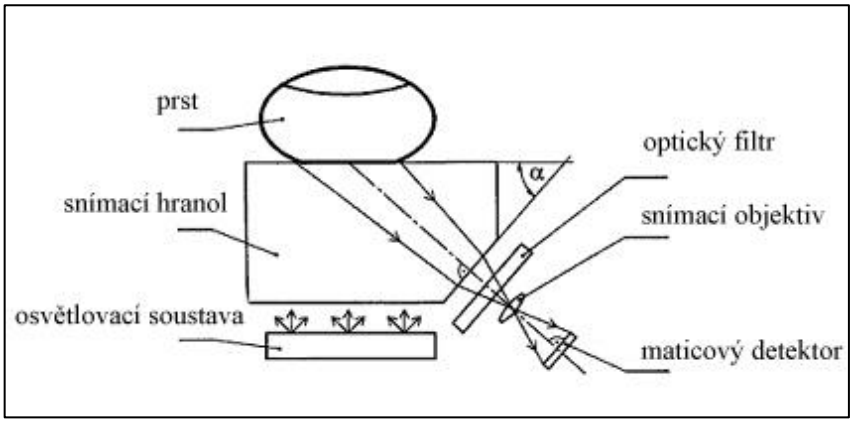
- malá odolnost vůči nečistotám,
- větší rozměry.

3.1.2 Opto-elektronický snímač

V dnešní době je technologie snímání pomocí opto-elektronického snímače otisků prstu považována za jednu z nejkvalitnějších. Technologie se neustále vyvíjí a má velmi dobrou perspektivu do budoucna.

Funguje na principu snímání odraženého světelného toku. Využívá se toho, že hloubka papilárních linií a brázd ovlivňuje množství odráženého světla. Světlo se odráží více od papilárních linií, než od brázd.

Opto-elektronický snímač se skládá ze dvou částí. V horní části je optický snímač, který obsahuje dotykovou plochu vyrobenou z polymeru TFT, je v kontaktu s prstem a má funkci emitovat světlo po přiložení prstu. TFT je průhledný film, obsahující miniaturní tranzistory, které umožňují přepínání jednotlivých pixelů mezi dvěma stavy (zapnuto a vypnuto). Další částí je maticový CCD nebo CMOS detektor, který zachytává světlo. Tvoří ho fotodiody, které jsou sestaveny v hustém poli. Fotodiody převádí světelný impuls na elektrický impuls. Po digitalizování obrazu otisku prstu je dále předán algoritmu, který obraz otisku prstu zpracuje.



Obrázek 13: Princip opto-elektronického snímače, (upraveno) [15]

Výhody:

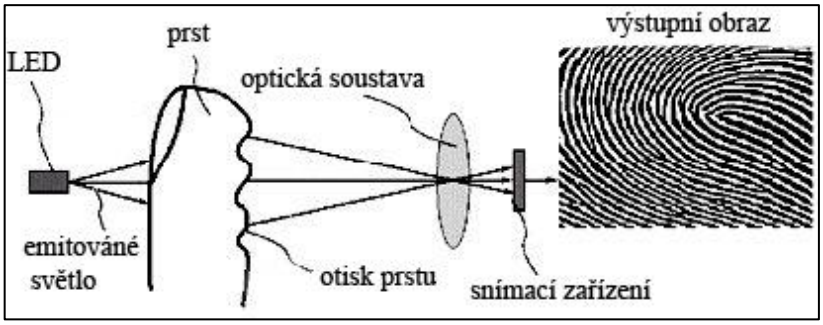
- vysoká kvalita snímání, velká snímací plocha a zároveň nízká pořizovací cena,
- odolnost proti vlhkosti a teplotním výkyvům – možnost venkovního použití.

Nevýhody:

- znečištěný prst může způsobit špatné vykreslení prstu,
- velké rozměry.

3.1.3 Transmisní optický snímač

Princip snímání spočívá v osvětlení prstu nejčastěji z infračervené LED diody. Prst je po přiložení na snímač osvětlen z vrchní strany. Světlo projde prstem do soustavy čoček, která světlo usměrní do snímacího zařízení. Snímací zařízení nejčastěji tvoří CCD nebo CMOS čip.



Obrázek 14: Princip transmisního snímače, (upraveno) [16]

Výhody:

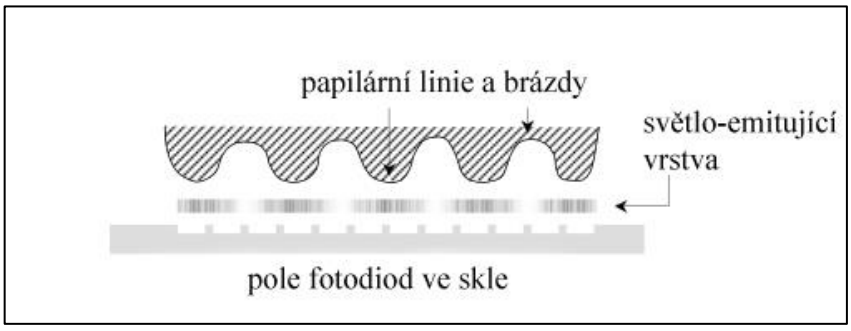
- nízká cena.

Nevýhody:

- nižší spolehlivost.

3.1.4 Elektroluminiscenční snímač

Jedna z nejnovějších technologií snímání. V horní části snímače se nachází snímací plocha, která se skládá z několika vrstev. Nejdůležitější z nich je světlo-emitující vrstva, která při styku s papilárními liniemi emituje světlo. Tímto vzniká světelný obraz, který definuje obraz papilárních linií. V dolní části se nachází husté pole fotodiod zatavené ve skle, které snímá světlo ze snímací plochy a vytváří z něj digitální obraz.



Obrázek 15: Princip elektroluminiscenčního snímače, (upraveno) [17]

Výhody:

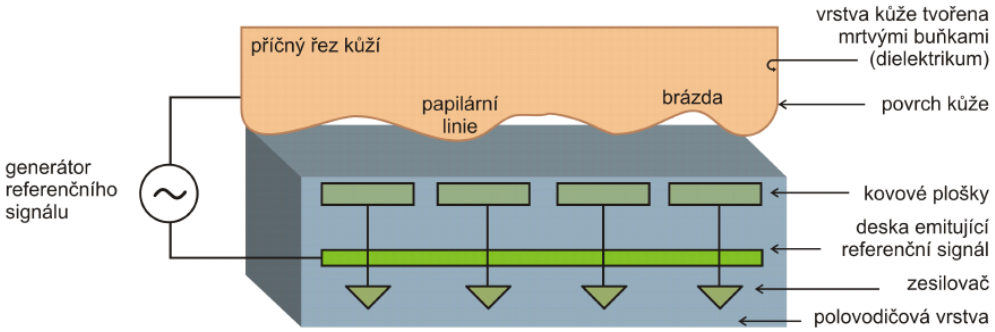
- vysoké rozlišení, miniaturní rozměry a nízká cena,
- vysoká kvalita obrazu, i když je prst suchý nebo vlhký.

Nevýhody:

- malá odolnost proti mechanickému poškození,
- citlivost na nečistoty.

3.1.5 Elektronický snímač

Elektronický snímač pracuje na principu vzniku elektrického pole. Snímač zahrnuje dvě paralelní desky, horní desku při snímání tvoří samotný prst a dolní desku tvoří dotyková plocha snímače. Elektrické pole je deformované horní deskou, tedy strukturou papilárních linií, do které je pouštěn řídící elektrický signál. Deformované elektrické pole se zachytí soustavou snímacích antén. Zachycený signál se upraví zesílením a transformuje se do elektronického obrazu.



Obrázek 16: Princip elektronického snímače [18]

Výhody:

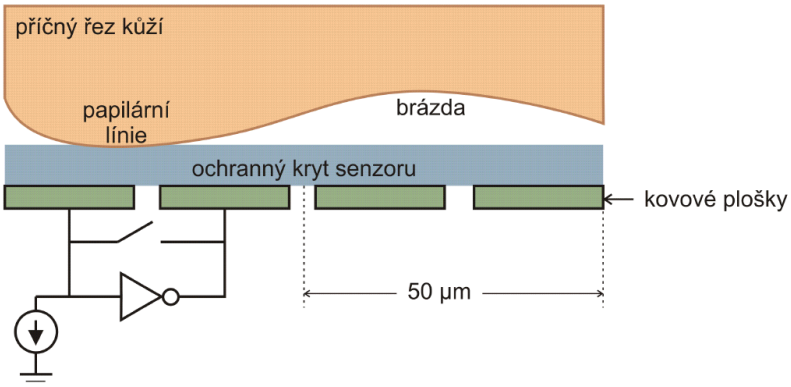
- rychlá a uživatelsky přívětivá metoda,
- odolnost proti nečistotám a vlhkosti prstu.

Nevýhody:

- málo rozšířené.

