Snímače otisků prstů v oblasti bezpečnosti

Jakub Klinčúch

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Jakub Klinčúch**
Osobní číslo:	**A12729**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Snímače otisků prstů v oblasti bezpečnosti**
Téma anglicky:	**Fingerprint Sensors in the Commercial Security Industry**

Zásady pro vypracování:

1. **Proveďte literární rešerši na zadané téma.**
2. **Uveďte jednotlivé typy snímačů otisků prstů a princip jejich činnosti.**
3. **Popište způsob zpracování dat ze snímačů otisků prstů, uchování a nakládání s takto získanými daty.**
4. **Charakterizujte oblasti využití snímačů otisků prstů.**
5. **Uveďte nové trendy v této oblasti.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RAK, Roman a Jiří STRAUS. Biometrie a identita člověka ve forenzních a komerčních aplikacích: (výzkum, pokroky, perspektivy). 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.**
2. **LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a management IV. 1.vyd. Zlín: VeRBum, 2014, 390 s. ISBN 978-80-87500-57-6.**
3. **KŘEČEK, Stanislav a Filip ORSÁG. Příručka zabezpečovací techniky: (výzkum, pokroky, perspektivy). Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.**
4. **CHIRILLO, John a Jiří STRAUS. Implementing biometric security: (výzkum, pokroky, perspektivy). Vyd. 1. Indianapolis: Wiley Publishing, 2003, 414 s. ISBN 07-645-2502-6.**
5. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie: (výzkum, pokroky, perspektivy). 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**
6. **BOLLE, Ruud M a Filip ORSÁG. Guide to biometrics: (výzkum, pokroky, perspektivy). Vyd. 2. New York: Springer Science Business Media, 2004, xxix, 364 s. ISBN 03-874-0089-3.**
7. **ASHBOURN, Julian a Filip ORSÁG. Practical biometrics: from aspiration to implementation. Vyd. 2. London: Springer-Verlag, 2004, xiv, 159 s. ISBN 18-523-3774-5.**

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

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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 diplomové/bakalářské práce využít ke komerčním účelům;
- berú 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 diplomové 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 2.6.2015

.....
podpis diplomanta

ABSTRAKT

Bakalárska práca je zameraná na snímače odtlačkov prstov v oblasti bezpečnosti, existujúce typy snímačov a princíp ich činnosti. Ďalej popisuje spôsob spracovania dát zo snímačov odtlačkov prstov, uchovanie a nakladanie s takto získanými dátami. V práci sú uvedené oblasti využitia snímačov odtlačkov prstov a nové trendy v tejto oblasti.

Kľúčové slová: biometria, biometrické metódy, odtlačok prsta, snímače odtlačkov prstov.

ABSTRACT

The bachelor´s thesis is focused on the fingerprint sensor for safety, existing sensors types and of their operation. Farther, is described a method for processing data from fingerprint readers, preservation and management of this data. Thesis presents the area of using fingerprint readers and new trends in this area.

Keywords: biometrics, biometric methods, fingerprint, fingerprint readers.

Týmto by som sa rád poďakoval vedúcemu mojej bakalárskej práce pánovi Ing. Petrovi Navrátilovi za odborné vedenie, pomoc pri poskytnutí odporúčanej literatúry a poskytnuté konzultácie pri spracovaní bakalárskej práce.

Ďalej by som sa chcel poďakovať svojej rodine a priateľom za ich podporu.

OBSAH

ÚVOD

Témou tejto bakalárskej práce sú snímače odtlačkov prstov a ich využitie v oblasti bezpečnosti. V súčasnej modernej dobe s nárastom modernizácie technológií a integrácie nových informačných aplikácií do bežného života narastá aj miera kriminality. S týmto nárastom kriminality stúpa zároveň potreba o integráciu bezpečnostných systémov, ktoré by zamedzili tomu, aby boli zneužité informačné aplikácie, ktoré uľahčujú činnosti bežného života. Ide o bežné činnosti ako napríklad Internetbanking, platba pomocou platobnej karty, autentizácia osôb pre prístup k výpočtovým a komunikačným prostriedkom či autentizácia vstupu osôb do fyzických objektov. Bezpečnostným prvok, ktorý sa v súčasnosti integruje k zabezpečeniu spomínaných prostriedkov či objektov sú snímače odtlačkov prstov, na základe ktorých je zosnímaný odtlačok prsta vyhodnotený a osoba jednoznačne identifikovaná a sú jej pridelené práva pre vstup do určitých objektov, prístup k výpočtovým a komunikačným prostriedkom či práva pre uskutočnenie platby. Snímače odtlačkov prstov sú v súčasnej dobe najrozšírenejším biometrickým systémom, pretože sú dostatočne presné, lacné a užívateľsky prívetivé. Ich zastúpenie na trhu tvorí takmer polovicu zo všetkých biometrických systémov. Snímače odtlačkov prstov majú prevažné využitie v štátnych organizáciách, postupne sa začleňujú do podnikov a poslednou dobou sa začínajú začleňovať do rôznych mobilných zariadení a niektorých domácností.

Bakalárska práca je rozdelená na teoretickú a praktickú časť. V prvej časti je objasnená časť terminológie, potrebná pre pochopenie ďalšieho výkladu, ako napríklad biometria, odtlačok prsta, sú vysvetlené pojmy identifikácia, verifikácia, aký je medzi nimi rozdiel a chyby, ktoré sa môžu vyskytnúť pri snímaní odtlačku prsta. Ďalej sú popísané jednotlivé typy snímačov odtlačkov prstov, ktoré sú rozdelené na kontaktné a bezkontaktné. V závere prvej časti je popísané spracovanie dát zo snímačov odtlačkov prstov. V druhej časti sú uvedené oblasti využitia snímačov odtlačkov prstov a nové trendy v tejto oblasti.

I. TEORETICKÁ ČASŤ

1 POUŽITÁ TERMINOLÓGIA

V tejto časti bude uvedená terminológia pre pochopenie výkladu nasledujúceho v ďalších častiach práce. Budú stručne rozobraté a vysvetlené pojmy ako biometria, čo to je, odkiaľ pochádza, prečo vznikla a načo slúži, odtlačok prsta a jeho charakteristika, identifikácia, verifikácia a procesy, ktoré pri nich prebiehajú a ďalej chyby, ktoré môžu vzniknúť pri zavádzaní odtlačkov prstov do biometrických aplikácií a pri ich používaní.

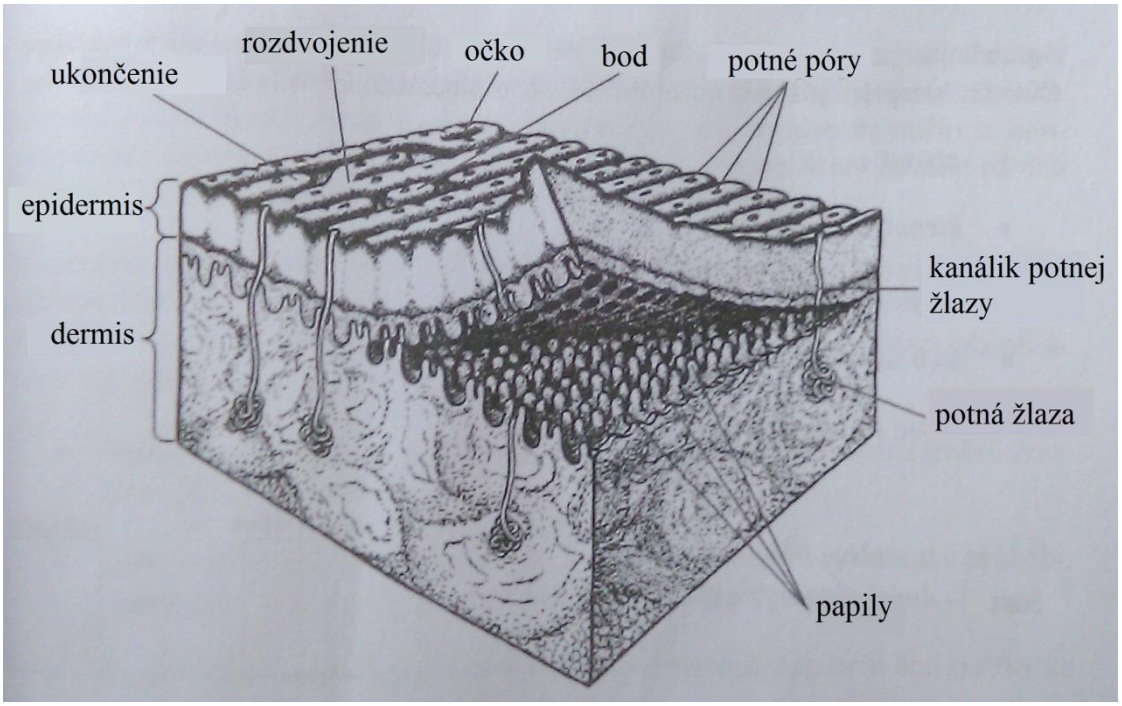
1.1 Biometria

Biometria je slovo pochádzajúce z gréčtiny a skladá sa z dvoch slov – „bios“(znamená život) a „metron“ (znamená merať). Ide teda ako keby o meranie života. V informačných technológiách sa týmto výrazom označuje postup rozpoznávania vzorov ľudských vlastností.

Biometria je automatizovaným rozpoznávaním ľudských jedincov na základe ich charakteristických anatomických rysov (napr. odtlačok prsta, tvár, sietnica, dúhovka, geometria ruky a prstov, DNA) a behaviorálnych rysov (napr. chôdza, dynamika stlačenia kláves, dynamika podpisu). [1]

1.2 Odtlačok prsta

Každý ľudský jedinec má na povrchu prstov (na rukách aj nohách) papilárne línie (vyvýšené reliéfy kože), ktorých tvar je u každého jedinca jedinečný. Na základe týchto papilár je možné jedincov medzi sebou rozlišovať a jednoznačne identifikovať. Výnimkou sú ľudia s rôznymi druhmi chorôb a poruchami kože. Odtlačok prsta je grafickou reprezentáciou papilárnych línií. Papilárne línie sa formujú behom embryonálneho vývoja a sú nemenné s časom, teda pokiaľ nedôjde k ich poškodeniu napríklad poranením. Výška papilárnych línií leží v rozmedzí 0,1 – 0,4 mm a šírka v rozmedzí 0,2 – 0,5 mm. Na svete neexistujú dva rovnaké prsty a teda každý prst je unikátnym vzorom. [1]



Obrázok 1 Rez kožou a zobrazenie priebehu papilárnych línií [1]

1.3 Identifikácia

Identifikácia je procesom porovnania (jeden k mnohým, 1:n) nasnímaného biometrického vzoru so všetkými referenčnými šablónami, ktoré sú uložené v databáze. Vedie to k zisteniu, ktorá referenčná šablóna (ak sa nachádza v databáze) zodpovedá šablóne vytvorenej z nasnímaného vzoru. Biometrická aplikácia pre identifikáciu potom rozpozná totožnosť preverovanej osoby. [2]

Identifikácia je typická pre policajno-súdne aplikácie a verifikácia skôr pre aplikácie bezpečnostno-komerčné.

Každé porovnanie má dve oddelené funkcie, ktoré sú navzájom duálne: [1,2]

- potvrdiť, že oprávnená osoba je tou, za ktorú sa vydáva
- dokázať, že neoprávnená osoba nie je tou, za ktorú sa vydáva

Hovoríme o pozitívnej a negatívnej identifikácií.

Pozitívna identifikácia (positive identification)

Cieľom pozitívnej identifikácie je zabrániť používanie identity jednej osoby ďalšími osobami. Keď biometrická aplikácia využívajúca princíp pozitívnej identifikácie v porovnávacom procese nenájde zhodu medzi šablónou predkladaného biometrického vzoru

s žiadnou referenčnou šablónou, ktorá je uložená v databáze, potom je výsledkom odmietnutie (rejection) prístupu užívateľa do objektu. Keď sú obidve šablóny stotožnené, ide naopak o prijatie (acceptance) užívateľa. [3]

Negatívna identifikácia (negative identification)

Cieľom negatívnej identifikácie je vylúčiť stav, kde jedna osoba využíva identitu viacerých osôb. Keď biometrická aplikácia využívajúca princíp negatívnej identifikácie v porovnávacom procese nenájde zhodu medzi šablónou predkladaného biometrického vzoru s žiadnou referenčnou šablónou, ktorá je uložená v databáze, potom je výsledkom prijatie (acceptance) prístupu užívateľa. Pri stotožnení obidvoch šablón, ide naopak o odmietnutie (rejection) užívateľa. [3]

1.4 Verifikácia

Verifikácia je procesom porovnania (jedna k jednej, 1:1) jedinej šablóny, ktorá je vytvorená z nasnímaného biometrického vzoru s jedinou referenčnou šablónou, ktorá patrí preverovanej osobe. Cieľom verifikácie je zistiť, či je preverovaná osoba naozaj tou, za ktorú sa vydáva. Biometrická aplikácia vyvracia alebo potvrdzuje identitu preverovanej osoby.

Verifikačné procesy sú vždy omnoho rýchlejšie, než procesy identifikačné, pretože porovnanie pri verifikácií je iba v pomere 1:1. Identifikačné procesy sú omnoho náročnejšie z pohľadu biometrickej aplikácie, keďže je potrebné vyhodnotiť všetkých *n* uložených referenčných šablón. [1,3]

1.5 FRR (False Rejection Rate)

Pravdepodobnosť chybného odmietnutia je jedným z kritérií, ktoré poukazuje na bezpečnostnú a užívateľskú spoľahlivosť. Udáva s akou pravdepodobnosťou bude chybovať biometrické zariadenie a nerozpozná oprávneného užívateľa alebo osobu, ktorá bola už skôr zaregistrovaná, ktorí majú v aplikácií už uloženú svoju referenčnú šablónu. Tento užívateľ je potom odmietnutý a musí sa pokúsiť preukázať svoju identitu znova. [3,5]

Pravdepodobnosť chybného odmietnutia FRR je definovaná: [3]

$$FRR = \frac{N_{FR}}{N_{EIA}} \; alebo \; FRR = \frac{N_{FR}}{N_{EVA}}$$

kde:

N_{FR} – Number of False Rejection (počet chybných odmietnutí)

N_{EIA} – Number of Enrol Identification Attempts (počet pokusov oprávnených osôb o identifikáciu)

N_{EVA} – Number of Enrol Verification Attempts (počet pokusov oprávnených osôb o verifikáciu)

Z bezpečnostného hľadiska nejde v prípade civilných aplikácií o kriticky negatívny jav, ale je to z pohľadu užívateľskej prítulnosti nežiaduce. Dôsledkom toho je potom pokles dôvery v dané zariadenie. [3,5]

1.6 FAR (False Acceptance Rate)

Na druhej strane je požiadavka na vysokú bezpečnosť biometrického zariadenia, ktoré nesmie akceptovať neoprávnené osoby. V živote je možné stretnúť osoby, snažiace sa prekonať kontrolné bezpečnostné mechanizmy, získať identitu niekoho iného, preniknúť do stráženého priestoru a následne vykonať nežiaducu činnosť. Takéto osoby musia byť biometrickým zariadením rozpoznané a nekompromisne odmietnuté. V aplikáciách, ktoré kontrolujú prístup do objektov, je chybné prijatie neoprávnenej osoby chápané ako bezpečnostný incident, dôsledkom ktorého môže dôjsť k nežiaducim aktivitám, narušeniu majetku, stability objektu atď. [3,5]

Pravdepodobnosť chybného prijatia FAR je definovaná: [3]

$$FAR = \frac{N_{FA}}{N_{IIA}} \; alebo \; FAR = \frac{N_{FA}}{N_{IVA}}$$

kde:

N_{FA} – Number of False Acceptance (počet chybných prijatí)

N_{IIA} – Number of Impostor Identification Attempts (počet pokusov neoprávnených osôb o identifikáciu)

N_{IVA} – Number of Impostor Verification Attempts (počet pokusov neoprávnených osôb o verifikáciu)

2 TYPY SNÍMAČOV ODTLAČKOV PRSTOV

Pomocou senzorov je realizované interaktívne snímanie odtlačkov prstov, ktoré je implementované do najrôznejších technických zariadení. Tieto senzory pracujú na rôznych fyzikálnych princípoch. Snímacie senzory sa rozdeľujú na senzory kontaktné a bezkontaktné, podľa toho, akým spôsobom snímajú povrch pokožky s daktyloskopickou kresbou.