3.1.6 Kapacitní snímač

Kapacitní snímač funguje na principu měření kapacitního odporu na dotykové ploše. Jednu polovinu kondenzátoru tvoří dotyková plocha a druhou polovinu tvoří snímaný prst. Snímač se skládá z velkého množství (řádově 100 000) miniaturních, vodivých, od sebe odizolovaných plošek, na kterých je napařena vrstva nevodivého oxidu křemičitého. Papilární linie dotykem přemosťují jednotlivé plošky, jsou tedy přilehlejší k dotykové ploše a mají tak vyšší odpor, zatímco brázdy plní funkci izolantů. Mezi jednotlivými ploškami se měří kapacitní úbytky a napětí. Tímto způsobem vznikne digitalizovaný obraz papilárních linií. [19]



Obrázek 17: Princip kapacitního snímače [18]

Výhody:

- nízká cena a malé rozměry, proto jsou vhodné pro integraci do přenosných zařízení, jako jsou notebooky, apod.,
- při metodě snímání přejetím prstu po dotykové ploše odpadá možnost získání otisku prstu z dotykové plochy snímače.

Nevýhody:

- malá životnost snímačů,
- citlivost na nečistoty a vlhkost prstu, které ovlivňují vodivost.

3.1.7 Teplotní (termický) snímač

Teplotní snímače jsou vybaveny citlivým, miniaturním, teplo detekujícím čipem, pyrodetektorem. Pyrodetektor snímá rozdíl teplot mezi papilárními liniemi, které jsou v kontaktu s dotykovou plochou a brázdami, které mají větší vzdálenost od dotykové plochy. Snímání se provádí metodou sweeping, což znamená, že uživatel přejíždí prstem

po dotykové ploše snímače, která má v případě teplotních snímačů rozměry 0,4x14 mm. Výstupem snímače je obraz otisku prstů ve formě tzv. frames neboli digitálních pásů. Příslušný software musí výstup snímače zpracovat do finální podoby.

Výhody:

- malé rozměry a nízká cena,
- vyšší odolnost proti použití falzifikátu.

Nevýhody:

- velmi nízká kvalita výsledných obrazů,
- malá dotyková plocha snímá pouze část prstu, pokud je v databázi uložena jiná část prstu a oprávněný uživatel se prokazuje jinou částí prstu (např. pootočením prstu), tak nemůže být správně autentizován.

3.1.8 Tlakový (piezoelektrický) snímač

Tlakové snímače snímají různé tlakové působení papilárních linií a brázd. Papilární linie vyvolávají na dotykové ploše větší tlakové působení než brázdy. Povrch senzoru je tvořen elastickými, piezoelektrickými krystaly, které tlak převádí do elektrického signálu, z kterého se vytváří digitální obraz otisku prstu.

Výhody:

- malé rozměry a nízké provozní náklady,
- příliš suché, či vlhké prsty neovlivňují kvalitu obrazu.

Nevýhody:

- málo rozšířené.

3.1.9 Radiofrekvenční snímač

Princip radiofrekvenčního snímače je založen na vysílání radiofrekvenčního signálu. Funkčnost metody spočívá na dvou rovnoběžně umístěných deskách, na kterých je připojen generátor střídavého signálu. První desku tvoří dotyková plocha snímače a druhou desku tvoří otisk prstu. Signál prochází prstem a je formován papilárními liniemi prstu. Síla signálu závisí na vzdálenosti prstu od snímače, tedy platí, že papilární linie mají větší signál, naopak brázdy nižší. Pole aktivních antén signál přijme, dále je signál zesílen, integrován a digitalizován.

Výhody:

- běžné nečistoty a poškození prstu neovlivňují snímání.

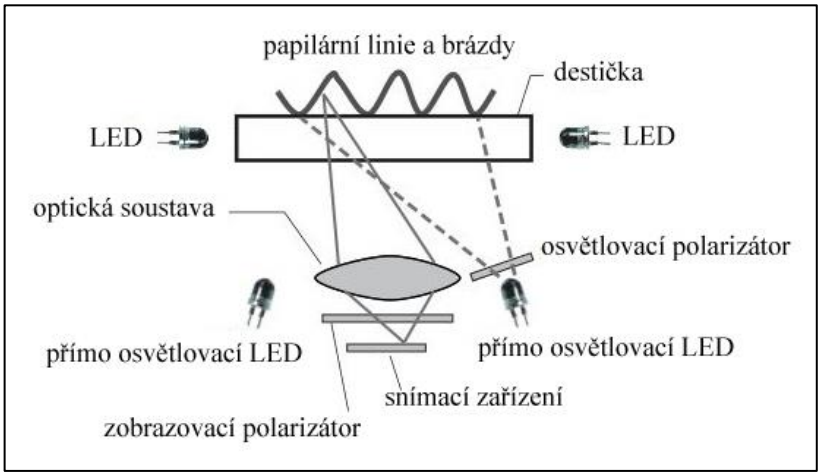
Nevýhody:

- delší doba autentizace – snímač může několikrát zopakovat postup, dokud nebude mít kvalitní obraz.

3.1.10 Multispektrální snímač

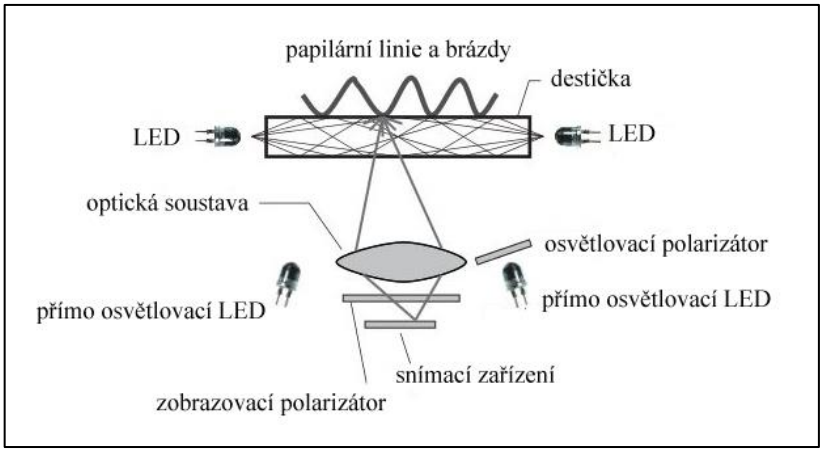
Multispektrální snímač je nová technologie pro snímání otisku prstů. Princip spočívá v použití více osvětlovacích soustav, které emitují světlo o různých vlnových délkách. Snímání probíhá ve dvou typech osvětlení, a to osvětlením s použitím polarizátoru a osvětlením bez polarizátoru.

První typ osvětlení spočívá v použití soustavy LED diod, které emitují světlo do osvětlovacího polarizátoru. Takhle lineárně polarizované světlo dopadá na dotykovou plochu snímače. Světlo je ovlivněno prstem a část světla je směřována do optické soustavy a zobrazovacího polarizátoru. Vzájemné umístění optické soustavy a polarizátorů má za důsledek zredukování vlivu světla odraženého od povrchu kůže a zdůraznění rozptýleného světla, které prošlo skrz kůži. [19]



Obrázek 18: Princip multispektrálního snímače s polarizátorem, (upraveno) [20]

Druhý typ osvětlení spočívá ve využití přímého náhodně polarizovaného osvětlení z LED diod. Odrážené světlo spolu se světlem, které prošlo skrz kůží, je schopno projít zobrazovacím polarizátorem a tvořit výsledný obraz. [19]



Obrázek 19: Princip multispektrálního snímače bez polarizátoru, (upraveno) [20]

Díky snímání s využitím světla o různých vlnových délkách, a tedy schopnosti snímat biometrické údaje pod povrchem kůže, se multispektrální snímač v porovnání s ostatními snímači považuje za velmi bezpečný prvek v oblasti biometrické autentizace.

Výhody:

- kvalitní obraz,
- odolnost proti znečištění a poranění prstu,
- odolnost proti falzifikátům,
- vhodný pro použití v extrémních podmínkách,
- schopnost dotvoření obrazu z důvodu slabého přitlačení prstu na dotykovou plochu nebo z důvodu nevýrazných papilárních linií.

Nevýhody:

- vysoká cena.

3.2 Bezkontaktní snímače

3.2.1 Optický snímač

Princip je podobný jako u kontaktního optického snímače otisku prstů. Prst je snímaný ve vzdálenosti 3 až 5 cm nejčastěji ze dvou zdrojů světla. Odrážené světlo prochází optikou, která světlo usměrní do snímacího prvku. Pokud vzdálenost musí být konstantní, z toho důvodu, že snímač neobsahuje automatické ostření, musí být snímač vybaven nápomocným zařízením, pomocí kterého je uživatel schopen udržet prst v konstantní vzdálenosti.

Výhody:

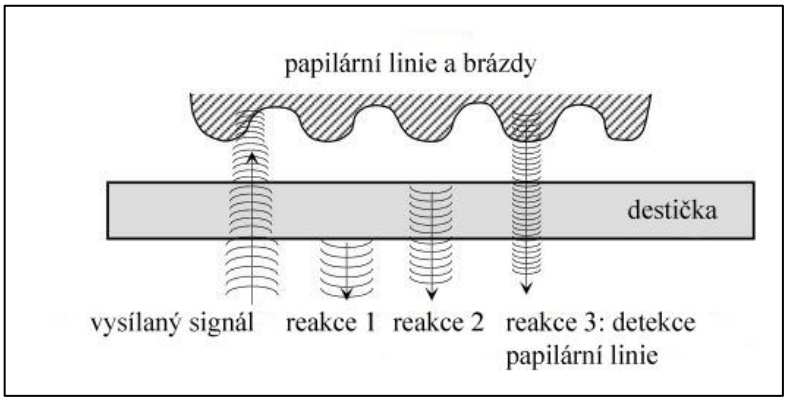
- vysoké rozlišení obrazu,
- bezkontaktní, hygienická metoda.

Nevýhody:

- nízký kontrast mezi papilárními liniemi a brázdami.

3.2.2 Ultrazvukový snímač

Principem ultrazvukového snímače je vysílání akustického signálu a následně jeho zachycení. Akustický signál má formu velmi krátkých impulsů s vysokou frekvencí (4 až 25 MHz). Vysílaný akustický signál naráží na spodní stranu prstu s papilárními liniemi. Papilární linie a brázdy modulují odražený akustický signál, z kterého se vyhodnotí výsledný obraz. Odražený akustický signál zachytává rotující hlava nebo hustá síť pevně, v rovině usazených čidel. Výsledný obraz je závislý na vyhodnocení funkční závislosti mezi vyslanými a odraženými zvukovými vlnami. Principiálně lze ultrazvukový snímač srovnávat se sonarem. Kvůli svým vlastnostem se ultrazvukový snímač využívá nejvíce v kriminalistice.



Obrázek 20: Princip ultrazvukového snímače, (upraveno) [21]

Výhody:

- vysoce kvalitní obraz,
- možnost snímání ze znečištěných, suchých, či vlhkých prstů

Nevýhody:

- vysoká cena,
- velké rozměry a dlouhá doba snímání.

II. PRAKTICKÁ ČÁST

4 V-PASS FX MV1610

Produkt V-Pass FX MV1610 je šablonovací snímač otisku prstů firmy Bioscrypt (nyní Morpho). Snímání prstu je založeno na kapacitní technologii. Snímač může být použit samostatně, nebo může být doplněn čtečkou karet.

Snímač pracuje ve dvou režimech:

- 1:N (identifikace) - přístup je povolen na základě přiloženého prstu,
- 1:1 (verifikace) – přístup je povolen po použití bezkontaktní karty a následného přiložení prstu na dotykovou plochu snímače.

Obrázek 21: Veri-Pass FX MV1610 [22]

Technické parametry snímače jsou uvedeny v tabulce (Tabulka 2).

Tabulka 2: Technické parametry V-Pass FX

Technický parametr	**Hodnota**
Rozměry v x š x h (mm)	130 x 50 x 64
Typ snímače	Kapacitní, šablonovací
Komunikační rozhraní	RS 232 RS 485 USB port Wiegand
Chybovost FAR – míra nesprávných přijetí	0,20 %
Chybovost FRR – míra nesprávných odmítnutí	1 %
Rychlost verifikace	<1 s
Rychlost identifikace	2–3 s
Kapacita paměti (v obrazech otisků prstů)	200 (1:N), 500 (1:1)
Velikost registračního otisku prstu	2488 b (1:N), 350 b (1:1)
Napájecí napětí	9–24 V DC (doporučeno 12 V DC)
Provozní teplota	0–60 ˚C
Softwarové vybavení	VeriAdmin

Kvůli kapacitě paměti snímače je snímač vhodný do malých až středně velkých objektů.

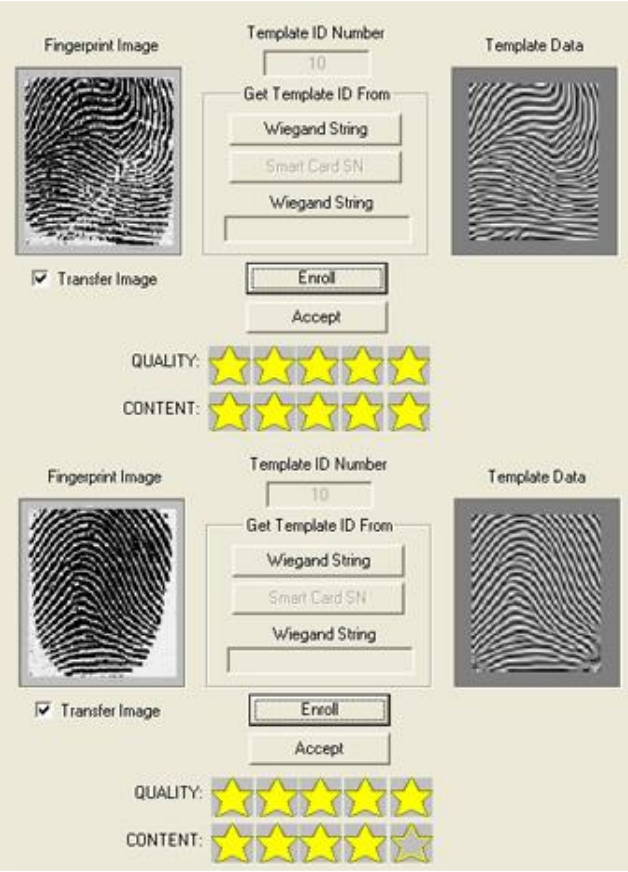
4.1 Testování funkčnosti

Pro testování funkčnosti jsem vybral několik situací, se kterými se může při autentizaci uživatel setkat. V následujících kapitolách uvádím výstupy snímače, a to jak otisk prstu (Fingerprint Image), tak jeho matematickou reprezentaci (Template Data) pro uložení do databáze. Snímal jsem pokaždé dva prsty (palec a ukazováček pravé ruky). Nejdříve jsem snímal palec, jeho matematická reprezentace a hodnocení kvalit jsou

uvedeny v horních částech obrázků v následujících testech. Dolní části obrázků se věnují ukazováčku.

4.1.1 Správné sejmutí otisku prstů

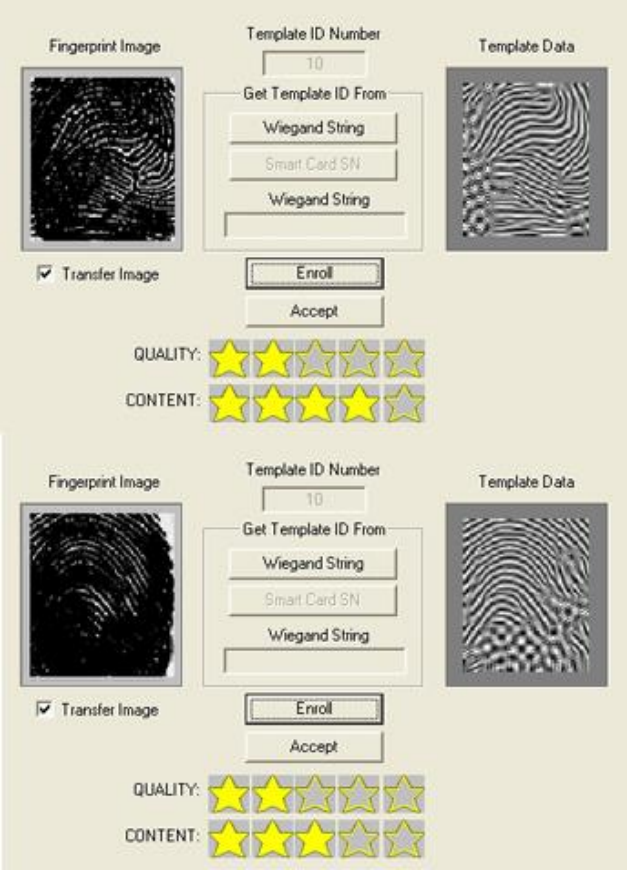
Nejdříve uvádím, jak takový obraz otisku prstů má vypadat. Prst jsem položil do středu na dotykovou plochu snímače. Během snímání jsem se snažil příliš s prstem nepohybovat. Nevyvíjel jsem prstem žádný přehnaný tlak.



Obrázek 22: Ukázka správně sejmutého prstu

4.1.2 Vlhký prst

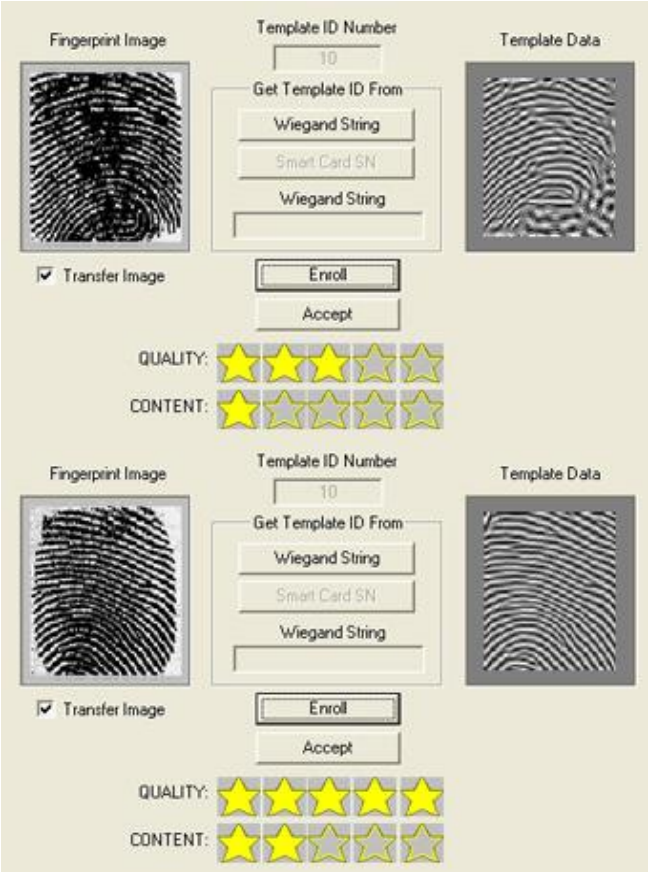
Je známo, že kapacitní snímače jsou velmi citlivé na vlhké prsty. Proto jsem do testování zahrnul nasimulování zpoceného prstu. Prst jsem namočil do vody a mírně utřel. Výsledek testu je znázorněn v následujícím obrázku (Obrázek 23).