2.1 Kontaktné senzory

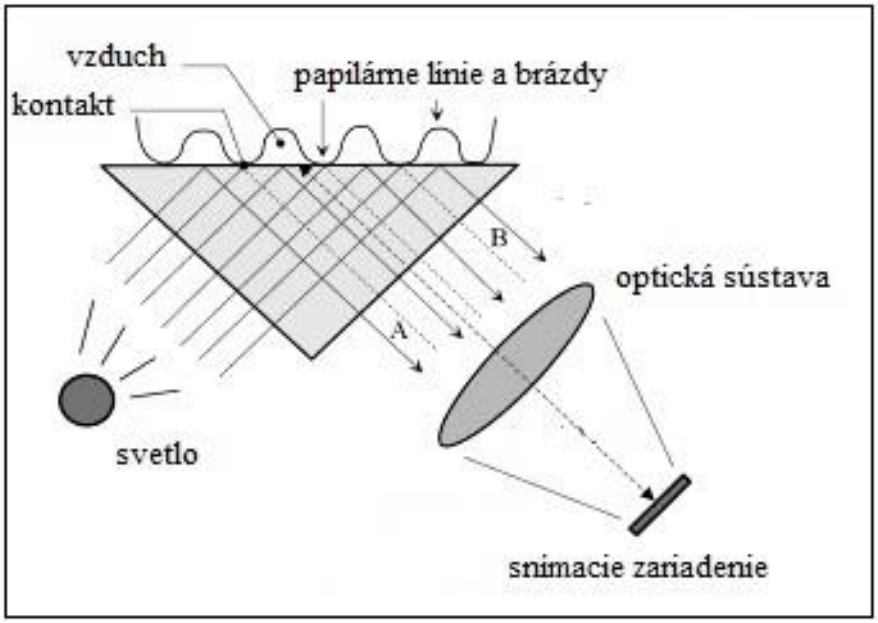
Kontaktné senzory zahŕňajú veľa fyzikálnych spôsobov snímania odtlačkov prstov. Patria sem: optické, transmisné, elektronické, optoelektronické, elektroluminiscenčné, kapacitné, tlakové, teplotné, rádiofrekvenčné a multispektrálne senzory. [3,4]

2.1.1 Optický senzor

Optický senzor pracuje na technológií FTIR (Frustrated Total Internal Reflection). Laserový lúč osvetľuje zospodu povrch prsta, ktorý sa dotýka priehľadnej dosky senzoru. Svetelný tok, ktorý je odrazený od povrchu prsta je snímaný CCD prvkom. Množstvo svetla, ktoré sa odrazí, záleží na papilárnych líniách a hĺbke brázd. Papilárne línie odrážajú svetlo viac a brázdy zasa menej. Vplyv na odraz má aj potno-tukový výlučok, poprípade zmiešaný so špinou, nachádzajúci sa medzi kožou a sklom. Citlivosť prvku CCD je nastavená tak, aby CCD prvok neregistroval odraz svetla od brázd. [3,4]

Optické snímače, ktoré nie sú založené na technológií FTIR, používajú optické vlákna. Hustý zväzok optických vlákien, postavených kolmo k rovine snímacej plochy senzoru. Takisto sa tu využíva metóda osvitu a odrazeného svetelného toku. Ďalšie senzory využívajú technológiu CMOS (Complementary Metallic Oxide Semiconductor). [3]

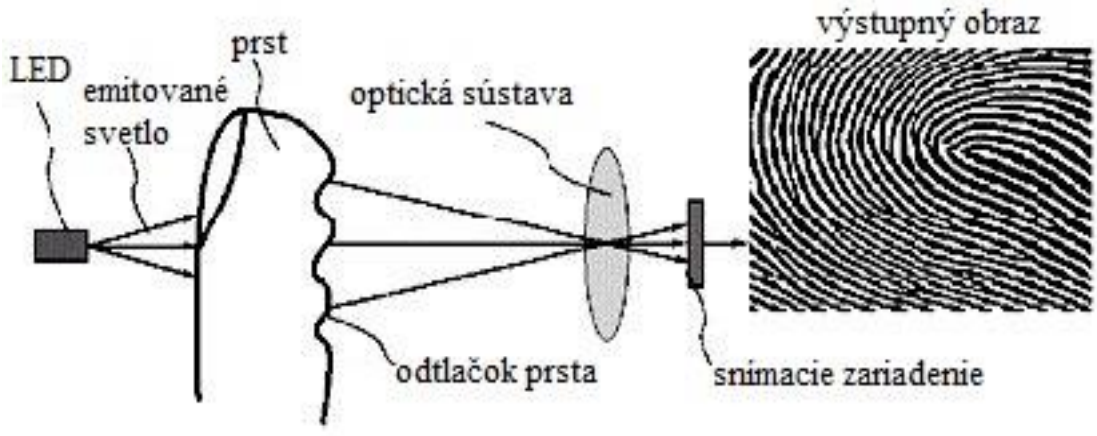
Senzory, ktoré sú založené na dvojrozmernom (2D) optickom snímaní, nemusia rozpoznať napodobneninu odtlačku prsta, získanú bez vedomia autentizovanej osoby a následne odtlačok vhodne upravený tak, aby bol dobre čitateľný pre senzor. [3,4]



Obrázok 2 Optický senzor [12]

2.1.2 Transmisný optický senzor

Transmisný optický snímač pracuje na princípe osvetlenia prsta, najčastejšie infračervenou LED diódou, ktorá prst po priložení osvieti z vrchnej strany. Svetlo prejde cez prst do sústavy čočiek, ktorá ho usmerní do snímacieho zariadenia. Snímacie zariadenie je najčastejšie tvorené CMOS alebo CCD čipom. [4]



Obrázok 3 Transmisný optický senzor [13]

2.1.3 Elektronický senzor

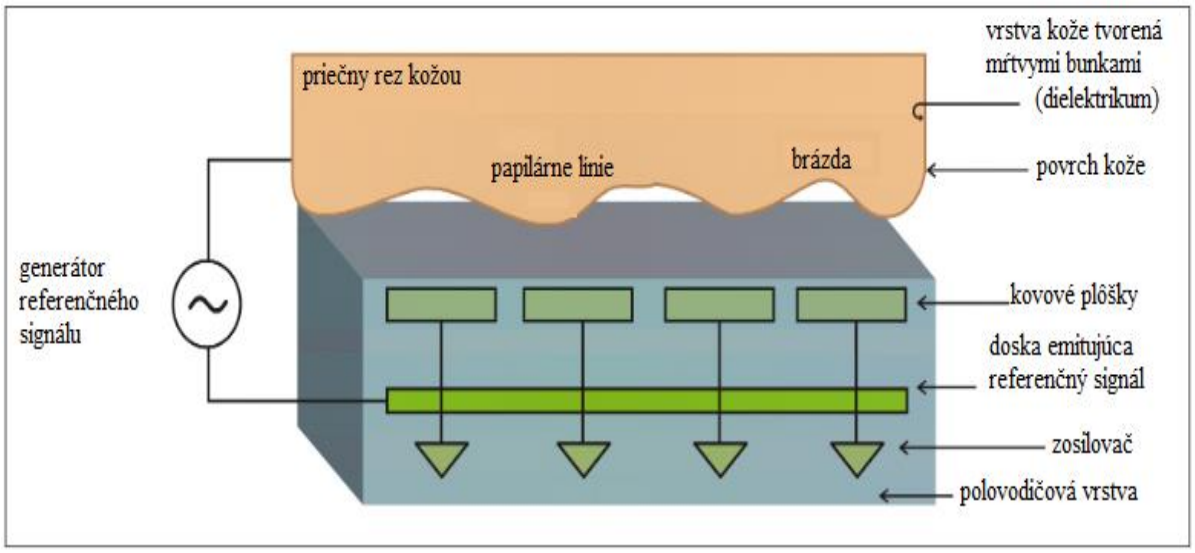
Elektronický senzor pracuje na princípe vzniku elektrického poľa medzi dvoma doskami. Tieto dosky musia byť paralelné, vodivé a elektricky nabité. Ak zmeníme pôvodný plochý

tvar hornej dosky na profil tvorený povrchom daktyloskopických papilár a brázd, zmení sa tak aj tvar elektrického poľa, ktorý je na tomto tvare závislý. Horná doska elektronického senzoru je tvorená povrchom kože, do ktorej je pustený riadiaci elektrický signál.