Obrázek 23: Ukázka snímání vlhkého prstu

4.1.3 Znečištěný prst

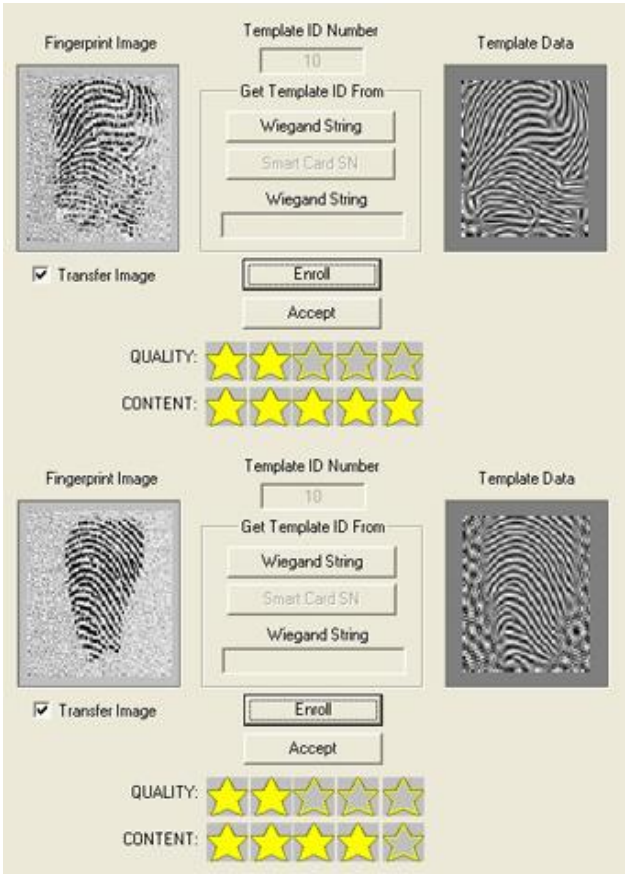
Většina snímačů otisku prstů má problémy se snímáním znečištěného prstu. Pro test bylo potřeba nějakým způsobem znečistit prst. Pro simulaci nečistot jsem zvolil tuhu tužky, kterou jsem nadrolil a následně prst znečistil. Výsledek výstupních snímků je uveden v dalším obrázku (Obrázek 24).



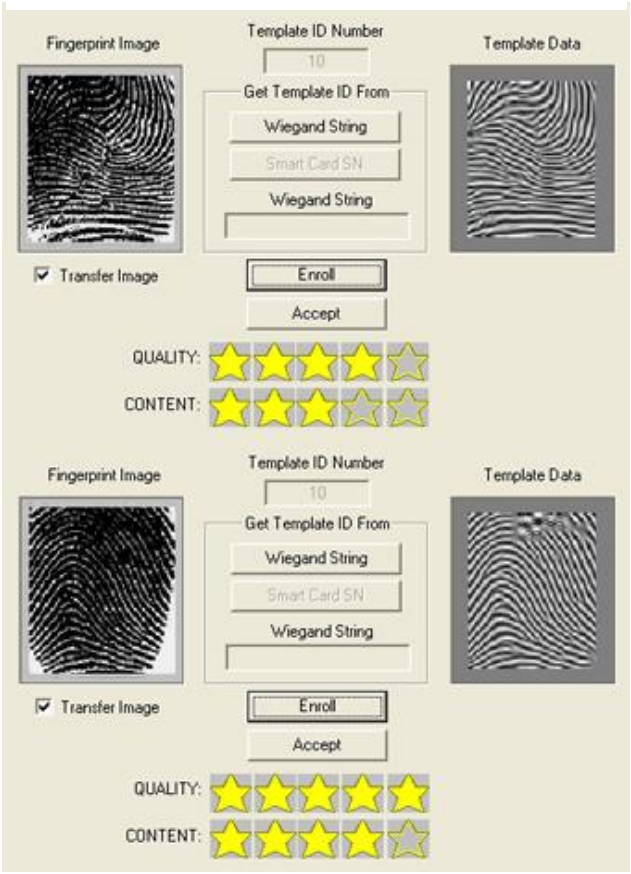
Obrázek 24: Ukázka snímání znečištěného prstu

4.1.4 Tlak prstu

Cílem testování bylo zjistit závislost kvality obrazů otisku prstů v souvislosti s vyvíjeným tlakem prstu na dotykovou plochu snímače. V testu jsem zkoumal, jak kvalitní vzorky je snímač schopen vytvořit, když budu vyvíjet prstem nejdříve velmi malý tlak a následně příliš vysoký tlak.



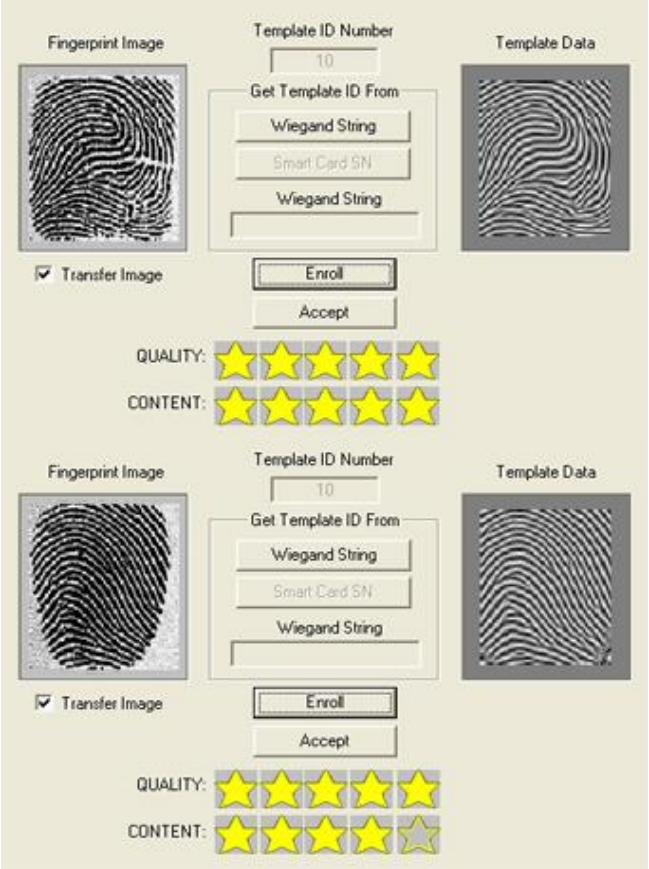
Obrázek 25: Ukázka snímání při malo vyvíjeném tlaku prstu



Obrázek 26 Ukázka snímání při silně vyvíjeném tlaku prstu

4.1.5 Snímání prstů s krémem na ruce

Cílem testu bylo zjistit, jestli nějak ovlivňuje snímání krém na ruce. Dalo by se předpokládat, že krém na ruce bude ovlivňovat prst zvýšenou vlhkostí a výsledek bude podobný, jako u testování snímání vlhkého prstu.



Obrázek 27: Ukázka snímání prstu s krémem na ruce

4.1.5.1 Zhodnocení výsledků testování

Kvalitní obraz je nutný především při registraci uživatele. Abychom docílili co nejkvalitnějšího registračního obrazu, je nutné, aby uživatel byl ochoten spolupracovat a byl obeznámen se správným postupem pro zachycení co nejkvalitnějšího obrazu otisku prstu. Kvalitní registrační obraz otisku prstu ovlivňuje míru chybovosti snímače při autentizaci uživatelů.

Správné umístění prstu. Obecně lze říct, že prst by měl být přiložen tak, aby snímač měl možnost sejmout co nejvíce charakteristických znaků prstu. Dotyková plocha

by měla být co nejvíce pokryta prstem. Uživatel by měl dbát i na to, aby měl prst vycentrován do středu dotykové plochy, pro zaznamenání jádra prstu a jeho okolí. Častou chybou při snímání je umístění prstu příliš ke kraji dotykové plochy, a tedy neumožnění snímání jádra prstu a jeho úplného okolí. Další chybou je pootočení prstu tak, že část prstu není v kontaktu s dotykovou plochou. Nesprávné umístění prstu má za důsledek získání nedostatečného počtu charakteristických prvků prstu. Takové obrazy prstu v databázi jsou příčinou zvýšené chybovosti autentizace.

Vlhkost prstu. Kvalitní obraz otisku prstu je podmíněn vlhkosti prstu, to obzvlášť platí u kapacitních snímačů otisku prstů. Optimální vlhkost prstu umožňuje kvalitní zachycení papilárních linií a brázd. Prst s vysokou vlhkostí je důvodem vzniku obrazu s nedostatečným rozlišením mezi papilárními liniemi a brázdami, a také sjednocení více charakteristických prvků prstu do jedné. Na obrázku (Obrázek 23) lze možné vysledovat, jak se papilární linie slévají a vytváří tmavé části v obrazu. Výsledný obraz otisku prstu měl nízké hodnocení v posuzování kvality snímku.

Nečistoty. Nečistoty negativně ovlivňují kvalitu obrazu otisku prstů. Nečistoty se dostávají do brázd a narušují vzor otisku prstu. Ze snímání lze konstatovat, že nečistoty negativně ovlivňují kvalitu snímku, převážně míru zastoupení markantů (hodnocení Content).

Tlak prstu. Tlak prstu na dotykovou plochu by měl být přiměřený. Příliš malý tlak může být příčinou sejmutí nedostatečného počtu markantů, což může být příčinou špatné autentizace. Test snímání prokázal, že snímači spíše více vadí nedostatečný tlak, než příliš velký. Nízký tlak převážně negativně ovlivňoval hodnocení kvality snímku.

Krém na ruce. Z výsledku testování snímání prstu, který byl potřený krémem na ruce, lze vyjádřit závěr, že neovlivňuje kvalitu snímku. Předpokládal jsem, že krém na ruce bude ovlivňovat vlhkost prstu. Výsledek testu můj předpoklad vyvrátil. Po snímání prstu se na dotykové ploše objevil mastný otisk prstu. Využil jsem situace a pokusil jsem se identifikovat. Na dotykovou plochu jsem dýchnul, abych simuloval teplotu pokožky. Pokus se nezdařil, snímač vůbec nereagoval. Druhý pokus spočíval v přiložení části těla, která neobsahuje papilární linie, chlupy a podobné prvky těla, které by narušily otisk. Zvolil jsem předloktí, abych simuloval teplo lidské pokožky. Vnitřní stranu předloktí jsem opatrně přiložil na dotykovou plochu. Vrstva krému, která zůstala na dotykové ploše, zanechala tvar papilárních linií a po přiložení předloktí se mi podařilo úspěšně

identifikovat do systému. Závěrem lze z výsledků testování konstatovat, že krém na ruce nijak neovlivňuje kvalitu obrazu otisku prstů, ale hrozí zde riziko zneužití pro identifikaci nebo získání otisku prstu z dotykové plochy snímače.

4.1.5.2 Metodika snímání

Z předchozích testů vyplývají základní pravidla pro sejmutí kvalitního obrazu otisku prstu.

- Prst musí být umístěný na střed snímače a po celou dobu snímání být ve stabilní poloze. Pro správné umístění slouží zarážka na snímači, kde má být položen kloub posledního článku prstu.
- Vlhkost prstu musí být přirozená. Příliš vlhké, nebo suché prsty znemožňují vytvoření kvalitního obrazu.
- Pro kvalitní snímání je nutné odstranit nečistoty z prstu, ale i z dotykové plochy snímače.
- Tlak vyvíjený prstem na dotykovou plochu musí být přiměřený.
- Po použití snímače je vhodné setřít latentní otisk z dotykové plochy snímače. Setřením se zabrání zneužití osobního citlivého údaje.

5 SOFTWARE VERIADMIN

VeriAdmin je software dodávaný pro snímače otisku prstu řady VeriSeries. Software se využívá pro správu snímače, popřípadě snímačů v síti. Je vhodný pro registraci nových uživatelů a správu jejich registračních obrazů otisku prstů. Umožňuje konfiguraci snímače a aktualizaci firmwaru.

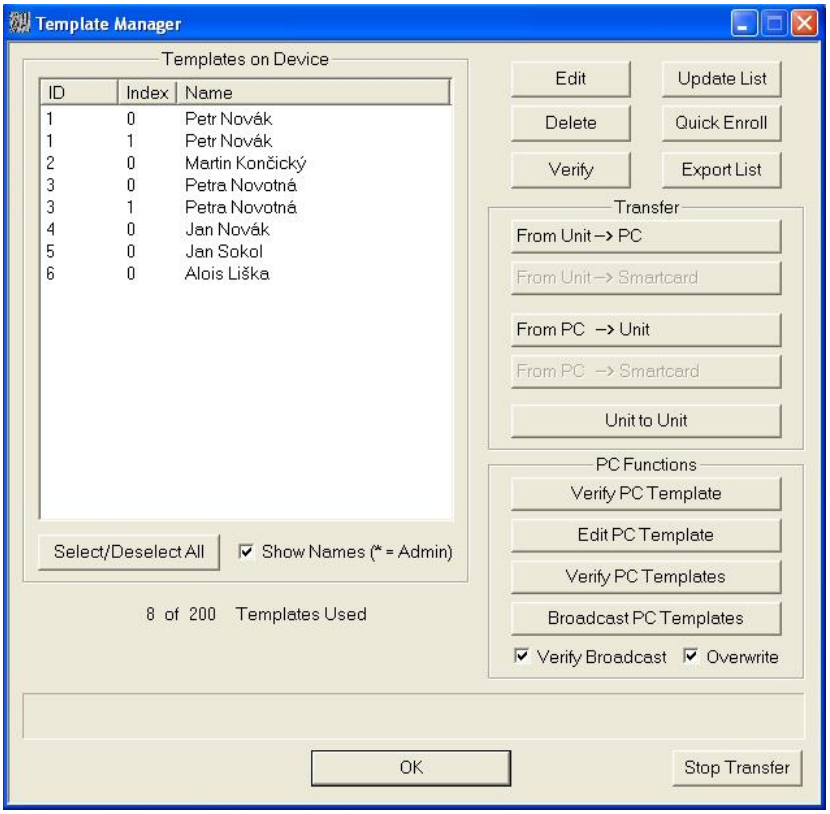
Systémové požadavky VeriAdminu jsou následující:

- operační systém minimálně Windows 2000,
- minimálně 30 MB volného místa na disku,
- minimálně 16 MB RAM,
- CD-ROM mechanika,
- USB port nebo sériový port,
- konvertor RS-232 na RS-485.

5.1 Funkce

5.1.1 Template manager

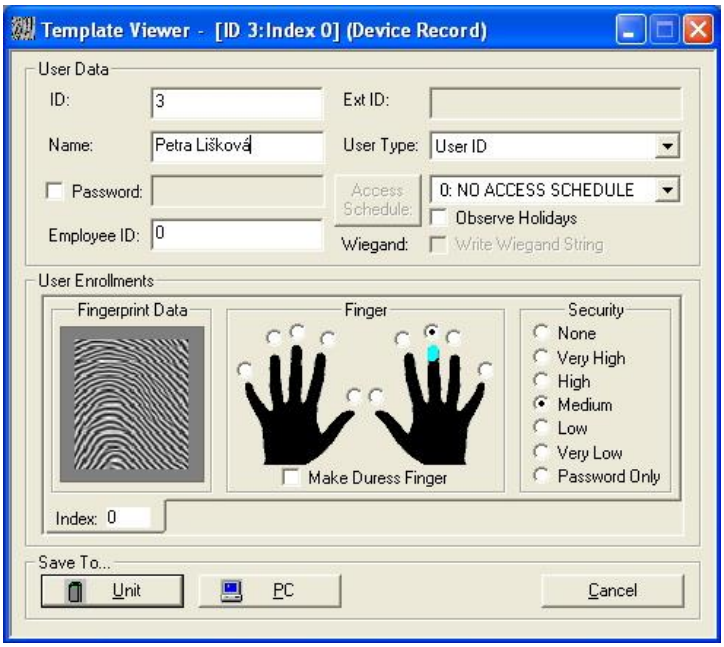
Template manager je nástroj pro správu registračních obrazů otisku prstů uživatelů. Zobrazuje identifikační údaje pro jednotlivé obrazce otisku prstů, jako je ID, Index a jméno uživatele. Pomocí nástroje lze přidávat, editovat a mazat obrazce, exportovat databázi do PC, přeposílat obrazce otisku prstů po síti do ostatních čteček nebo PC, atd. Nástroj také obsahuje funkci verifikace, kdy po vybrání registrovaného obrazce z databáze, podle kterého chceme verifikovat a přiložení prstu na snímač, dostaneme zprávu o porovnání obrazců. Pokud je verifikace úspěšná, tedy obrazce jsou totožné, výstupem je tzv. skóre (Score), které určuje stupeň shody dvou porovnávaných obrazců otisku prstů. Skóre může mít maximální hodnotu 100, což znamená, že obrazce jsou 100% shodné. Takovou vysokou hodnotu skóre ovšem nikdy nebude možné získat.



Obrázek 28: Template Manager

5.1.1.1 Template Viewer

Template Viewer zprostředkovává editaci existujícího obrazu otisku prstu. Dialogové okno lze vyvolat dvěma způsoby. Buď vybráním určitého obrazu otisku prstu a použití funkce Edit, nebo dvojklikem na obraz otisku prstu v databázi. Můžeme měnit parametry obrazu otisku prstu, jako je jeho ID, jméno uživatele, ID uživatele, typ uživatele, stupeň zabezpečení, atd. Změny lze uložit do počítače nebo do snímače.



Obrázek 29: Template Viewer

5.1.2 Command Card Manager

Command Card Manager je nástroj pro přidávání a odebírání uživatelů ze snímače bez nutnosti přístupu k VeriAdminu. Přístup se edituje pomocí předem definovaných čipových karet. Nástroj je využitelný v případě, kdy potřebujeme uživateli přidělit dočasný přístup a počítač s VeriAdminem je momentálně nedostupný. Command Card Manager lze samozřejmě využít jen tehdy, pokud snímač otisku prstů spolupracuje se čtečkou čipových karet.