Vrchná vrstva pokožky je tvorená odumretými bunkami, ktoré sú nevodivé. Pod touto vrstvou sa nachádza vysoko vodivá vrstva slanej tekutiny. Slaná tekutina vzniká ako produkt rastu a odumierania povrchových buniek kože. Táto vodivá vrstva kopíruje priestorovo profil vonkajšej vrstvy kože. [3]

Okolo senzoru sa nachádza vodivý prstenec a hneď ako sa prst dotkne tohto prstenca, nastane uzavretie elektrického obvodu. Pole snímacích antén ležiace nad základnou doskou, vysiela referenčný signál, zachytí elektrické pole deformované tvarom daktyloskopických papilár a brázd. Signál je následne zosilnený a transformovaný do elektronickej podoby daktyloskopického odtlačku. [4]

Elektronický senzor nereaguje na vrchnú vrstvu kože, ani na špinu. Preniká hlbšie pod povrch, čo má výhodu, že snímač nesníma len daktyloskopický profil povrchu kože, ktorý môže byť poškodený alebo znečistený. Snímač nie je citlivý ani na suché alebo mokré odtlačky. [3,4]



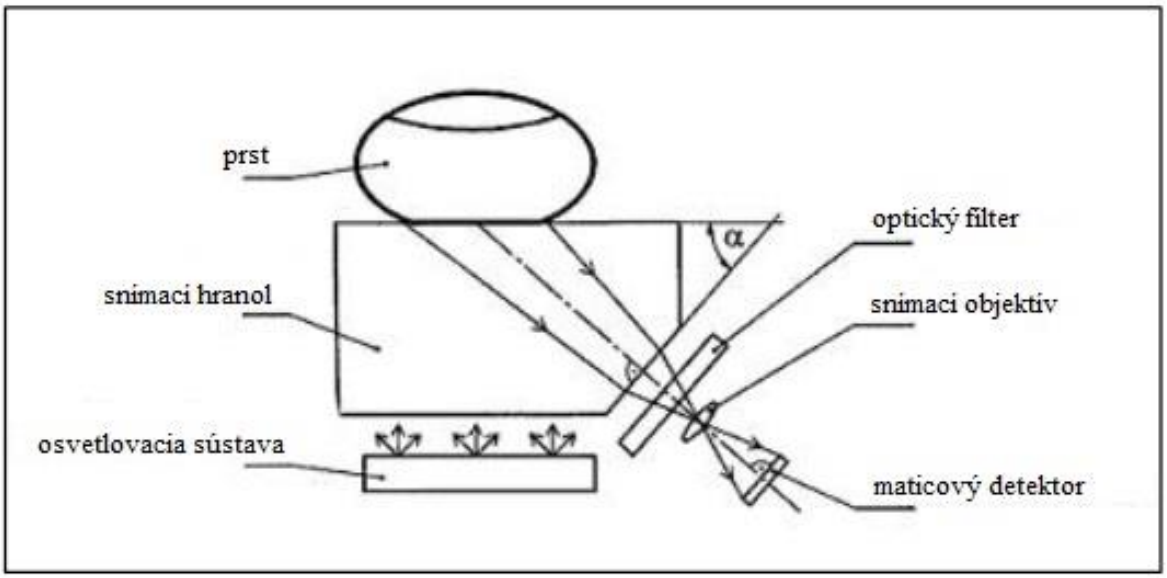
Obrázok 4 Elektronický senzor [14]

2.1.4 Optoelektronický senzor

Optoelektronický senzor sa skladá z dvoch vrstiev. Horná vrstva, ktorá má priamy kontakt s kožou verifikovanej osoby a je vyrobená z polyméru TFT (Thin Film Transistors). TFT je priehľadný film, ktorý tvoria miniatúrne tranzistory, umožňujúce vysoko efektívnu

metódu prepínania jednotlivých pixelov medzi stavmi „zapnuté“ a „vypnuté“. Tento polymér má schopnosť po dotyku emitovať svetlo, ktoré je zachytené v ďalšej sklenenej vrstve, v ktorej sú v hustom poli zatavené fotodiódy. Fotodiódy prevádzajú svetelný impulz na elektrický impulz. Týmto spôsobom sa vytvorí elektronický obraz daktyloskopického odtlačku. [3,7]

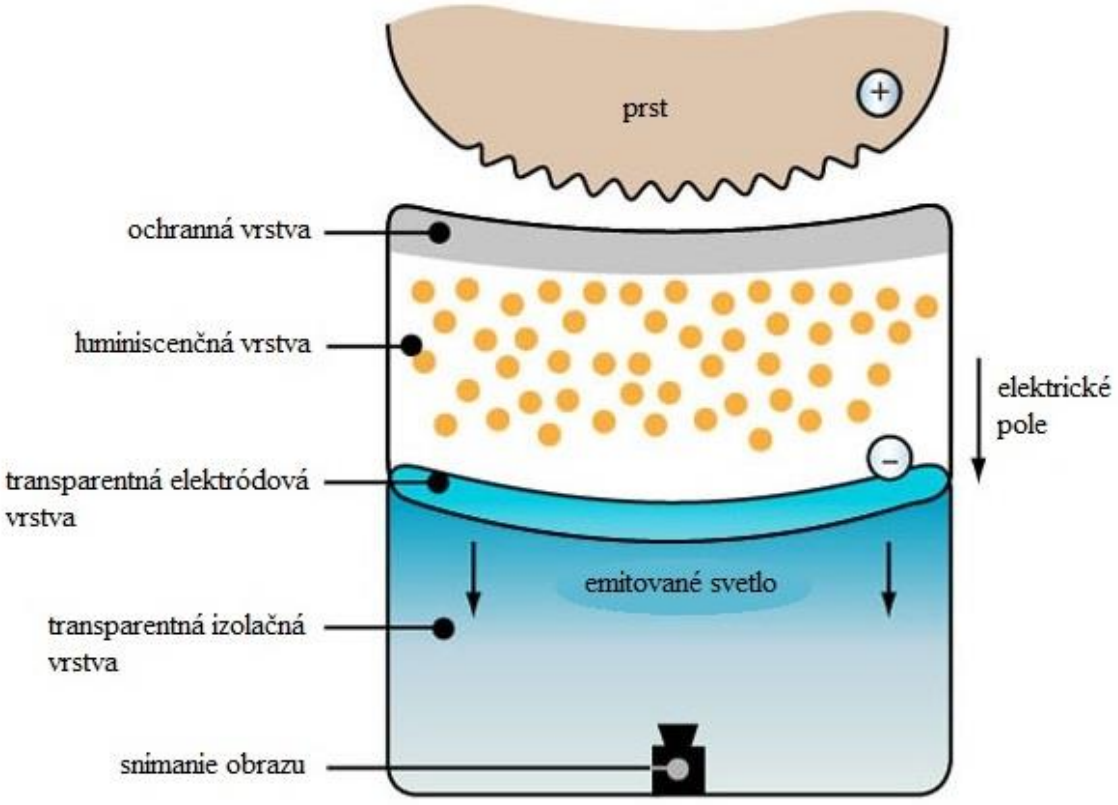
Technológia optoelektronického snímača je v dnešnej dobe považovaná za jednu z najkvalitnejších a má veľmi dobrú perspektívu do budúcna. [3]



Obrázok 5 Optoelektronický senzor [15]