5.1.3 Network Configuration Manager

Network Configuration Manager je primární nástroj pro konfiguraci sítě. Nástroj umožňuje přidávání a odebírání zařízení ze sítě, definování komunikačních portů, které bude VeriAdmin používat (Network Setup), skenování sítě a zjišťování funkčnosti obsažených zařízení (Network Status), otestování komunikace na určitém komunikačním portu (Test Communications). Levá část dialogového okna uvádí stromovou strukturu vytvořené sítě. Po vybrání určitého zařízení ze stromové struktury sítě, se pravá část dialogového okna věnuje informacím právě vybraného prvku sítě. Uvádí se identifikační ID prvku, typ zařízení, jméno zařízení, verze firmwaru a indikace momentálního stavu zařízení.

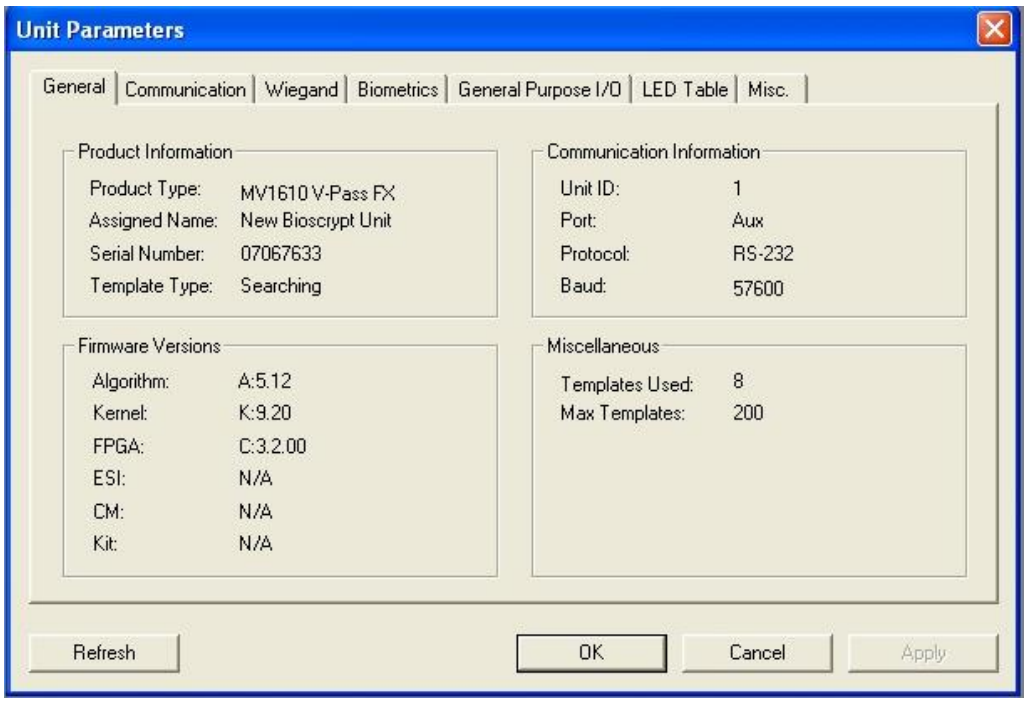
5.1.4 Unit Parameters

Unit Parameters slouží k nastavení snímače otisku prstů. Dialogové okno obsahuje následující záložky:

- General – obsahuje informace o určitém zařízení v síti. Informuje nás o základních informacích o zařízení (Product Information), jako je typ zařízení, jméno zařízení, sériové číslo a typ obrazců otisku prstů. Dále lze vyčíst informace o komunikaci, jako je typ komunikačního portu, komunikační protokol atd. (Communication information) a informace o používaném firmwaru (Firmware Versions). Poslední část dialogového okna se věnuje ostatním informacím (Miscellaneous), a to počet uložených obrazců otisku prstů a jejich maximální počet, který lze uložit do databáze.
- Communication – umožňuje nastavit komunikační parametry zařízení. Lze přiřadit ID číslo, pod kterým bude zařízení v síti jednoznačně identifikované (Network Identification Number) a definovat komunikační rozhraní

(VeriSeries Port Mode). Obsahuje funkci Aux Port Security, která umožňuje zabezpečení komunikačního portu. Je výrobcem doporučováno, aby komunikace Aux Port byla vypnuta a chráněna heslem. Zabrání se tím neoprávněnému vniknutí do zařízení. Aby bylo možné se zařízením pracovat je nutné, aby funkce Aux Port Security byla zapnuta a bylo zadané správné heslo.

- Wiegand – umožňuje nastavit parametry Wiegand efektu pro identifikační karty. Wiegand je rozhraní, pomocí kterého komunikují čtečky bezkontaktních karet.
- Biometrics – umožňuje nastavení biometrické autentizace. Lze nastavit globální bezpečnostní úroveň pro verifikaci (Global Security Threshold). Je možné vypnout respektive zapnout biometrickou autentizaci (Biometric Verification) a automatickou detekci prstu na dotykové ploše (Auto Finger Detect). Lze nastavit chování zařízení v situaci, kdy je biometrická verifikace ignorována (Security Level NONE Options) a to tak, že zařízení požaduje detekování prstu na dotykové ploše, nebo nepožaduje. Pro větší bezpečnost je umožněno nastavit vyžádání přiložení více prstů pro úspěšnou autentizaci (Multi-User Verification).
- General Purpose I/O – je vhodný ke konfiguraci vstupních a výstupních TTL linek.
- LED Table – slouží k definování chování LED a zvukové signalizace vzhledem k provedení určité operace. U LED je možnost nastavení doby a frekvence signalizace.
- Miscellaneous – obsahuje volby odesílání výsledků verifikace po komunikačním rozhraní.



Obrázek 30: Unit Parameters

5.1.5 Quick Enroll

Nástroj Quick Enroll, jak už název napovídá, slouží k rychlému registrování nového uživatele. Quick Enroll umožňuje vytvoření pouze jednoho obrazu otisku prstu. Pokud se proces snímání nezdaří a obraz není kvalitní, Quick Enroll umožňuje proces snímání neustále opakovat pro získání nejvhodnějšího obrazu otisku prstu. V dialogovém okně se zobrazuje reálný obraz otisku prstu (Fingerprint Image) a matematickou reprezentaci (Template Data), která se ukládá do databáze. Funkce pouze vyžaduje zadání ID číslo obrazu otisku prstu.

5.1.6 Advanced Enroll

Advanced Enroll je další nástroj pro registraci uživatele. Tento nástroj je výrobcem doporučován pro snímání všech otisků prstů. Jeho pomocí je možné zaregistrovat až tři odlišné otisky prstu, nebo pouze jeden. Pokud registrujeme pouze jeden prst, tak VeriAdmin ze tří snímání doporučí ten, který má nejlepší hodnocení, a tedy je ze všech nejvhodnější pro uložení do databáze. Funkce stejně jako Quick Enroll vyžaduje zadání ID číslo obrazu otisku prstu. Navíc umožňuje zadání čísla (Index), které rozlišuje obrazy otisku prstů jednoho uživatele.

5.1.6.1 Hodnocení kvality obrazů otisku prstů

Hodnocení obrazů otisků prstů se provádí u obou dvou registračních funkcí VeriAdminu. Kvalita obrazů otisků prstů je znázorněna grafickou stupnicí formou hvězdiček. Platí, že žádná hvězdička je nejhorší ohodnocení a pět hvězdiček značí nejlepší možnou kvalitu. Hodnocení probíhá ve dvou ohledech.

- Quality – posuzuje se kvalita obrazu otisku prstu. Kvalitu může ovlivnit vlhkost prstu nebo znečištění. Výrobce doporučuje, aby obraz otisku prstu byl ohodnocen minimálně třemi hvězdičkami.
- Content – posuzuje se míra zastoupení charakteristických znaků prstu. Počet charakteristických znaků může ovlivnit nesprávné umístění prstu na dotykové ploše. Výrobce doporučuje, aby obraz otisku prstu byl ohodnocen minimálně třemi hvězdičkami.

Je výhodné, aby obě funkce posuzování kvality měly co největší hodnocení. Kvalitní registrační obrazce otisku prstů značně snižují pravděpodobnost nesprávného odmítnutí při autentizaci.

5.2 Návrh dalších funkcí

Software VeriAdmin je dostačující pro základní správu se snímačem. Administrátorovi ovšem nějaké funkce mohou chybět. Ve zbylé části kapitoly uvádím funkce, o které by mohl být software obohacen.

- Doba přístupu – funkce by umožňovala nastavovat dobu, kdy může snímač uživatele úspěšně autentizovat. Uživatel by měl možnost vstupu pouze v definovanou dobu administrátorem. Přístupová doba by byla definována časem, datem a dny v týdnu. Doplňkovým nástrojem by mohl být kalendář, kde by měl administrátor možnost rychle ručně zadat dobu přístupu, např. pro uživatele s požadavkem na nepravidelnou návštěvu.
- Historie autentizace – administrátor by měl možnost zjistit historii autentizace. Do databáze by se ukládaly informace, kdo a kdy byl úspěšně autentizován.
- Informace o uživatelovi – do databáze by se mohly ukládat více informací, než umožňuje VeriAdmin. Vedle jména bych uvítal informace, jako jsou

např. kontaktní údaje (e-mail, telefonní číslo do kanceláře), číslo kanceláře nebo pracovní pozice. Nástroj by umožňoval i přidání fotky uživatele.

- Přihlášení administrátorů – nástroj pro přihlášení administrátorů by mohl sloužit jako prevence proti zneužití systému administrátorem na pozici např. nespokojeného zaměstnance. Po spuštění VeriAdminu by administrátor musel zadat svoje přihlašovací jméno a heslo. Do databáze by se ukládaly informace, který z administrátorů se přihlásil a jaké udělal změny v databázi otisků prstů nebo v nastavení systému. Přístup do databáze by byl zabezpečen např. heslem, které by znal pouze jeden z administrátorů. Tato funkce by umožňovala zjistit, který z administrátorů zneužil svých privilegií, sabotoval systém, atd.

6 LABORATORNÍ ÚLOHA

Laboratorní úloha je stavěna na vyzkoušení snímače Veri-Pass FX MV1610 a dodávaného softwaru VeriAdminu. Snímač je již nainstalován na škole v laboratoři 54/309.

6.1 Návrh laboratorní úlohy

Teoretická část:

1) Uveďte příklady metod biometrické autentizace.
2) Vysvětlete pojmy verifikace a identifikace.
3) Uveďte, na jakých principech fungují snímače otisku prstů.
4) Vysvětlete princip kapacitního snímače otisku prstů.

Praktická část:

5) Vytvořte alespoň 9 obrazů otisku prstů. Napište postup jejich vytvoření.
6) U registrovaného obrazu otisku prstu změňte jméno vlastníka. Uveďte, jak jste postupoval.
7) Vyzkoušejte funkci verifikace pro 5 prstů minimálně 5x. Zaznamenejte úspěšnost a výsledné skóre do tabulky.
8) Vyzkoušejte se identifikovat alespoň 30 pokusy. Napište jaký je postup a Vaše úspěšnost identifikace. Jak snímač reaguje na úspěšnou a neúspěšnou identifikaci?
9) Pomocí VeriAdminu zjistěte kolik obrazů otisku prstů je uloženo v databázi a kolik jich může maximálně být.

6.2 Vypracování laboratorní úlohy

1) Mezi metody biometrické autentizace patří snímání otisku prstů, snímání oční sítnice a duhovky, autentizace na základě geometrie ruky a žilního řečiště ruky, snímání tvaru ucha, tváře, struktury nehtu. Další metody se zabývají hlasem, dynamikou podpisu, dynamikou stisknutí kláves a pohybu myší, tvarem a pohybem rtů, dynamikou úsměvu, chůzí, pachem, DNA, atd.

2) Identifikace znamená zjištění a stanovení totožnosti na základě stejných charakteristik.

   Verifikace znamená ověření pravdivosti výroku, argumentu, apod.

3) Existuje několik typů snímačů otisku prstů, jako je optický, kapacitní, teplotní, opto-elektronický, elektroluminiscenční, elektronický, ultrazvukový, multispektrální, radiofrekvenční, tlakový a transmisní.

4) Kapacitní snímač otisku prstů vytváří obrazy otisku prstů na základě měření kapacitního odporu. Využívá se toho, že papilární linie jsou přilehlejší k dotykové ploše, a tedy mají vyšší kapacitní odpor. Naopak brázdy jsou od dotykové plochy vzdálenější a mají nižší kapacitní odpor.

5) K vytvoření registračních otisků prstů jsem použil nástroj Quick Enroll. Nástroj lze vyvolat z horního panelu VeriAdminu, kde je zastoupen ikonou. Popřípadě je umístěn v záložce Configure. Před snímáním je nutné zadat ID obrazu otisku prstu, poté stačí vybrat možnost Enroll a položit prst na dotykovou plochu snímače. Pro uložení obrazu do databáze je nutné vybrat možnost Accept. Objeví se dialogové okno, kde lze obraz otisku prstu editovat, jako např. přidat jméno majitele. Tento postup jsem opakoval ještě celkem osmkrát.

6) Editaci obrazu otisku prstu lze provést v dialogovém okně s názvem Template Manager. Nástroj je umístěný v záložce File nebo ho lze vyvolat i pomocí ikony na horním panelu softwaru. V levé části jsem vybral obraz otisku prstu, u kterého chci změnit jméno majitele a vybral jsem možnost Edit. Otevřelo se dialogové okno s vlastnostmi obrazu otisku prstu, kde lze i změnit jméno vlastníka.

7) Verifikaci si lze vyzkoušet v již zmiňovaném dialogovém okně Template Manager. Po vybrání obrazu otisku prstu, podle kterého se chci verifikovat, jsem vybral funkci Verify. Výsledky verifikací jsou uvedeny v tabulce (Tabulka 3).

Tabulka 3: Výsledky skóre při verifikaci

Číslo pokusu / prst	**Palec pravé ruky**	**Ukazovák levé ruky**	**Malíček levé ruky**	**Prsteníček pravé ruky**	**Prostředníček levé ruky**
1	78	74	69	70	72
2	81	79	71	69	74
3	81	79	68	75	72
4	82	76	69	76	73
5	75	75	68	71	74

Úspěšnost byla 100%, po každé se mi podařilo verifikovat. Skóre závisí na kvalitě registračního obrazu otisku prstu a správného sejmutí verifikovaného prstu. Nejvyšší skóre měli palec a ukazováček. Nejspíš proto, že je použití těchto prstů pro snímání nejpohodlnější.

8) Identifikace je možná jen v případě, kdy je v nastavení zapnuta funkce Auto Finger Detect. Nastavení zařízení (Unit Parameters) je umístěno v záložce Configure, nebo ho lze vyvolat ikonou z horního panelu VeriAdminu. Funkci automatické detekce prstu (Auto Detect Finger) je možné zapnout v záložce Biometrics kliknutím na možnost Enabled. Nyní je možné vyzkoušet identifikaci. Po přiložení prstu na dotykovou plochu a úspěšné identifikace, snímač reaguje akustickým signálem a zeleným rozsvícením LED. V klidovém režimu je LED oranžová. Pokud je identifikace neúspěšná, tak se LED rozsvítí červeně. Během snímání různých otisků prstů jich bylo všech 30 úspěšně identifikováno.

9) Informace o snímači je možné vyčíst pomocí nástroje Unit Parameters. Konkrétně kolik obrazů otisků prstů je uloženo a jejich maximální možný počet, je uveden hned v první v záložce General. Používaných obrazů otisků prstů je 10, maximální množství je 200.

6.3 Přínos laboratorní úlohy

Laboratorní úloha poskytuje pro řešitele možnost se seznámit se správou snímače otisků prstů na pozici administrátora. Laboratorní úloha může sloužit pro studenty oboru BTSM v rámci výuky elektronické kontroly vstupu na základě biometrie.

V teoretické části se řešitelé obeznámí s pojmy identifikace a verifikace, s metodami biometrické autentizace, s typy snímačů otisků prstů a s principem kapacitního snímače otisku prstů.

V praktické části si řešitelé vyzkouší práci s databází obrazů otisků prstů a jejich editací, seznámí se s rozhraním VeriAdminu. Po vytvoření registračních obrazů otisků prstů si následně vyzkouší identifikaci a verifikaci.

7 ODHAD VÝVOJE

Lidstvo neustále zkoumá a vyvíjí další technologie, které napomáhají k vzestupu biometrické identifikace. Díky neustálému vývoji se snímače otisku prstů stávají kvalitnějšími, odolnějšími a uživatelsky přijatelnějšími zařízeními. Díky tomu budou snímače otisku prstů přístupnější pro společnost.

Snímání otisku prstů je jednou z metod autentizace. Člověk se potřebuje autentizovat téměř denně. Snímače otisku prstů se často používají v kancelářích, skladech, nemocnicích, v objektech s nebezpečnými látkami, na úřadech, apod. Začínají se využívat i v soukromých firmách a domácnostech. Proto význam snímání otisku prstů neustále roste.

Dalším faktorem přispívající k vývoji snímačů otisků prstů je neustále rostoucí kriminalita. Policie a další orgány jsou velmi zainteresovány do co nejkvalitnější identifikace.

V dnešní době se zkoumá integrace snímačů otisku prstů do různých zařízení. Ve zbrojním odvětví se vyvíjí začlenění snímačů otisku prstů do zbraní (tzv. Smart Guns). Cílem je zabránit zneužití zbraně nepřítelem nebo po jejím odcizení. Automobilový průmysl také integruje snímače otisků prstů do svých produktů. Aby majitel auta mohl vůbec nastartovat, tak musí přiložit svůj prst. Důvod je stejný jako u zbrojního průmyslu, zabránění zneužití věci. Osobní doklady také nezůstávají pozadu. Dnešní cestovní pasy obsahují otisk prstu majitele. Otisk prstu není v cestovním pase nikde viditelný, je uložen na čipu uvnitř cestovního pasu.

Využití snímačů otisků prstů by měl smysl i ve finančním odvětví. Například při vybírání peněz z bankomatů nebo během placení platební kartou. Bezpečnostní význam by měl i u mobilních telefonů. Při zapínání nebo odblokování mobilního telefonu by musel majitel položit prst na snímač. Díky tomu by nemohl neoprávněný uživatel s telefonem pracovat a získávat osobní údaje.