2.1.5 Elektroluminiscenčný senzor

V hornej časti elektroluminiscenčného snímača sa nachádza snímacia plocha, zložená z niekoľkých vrstiev. Najdôležitejšou z týchto vrstiev je svetlo emitujúca vrstva, ktorá emituje svetlo pri styku s papilárnymi líniami. Vzniká tak svetelný obraz definujúci obraz papilárnych línií. V dolnej časti je zatavené husté pole fotodiód v skle. Pole fotodiód sníma svetlo zo snímacej plochy a vytvára digitálny obraz. [4]



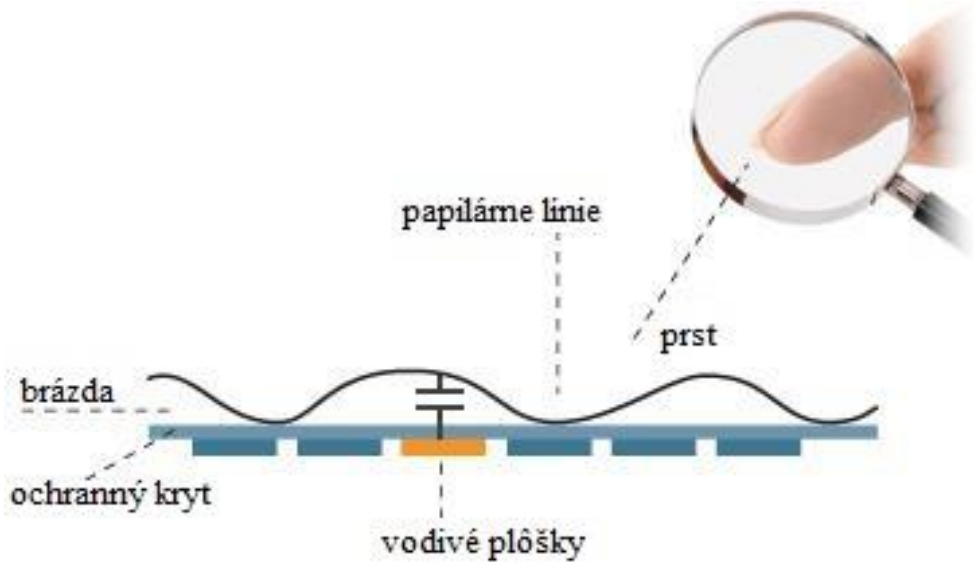
Obrázok 6 Elektroluminiscenčný senzor [16]

2.1.6 Kapacitný senzor

Kapacitný senzor pre snímanie odtlačku prsta používa technológiu merania elektrickej kapacity. Senzor je zložený zo stoviek tisíc vodivých plôch, ktoré sú medzi sebou odizolované. Dotykom kože papilárne línie premosťujú jednotlivé vodivé plôšky v závislosti na ich kresbe. Brázdy sa chovajú ako izolant. Medzi jednotlivými vodivými plôškami sa meria napätie a kapacitné úbytky a vzniká tak digitalizovaný obraz papilárnej kresby. [3]

Každý pixel (obrazový bod) má 8 bitov, čo znamená že odtlačok môže byť zobrazený v 256 odtieňoch šedej farby. V terminológií spracovania obrazov predstavuje hodnota nula farbu čiernu a hodnota 255 farbu bielu. V praxi je ale obmedzený rozsah stupňov šedej farby z obidvoch strán, ktoré sa v anglickej literatúre nazývajú „water line" a "air line". "Water line" je stav, v ktorom je celý povrch senzoru pokrytý vodou (v odtlačku neexistujú brázdy, teda povrch kože nie je zvrásnený papilárnymi líniami). „Air line" je stav, kedy nedochádza k žiadnemu kontaktu, teda senzor je v kontakte iba zo vzduchom. Niekde medzi týmito dvoma hranicami sa nachádza odtlačok prsta. [3,4]

Slabým miestom kapacitných senzorov je citlivosť na znečistenie pokožky prstov od zvyškov jedla, obsahujúcich napríklad soľ alebo cukor, ktoré menia vodivosť ľudskej kože. Takisto aj používanie ochranných a liečivých krémov na ruky, môže ovplyvňovať kvalitu snímania odtlačku. [3,4]



Obrázok 7 Kapacitný senzor [17]

2.1.7 Tlakový senzor

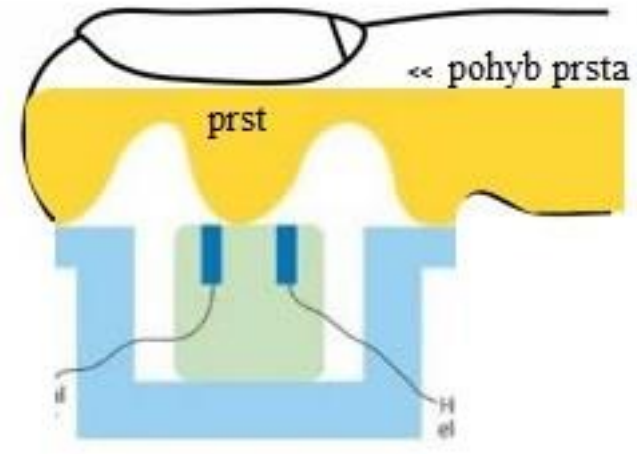
Tlakový senzor reaguje na tlak papilár na povrch senzoru. Povrch senzoru tvorí elastický, piezoelektrický materiál, ktorý transformuje tlak papilárnych línií do elektrického signálu. Vytvára tak obraz daktyloskopického obrazu. Papilárne línie vyvolávajú lokálne tlakové pôsobenie na snímacej ploche, zatiaľ čo brázdy vytvárajú tlak nižší. Všeobecne pre tlakové senzory pre snímanie odtlačkov platí, že pracujú rovnako dobre v suchom aj mokrom prostredí. Tlakový senzor nie je teda citlivý na „vlhké“ ani na „mokré“ odtlačky prstov určitých skupín ľudí. [3]

Tento senzor, jeho riadiaca a porovnávacia technológia bola miniaturizovaná tak, že je možné ho implementovať do klasickej bankomatovej karty. Tým je zaistená neprenosnosť karty na neoprávnenú osobu a zároveň odpadá potreba prenosu daktyloskopickej šablóny. Tým je odstránený jeden z bezpečnostne slabých faktorov. [3,7]

2.1.8 Teplotný senzor

Teplotný senzor reaguje veľmi citlivo na teplotné zmeny medzi papilárnymi líniami dotýkajúcich sa snímacieho povrchu a brázdami, ktoré majú väčšiu vzdialenosť od povrchu

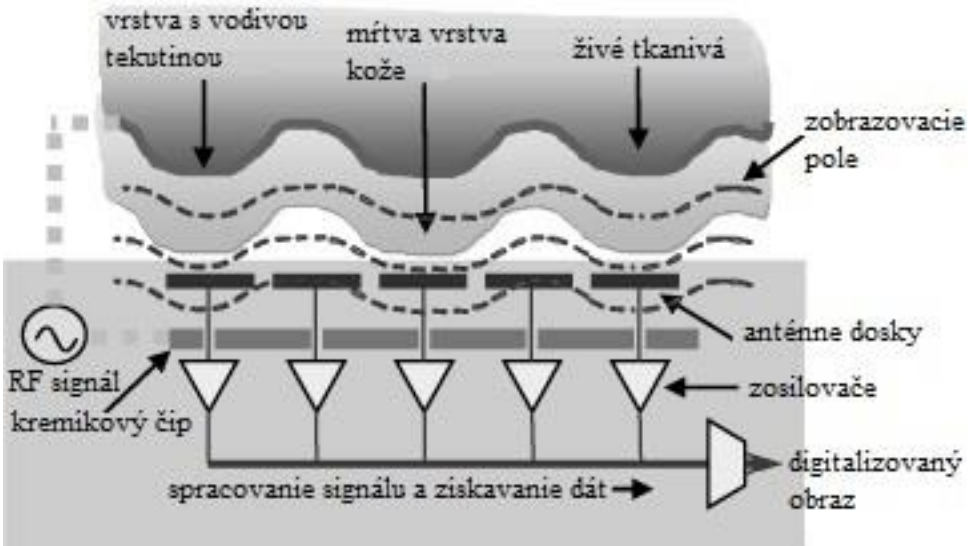
a teda aj inú teplotu. Teplota je dôležitým faktorom, pretože napovedá či snímaný odtlačok patrí živej osobe. Sú tak eliminované rôzne pokusy o napodobnenie odtlačku. [5,7]



Obrázok 8 Teplotný senzor [18]

2.1.9 Rádiofrekvenčný senzor

Rádiofrekvenčný senzor pracuje na princípe vysielania rádiofrekvenčného signálu. Táto metóda spočíva na dvoch doskách, ktoré sú umiestnené rovnobežne a je na ne pripojený generátor striedavého signálu. Jednu z dosiek tvorí dotyková plocha snímača a druhú samotný odtlačok prsta. Papilárne línie formujú signál prechádzajúci prstom. Vzdialenosť prsta od snímača určuje silu signálu, čo znamená že papilárne línie majú väčší signál a brázdy menší. Signál je prijímaný poľom aktívnych antén, zosilnený, integrovaný a na záver digitalizovaný. [3,4]



Obrázok 9 Rádiofrekvenčný senzor [19]

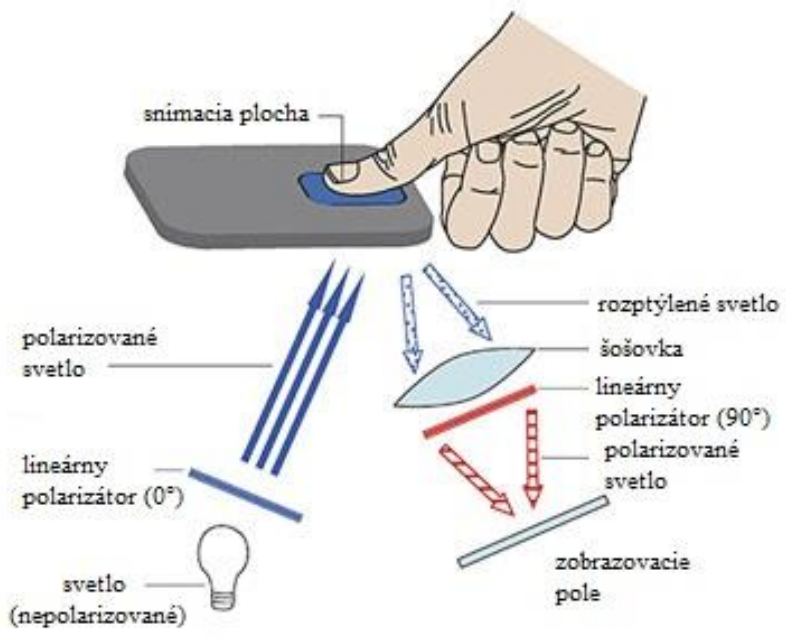
2.1.10 Multispektrálny senzor

Multispektrálny senzor sa radí k novým technológiám snímania odtlačkov prstov. Jeho princíp spočíva v použití viacerých osvetľovacích sústav, emitujúcich svetlo rôznych vlnových dĺžok. Snímanie prebieha osvetlením s použitím polarizátora a bez použitia polarizátora. [3,5]

Osvetlenie s použitím polarizátora používa sústavu LED diód, ktoré emitujú do polarizátora svetlo. Na dotykovú plochu snímača tak dopadá lineárne polarizované svetlo. Do optickej sústavy a zobrazovacieho polarizátora je smerovaná časť svetla ovplyvnená prstom. Vzájomným umiestnením polarizátora a optickej sústavy, sa dosiahlo zredukovanie vplyvu odrazeného svetla od povrchu kože a zdôraznenie rozptýleného svetla, ktoré prešlo kožou. [5]

Osvetlenie bez polarizátora využíva priame, náhodne polarizované osvetlenie z LED diód. Svetlo, ktoré sa odrazilo spolu so svetlom, ktoré prešlo cez kožu, dokáže prejsť zobrazovacím polarizátorom a vytvoriť výsledný obraz. [5]

Multispektrálny senzor sa považuje v porovnaní s ostatnými typmi senzorov za veľmi bezpečný prvok v oblasti biometrickej autentizácie, vďaka snímaniu s použitím svetla o viacerých vlnových dĺžkach a teda schopnosti snímať biometrické údaje pod povrchom kože. [3,5]



Obrázok 10 Multispektrálny senzor [20]

2.2 Bezkontaktné senzory

K najznámejším skupinám bezkontaktných senzorov patria:

- optické
- ultrazvukové

2.2.1 Optický senzor

Princíp na akom pracuje bezkontaktný optický senzor je podobný dotykovému optickému senzoru. Svetelný lúč sníma odtlačok zo vzdialenosti 30 až 50 mm. Týmto spôsobom je eliminované znečistenie snímacieho povrchu senzora dotykmi špinavých prstov a zároveň je eliminované aj zachytávanie papilárnych línií na povrchu snímača. [3]

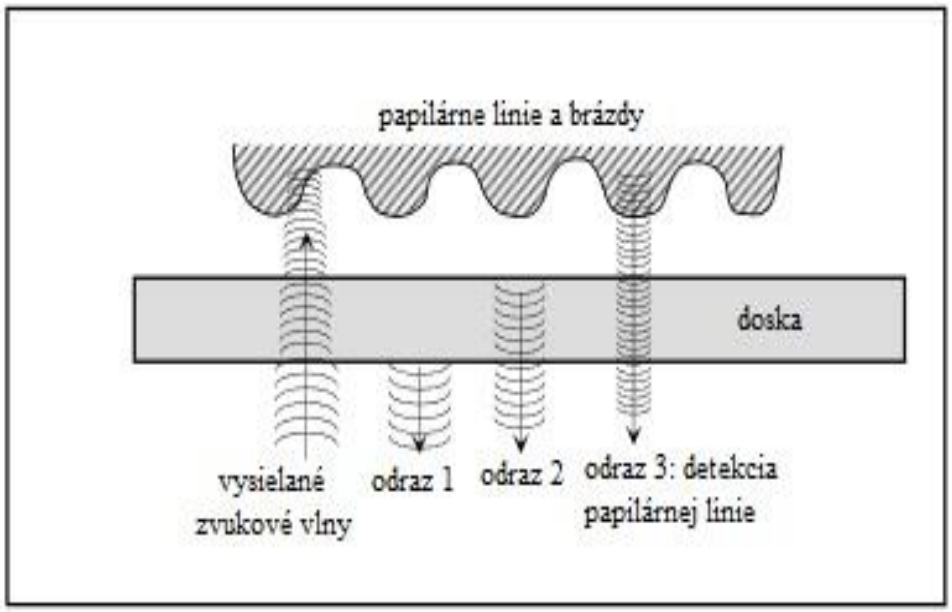
2.2.2 Ultrazvukový senzor

Ultrazvukové senzory využívajú princíp lekárskeho sonografu, s cieľom vytvoriť vizuálny obraz odtlačku prsta. Používajú veľmi vysoké frekvencie zvukovej vlny, ktorá dokáže preniknúť pod vrchnú vrstvu kože. Zvukové vlny sú generované pomocou piezoelektrických meničov a odrazené vlny sa merajú pomocou piezoelektrických materiálov. Snímanie odrazených a deformovaných vĺn je realizované rotujúcou hlavou alebo hustou sieťou pevných snímacích čidiel umiestnených v rovine. Vzhľadom k tomu, že vnútorná vrstva kože vykazuje rovnaký charakteristický vzor odtlačku prsta ako vrchná vrstva kože, odrazené vlny merania sa môžu použiť na vytvorenie obrazu odtlačku prsta. To eliminuje potrebu čistej, nepoškodenej vrchnej vrstvy kože a čistý snímací povrch. Nasnímaný obraz odtlačku prsta je trojrozmerný (3D) a má vysoký kontrast. [5]

Vďaka týmto vlastnostiam je možné pomerne ľahko rozpoznať daktyloskopický falzifikát, ktorý je spravidla dvojrozmerný.