ZÁVĚR

Biometrické vlastnosti částí lidského těla se staly předmětem jednoznačné autentizace uživatele. Kvůli neustálému vývoji se stanou biometrické systémy levnějšími a pro společnost dostupnějšími. Tento fakt začínáme pozorovat u notebooků, do kterých se velmi často integrují snímače otisků prstů pro ověření uživatele. Protože jsou snímače otisku prstů bezpečné, levné, pohodlné a uživatelsky přijatelné lze předpokládat, že se snímače otisku prstů začnou ve značné míře integrovat do dalších zařízení, jako je např. mobilní telefon, automobil, apod. nebo vytlačí z kontroly vstupu používání identifikačních karet, hesel, atd.

Prvním úkolem bakalářské práce bylo zpracovat literární rešerši zaměřenou na biometrické metody autentizace a biometrickou terminologii. V této kapitole jsou vysvětleny základní biometrické termíny a vypsány nejčastěji používané biometrické technologie. Pro lepší přehlednost jsou biometrické metody rozdělené do dvou skupin s ohledem na to, která z biometrických vlastností je předmětem jejich snímání. Dalším úkolem teoretické části bylo popsat vlastnosti lidské pokožky. Strukturou kůže a jejími vlastnostmi se zabývá druhá kapitola teoretické části. V kapitole jsou také zmíněny informace o papilárních liniích a markantech. Poslední část teoretické části se zaobírá jednotlivými typy snímačů otisků prstů. Je kladen důraz především na vysvětlení principů snímání u každého snímače otisků prstů.

Jedním z cílů praktické části bylo ověřit funkčnost snímače otisků prstů. Ke splnění úkolu byl použit kapacitní snímač V-Pass FX MV1610, který je instalován ve školní laboratoři. Čtvrtá kapitola popisuje, jakým způsobem byla testována funkčnost snímače. Testování bylo prováděno v situacích, se kterými se může uživatel běžně setkat. Na základě výsledků testů byla vytvořena metodika snímání. Další část praktické části se zabývá analýzou softwaru. V této části jsou popsány funkce softwaru a návrh doplnění dalších funkcí. Dalším cílem praktické časti, bylo vytvoření laboratorní úlohy. Laboratorní úloha je postavena na základě získaných poznatků z předchozích dvou kapitol. Poslední kapitola se zabývá odhadem pravděpodobného vývoje snímačů otisků prstů.

ZÁVĚR V ANGLIČTINĚ

Biometric properties of the human body are widely used as unique instrument for user authentication. Thanks to incessant development in this area, biometric systems will be cheaper and also more accessible for the society during the time. Nowadays, fingerprints scanners are mostly used as user identification authenticates protocol for notebooks. Security, cheapness, comfort and user acceptability are a prerequisite for expansion of scanners into another devices and processes, e.g. mobile phones, cars, ID cards and passwords.

In a first part of the presented work, review of the current state of the art about authetication biometric methods is presented. Basic terms used in this technical area are explained, and most widely used biometric technologies are described. Biometric methods are divided into two groups by property, which is main object of the scanning. Properties of the human skin are described in second chapter of this work. There can be found information about ridges and minutiae also. Last theoretical part is dealing with types of the fingerprints scanners. Principle of the scanning is explained for each of the mentioned scanner type.

Function verification of the capacity sensor V-Pass FX MV1610 was one of the bachelor's thesis aims. Testing of the sensor functions is described in chapter four, and it was performed under common user situations. Based on the test results, scanning procedure was created. Software analysis was performed in next part of work. Existing functions of the software are described, and a few new useful functions are proposed for further possible addition. Creation of the laboratory task was last part of the presented work. This task was completed based on the knowledge learned in previous parts of the work. Estimation of the further fingerprint scanners development is discussed in the last chapter of the bachelor`s thesis.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[2] AFCEA/ USNI West 2009 Convention. *Running the Bases with Powayslugger* [online]. 11.3.2009 [cit. 2013-03-28]. Dostupné z: http://powayslugger77.blogspot.cz/2009/02/afcea-usni-west-2009-convention.html

[3] Bunker Archaeology. *SportsBabel* [online]. 5.4.2012 [cit. 2013-04-10]. Dostupné z: http://www.sportsbabel.net/2012/04/bunker-archaeology.htm

[4] Facial Analysis. *University of Surrey* [online]. [23.7.2012] [cit. 2013-04-10]. Dostupné z: http://www.surrey.ac.uk/cvssp/research/facial_analysis/index.htm

[5] Thermal Infrared Face Recognition – a Biometric Identification Technique for Robust Security System. *Intech* [online]. © 2004–2013 [cit. 2013-04-10]. Dostupné z: http://www.intechopen.com/books/reviews-refinements-and-new-ideas-in-face-recognition/thermal-infrared-face-recognition-a-biometric-identification-technique-for-robust-security-system

[6] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

[7] Just Ear Us Out… Give These Unique Forms of Biometrics a Chance!. *Ievo* [online]. 31.3.2012 [cit. 2013-04-10]. Dostupné z: http://www.ievoreader.com/blog/archives/611

[8] FAQ - Hand Geometry. *360 biometrics* [online]. © 2011 [cit. 2013-04-12]. Dostupné z: http://360biometrics.com/faq/Hand-Geometry-Biometrics.php

[9] Vein pattern palm reading by Fujitsu!. *360 biometrics* [online]. 20.8.2008 [cit. 2013-04-12]. Dostupné z: http://www.fujitsu.com/th/en/news/archives/2008/news_fujitsu_palm_08en.html

[10] Hypro-Flex. *Hypro* [online]. © 2010 [cit. 2013-04-16]. Dostupné z: http://www.hypro.cz/hyRubrIn.aspx?intRubrKis=1263&intLang=0

[21] Classification. *Staples High School* [online]. © 2013 [cit. 2013-04-16]. Dostupné z: http://shs.westport.k12.ct.us/forensics/04-fingerprints/classification.htm

[12] LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.

[13] Obrazce a znaky kůže. *Krimi* [online]. [2012] [cit. 2013-04-18]. Dostupné z: http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

[14] FINGERPRINT RECOGNITION ROBOT. *Roboticsclub_fingerprint* [online]. 26.6.2012 [cit. 2013-04-18]. Dostupné z: http://students.iitk.ac.in/projects/roboticsclub/fingerprint

[15] Optoelektronické snímače otisků prstů. *Z.L.D s.r.o.* [online]. © 2003 [cit. 2013-04-18]. Dostupné z: http://www.zld.cz/cinnost/vyvoj/biometrie/sni_opt.php?p=2|5|7|25|38|#26

[16] Fingerprint sensing techniques. *Fingerchip* [online]. 13.4.2012 [cit. 2013-04-22]. Dostupné z: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.htm

[17] MALTONI, Davide. *Fingerprinc Recognition: Sensing, feature extraction and matching* [online]. Alghero (Itálie), 6.6.2003, 17 s. [cit. 22.4.2013]. Dostupné z: http://perso.telecom-paristech.fr/~chollet/Biblio/Cours/Biomet/fribourg/maltoni_1.pdf

[18] SCHLENKER, Anna a Milan ŠÁREK. *Biometrické metody pro aplikace v biomedicíně* [online]. 2011, 7 s. [cit. 23.4.2013]. Dostupné z: http://www.ejbi.org/img/ejbi/2011/1/Schlenker_cs.pdf

[19] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

[20] ROWE, Robert K., Kristin Adair NIXON a Paul W. BUTLER. *Multispectral Fingerprint Image Acquisition* [online]. 2008, 20 s. [cit. 25.4.2013]. Dostupné z: http://www.makortech.co.il/_Uploads/dbsAttachedFiles/Multispectral-Fingerprint-Image-Acquisition.pdf

[21] MALTONI, Davide. *A Tutorial on Fingerprint Recognition* [online]. Boloňa (Itálie), 26 s. [cit. 26.4.2013]. Dostupné z: http://sas4.ewi.utwente.nl/open/courses/intro_biometrics/Maltoni05.pdf

[22] Bioscrypt V-Pass FX. *SC Magazine* [online]. 5.9.2008 [cit. 2013-05-02]. Dostupné z: http://www.scmagazine.com/bioscrypt-v-pass-fx/review/2562/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D Dvourozměrný obraz (Two-dimensional space).

3D Třírozměrný obraz (Three-dimensional space).

CCD Typ snímací, elektronické součástky (Charge-coupled device).

CMOS Typ snímací, elektronické součástky (Complementary Metal–Oxide–Semiconductor).

DC Stejnosměrný elektrický proud (Direct Current).

FAR Pravděpodobnost nesprávného přijetí (False Acceptance Rate).

FRR Pravděpodobnost nesprávného odmítnutí (False Rejection Rate).

FTA Pravděpodobnost nemožnosti sejmutí biometrické vlastnosti (Failure To Enroll Rate).

FTE Pravděpodobnost neúspěšného pokusu o registraci (Failure To Acquire Rate).

LED Polovodičový světelný zdroj (Light-Emitting Diode).

PC Osobní počítač (Personal Computer).

RAM Typ počítačové paměti (Random-Access Memory).

TFT Typ polymeru.

TTL Standard v komunikaci integrovaných obvodů (Transistor-Transistor-Logic).

UV Ultrafialové (Ultraviolet).

SEZNAM OBRÁZKŮ

SEZNAM TABULEK