Snímanie ultrazvukovým senzorom odstraňuje niektoré nedostatky vznikajúce pri ostatných metódach snímania. Napríklad opticky snímané odtlačky sú iba dvojrozmerné (2D) a často majú nízky kontrast. Ďalej so sebou optické metódy nesú určité riziko nízkej kvality, čo môže byť spôsobené znečisteným odtlačkom, alebo nízkou či naopak vysokou vlhkosťou povrchu kože. Vďaka fyzickému kontaktu kože s plochou senzora môžu zostávať odtlačky, poprípade kožné tukové výlučky potu v tvare papilárnych línií na povrchu snímača a môžu byť vyhodnotené ako pravé, aj keď už užívateľ nie je v

priamom kontakte so zariadením. Na základe takto zanechaných daktyloskopických stôp je potom v niektorých prípadoch možné sa znova prihlásiť do zariadenia. [5]



Obrázok 11 Ultrazvukový senzor [21]

3 SPRACOVANIE DÁT ZO SNÍMAČOV ODTLAČKOV PRSTOV

V tejto oblasti budú uvedené biometrické pojmy ako biometrický vzor, biometrické charakteristiky, markanty, biometrická šablóna, kde sa používajú a k akým účelom sú potrebné. Ďalej bude popísaný spôsob zberu dát, ich prenos, spracovanie a následné uchovanie.

3.1 Základné biometrické pojmy

V nasledujúcej časti uvediem štyri základné pojmy, na ktoré sa budem ďalej odkazovať a ktoré budem postupne rozvíjať.

Biometrický vzor – je to odraz anatomicko-fyziologických charakteristík človeka do vonkajšieho sveta, v tomto prípade daktyloskopický odtlačok prsta na predmete.

Biometrické charakteristiky – z biometrického vzorku akýmkoľvek spôsobom merateľné charakteristiky. Odtlačok prsta sa skladá z rôzne tvarovaných papilárnych línií, ktoré sa rôzne rozvetvujú, končia alebo krížia. Miestami môžu byť tieto línie porušené, zjazvené, poleptané a pod. Všetky tieto údaje je možné popísať a zmerať. Pre identifikáciu nie sú ale potrebné všetky. [6]

Biometrické markanty – biometrické charakteristiky, ktoré sú potrebné pre identifikáciu alebo verifikáciu. V odtlačku prsta je možné nájsť markanty ako napríklad začiatok a koniec línie, kríženie, očko, dvojitá vidlica, trojitá vidlica a pod. Spravidla sa v biometrickom vzore nachádza vždy väčšie množstvo upotrebiteľných markantov, ako je potrebné pre identifikáciu alebo verifikáciu. [6]

Biometrická šablóna – je konečným výsledkom formalizácie a optimalizácie biometrického vzoru pre identifikačné alebo verifikačné účely. Biometrická šablóna sú namerané charakteristiky s minimálnym počtom markantov, ktoré úplne stačia pre jednoznačnú identifikáciu alebo verifikáciu. Ukladá sa na rôzne nosiče informácií (počítačové databázy, identifikačné karty, platobné karty a pod.). Veľkosť šablóny uloženej na záznamovom nosiči sa udáva pomocou informačnej jednotky byte. Automatizované vyhodnotenie identifikácie alebo verifikácie prebieha na základe biometrických šablón. [6]

Každé biometrické spracovanie má päť základných etáp: [3]

- zber biometrických dát

- prenos dát
- spracovanie nameraného signálu
- proces rozhodovania
- uloženie dát

3.2 Zber dát

Zberom biometrických dát rozumieme biometrické spracovanie, ktoré začína meraním anatomicko-fyziologických charakteristík človeka. Základný predpoklad pre identifikáciu alebo verifikáciu je jednoznačnosť identifikačných charakteristík (tzv. markantov), ich merateľnosť a časová stálosť, teda ich nemennosť. Meranie biometrických charakteristík musí byť teda opakovateľný jav, pri ktorého každom meraní je potrebné dosiahnuť rovnakých výsledkov, alebo výsledkov s vyhovujúcou chybovosťou, ktorá musí byť dopredu známa. [3,6]

Užívateľ musí či už vedome, alebo nevedome umožniť odňatie svojich biometrických charakteristík pomocou snímacieho senzoru. Tým môže byť mechanický odtlačok palca a následne jeho skenovanie pre získanie elektronického obrazu, alebo klasická kriminalistická metóda odtlačku prsta pomocou daktyloskopickej černe. Každé spracovanie musí brať na ohľad chovanie užívateľa (užívateľ je zoznámený, alebo nie je zoznámený s biometrickou metódou, jej podstatou a hlavne s cieľom preverovania, užívateľ spolupracuje, alebo nespolupracuje a pod.) [6]

Ak má byť biometrická aplikácia schopná vymieňať si údaje s inou aplikáciou, musí byť štandardizovaná. Je to jediný spôsob, akým je možné zabezpečiť zhodnosť nameraných údajov pri jednej a tej istej osobe v rôznych aplikáciách a rôznymi senzormi.

Nasnímaný obraz biometrických identifikačných charakteristík, v mojom prípade odtlačok prsta, budem ďalej nazývať všeobecne „biometrický vzor“. Je to jednoznačný, nespracovaný obraz anatomicko-fyziologickej charakteristiky získaný snímaním, ktorý je určený k vytvoreniu biometrickej šablóny. [3,6]

3.3 Prenos dát

Zber biometrických dát niektorými aplikáciami prebieha na jednom mieste a ich spracovanie a uskladnenie prebieha na mieste druhom. V takýchto prípadoch je nutnosť zabezpečiť prenos dát. Jedná sa o pomerne veľké objemy dát a aby prenos dát a ich

uloženie bolo rýchle a kládlo minimálne nároky na skladovacie miesto, treba pred prenosom tieto dáta skomprimovať. Keď sú dáta prenesené, pred ich ďalším vstupom do technologického spracovania, je potreba dáta opäť dekomprimovať. Komprimácia a dekomprimácia spôsobuje určitú stratu kvality dekomprimovaného signálu. [3,6]

Techniky používané pre kompresiu dát závisia od druhu biometrického signálu, ktorý je spracovávaný. Na výskum, rozvoj a realizáciu komprimačných metód je kladená veľká vedecká pozornosť, aby boli nájdené metódy, ktoré minimálne ovplyvňujú kvalitu dekomprimovaných dát. [6]

Ak má byť biometrická aplikácia otvorená a dokázať si vymieňať dáta s ostatnými aplikáciami, musia byť komprimačné, dekomprimačné a prenosové pravidlá štandardizované tak, aby každá ďalšia aplikácia dokázala zrekonštruovať originálny biometrický vzor. [3,6]

3.4 Spracovanie nameraného signálu

Spracovanie biometrického signálu je možné formálne rozdeliť do troch častí: [3]

- extrakcia jedinečných biometrických charakteristík zo vzoru
- kontrola kvality
- vyhľadávanie v databáze porovnaním s ďalšími vzormi markantov

3.4.1 Extrakcia biometrických charakteristík

Prvou úlohou extrakcie biometrických charakteristík je získať všetky biometrické charakteristiky z dát nasnímaných senzormi, ktoré sú prenesené a dekomprimované k ďalšiemu spracovaniu. Pri daktyloskopickom odtlačku prsta je to umiestnenie a smer charakteristických bodov odtlačku.

Ďalším dôležitým cieľom je rozlíšenie jednoznačných a dostatočných identifikačných markantov a odfiltrovanie rušiacich vplyvov. [3,6]

Pre extrakciu biometrických charakteristík sa používajú najrôznejšie matematické postupy, ktoré sú neustále zdokonaľované. Extrakcia markantov je nezávislá na komprimačných a dekomprimačných postupoch a je vykonávaná z dekomprimovaného biometrického vzoru. Tento proces je spravidla automatizovaný a jeho cieľom je nájsť a definovať jednoznačné identifikačné charakteristiky. Extrakcia biometrických charakteristík používa špecifické metódy a postupy, ktoré sú výrobcami biometrických aplikácií úzkostlivo

utajované. Výsledkom tohto procesu je tzv. šablóna, pod ktorou si môžeme predstaviť minimálnu množinu bodov, ktoré úplne odrážajú jedinečnú identitu preverovaného jedinca a teda spĺňajú základné identifikačné podmienky – jedinečnosť, presnosť, časovú stálosť. Extrahovaná šablóna je matematickým vyjadrením fyzickej podstaty biometrického vzoru. So šablónami obvykle pracuje samotné porovnanie a vyhodnotenie biometrických charakteristík. [3,6]

Všeobecne je možné povedať, že extrakcia biometrických charakteristík má nevratný charakter. Z extrahovaných markantov nie je možné získať pôvodný obraz biometrického vzoru. Extrahované markanty majú totiž menší objem ako celý pôvodný vzor. V niektorých aplikáciách je preto extrakcia robená ihneď po snímaní biometrického vzoru a k ďalšiemu spracovaniu sa prenášajú len nízko-objemové šablóny. [6]

Z právneho a etického charakteru má extrakcia dôležitý význam. V databázach, ktoré slúžia k biometrickej identifikácií alebo verifikácií sú síce uložené biometrické šablóny, ale ako som práve uviedol, nie je z nich možné zrekonštruovať pôvodne nasnímaný biometrický vzor. K dispozícií máme teda šablónu – markantné body odtlačku prsta, ale nie je z nich možné zobraziť krivky papilárnych línií, ktoré nimi prechádzajú alebo sa ich dotýkajú. Týmto je zaručená ochrana súkromia osôb a osobných údajov. [3,6]

3.4.2 Kontrola kvality

Po procese extrakcie identifikačných charakteristík potrebujeme vedieť, či obdržaný biometrický vzor zo snímacieho senzoru je dostatočne kvalitný. Ak sú nasnímané charakteristiky akýmkoľvek spôsobom nedostatočné, konštatujeme, že biometrický vzor je nedostatočný a po snímacom zariadení požadujeme nový vzor, ktorý bude kvalitný.

Podobným spôsobom sa kontrola kvality realizuje pri súdno-policajných aplikáciách napr. pri prevode klasických daktyloskopických kariet do systému AFIS (Automated Fingerprint Information System). Papierové karty s odtlačkami všetkých desiatich prstov sú skenované do elektronickej podoby a kvalita výsledku je pribežne kontrolovaná a vyhodnocovaná obsluhujúcim personálom. [3,6]

3.4.3 Porovnávanie šablón

Extrahovaná šablóna s malými rozmermi je odoslaná do porovnávacieho procesu. Porovnanie prebieha medzi práve nasnímanou šablónou a šablónami, ktoré už boli

nasnímané do databáze uložených šablón. Prvé ukladanie takzvanej „referenčnej šablóny“ do databáze sa nazýva zavádzanie šablóny (enrolment template).

Porovnanie šablón slúži k stotožneniu práve načítanej šablóny snímacím podsystémom s jednou alebo viacerými šablónami, ktoré boli uložené v databázovom systéme. Šablóny uložené v databáze, môžu byť spojené s identitou známych osôb. Môžu to byť osoby s prístupovými právami do budovy, počítača, technologickej aplikácie a pod. v bezpečnostných aplikáciách. Osoba oprávnená k určitej činnosti má uloženú v databáze svoju referenčnú šablónu, ktorá sa zavádza do databáze ako prvá. O tom, či bude osoba prezentujúca svoje biometrické charakteristiky, uznaná ako oprávnená alebo neoprávnená, rozhoduje porovnanie s jej referenčnou šablónou. [6]

Policajno-súdne aplikácie majú v databáze uložené referenčné šablóny známych zločincov, delikventov a pod. S týmito evidovanými charakteristikami známych zločincov, napr. z iných prípadov, sa porovnávaním stotožňujú stopy neznámeho páchateľa z miesta trestného činu a tým sa identifikuje možný páchateľ. Opačným prípadom môže byť, keď sú v databáze uložené biometrické charakteristiky z dosiaľ neobjasnených prípadov. Biometrickému systému sú v procese snímania biometrického vzoru predkladaný potenciálny páchatelia. Porovnávacím procesom sa zisťuje, či sa biometrické charakteristiky potenciálnych páchateľov zhodujú s biometrickými charakteristikami zanechanými na mieste činu. [3,6]

3.5 Proces rozhodovania

Rozhodovací proces je ďalšou časťou spracovania biometrických údajov, v ktorom sa stanoví identifikačný záver. Na základe vypracovaných metód, algoritmov a merateľných charakteristík, sa stanoví miera zhody medzi šablónou predloženou a šablónou nájdenou. Tento proces je v bezpečnostno-komerčných aplikáciách automatizovaný. [3,6]

V policajno-súdnych aplikáciách stanovuje identifikačný záver vždy odborník, súdny znalec a pod. Na procese rozhodovania záleží, aký bude výsledok celého biometrického spracovania a všetky od neho sa odvíjajúce činnosti. Aplikácia musí byť odolná voči najrôznejším chybám a oprávnený užívateľ by mal mať vždy zaistené pozitívne vyhodnotenie. Nemal by byť odmietaný z dôvodu akejkoľvek technologickej chyby. V odbornej literatúre je tento stav nazývaný „falošné odmietnutie oprávneného užívateľa“, v anglickej terminológií označovaný „false rejection“. Neoprávnený užívateľ musí byť

naopak aplikáciou rozpoznaný a odmietnutý. Tu môže vzniknúť chyba, ktorá je nazývaná „falošné prijatie neoprávneného užívateľa“, v anglickej literatúre „false acceptance“. Aplikácia musí byť kalibrovaná na obidva typy chýb. [3]

Rozhodovací proces odpadá v prípade prvého zavádzania biometrickej šablóny do databáze. Vyhodnocuje sa tu len kvalita odňatého vzoru a preveruje sa, či sa už v systéme nenachádza. Cieľom je vylúčiť duplicitné referenčné šablóny. [3,6]

3.6 Uloženie dát

Uloženie dát je poslednou časťou spracovania dát každej biometrickej aplikácie. V závislosti na biometrickom systéme sa tu ukladá jedna alebo viac referenčných šablón. Referenčné šablóny sa ukladajú, aby bolo v budúcnosti možné rýchlo porovnať šablónu preverovanej osoby alebo stopy s týmito referenčnými údajmi. Porovnanie prebieha v podobe verifikácie alebo identifikácie. Pri verifikácií sa porovnáva jedna vstupná šablóna s jednou referenčnou šablónou, nazývané aj porovnanie jedna k jednej (one-to-one; 1:1). Pri identifikácií sa porovnáva jedna vstupná šablóna so všetkými uloženými referenčnými šablónami, nazývane porovnanie jedna k mnohým (one-to-many; 1:n). [3,6]

II. PRAKTICKÁ ČASŤ

4 OBLASTI VYUŽITIA SNÍMAČOV ODTLAČKOV PRSTOV

Snímače odtlačkov prstov sa využívajú v rôznych oblastiach. V administratívno-správnej sfére sa využívajú vo viacúčelových identifikačných kartách pre identifikáciu a verifikáciu obyvateľov, v komerčnej oblasti sa využívajú pre vstup osôb do chránených objektov a pridelenie konkrétnych práv osobe, ktorá má povolený vstup do chráneného objektu, pre prístup k výpočtovým a komunikačným prostriedkom. Ďalej sa v tejto oblasti používajú karty s biometrickým prvkom, ktoré sa v praxi využívajú vo finančnom sektore alebo v oblasti rôznych športových klubov a poslednou oblasťou, ktorá bude uvedená v nasledujúcich kapitolách je ochrana drahých alebo nebezpečných zariadení, technológií alebo majetku pred ich neoprávneným použitím alebo zneužitím za použitia daktyloskopického odtlačku a biometrického zabezpečovacieho prvku.

4.1 Využitie odtlačkov prstov v administratívno-správnej sfére

Prvé viacúčelové identifikačné karty, využívajúce biometrickú identifikáciu a verifikáciu (odtlačky prstov), boli celosvetovo implementované v Bruneji.

Do projektu je všeobecne zaintegrovaný register všetkých obyvateľov národa, aplikáciu AFIS (Automated Fingerprint Identification System) pre civilné využitie a čipové identifikačné karty z plastu, ktoré sú chránené vysoko kvalitnými ochrannými prvkami.

Register obyvateľov národa obsahuje identifikačné osobné údaje ako: meno a priezvisko, dátum a miesto narodenia, miesto trvalého pobytu a unikátne identifikačné číslo. V tomto registri je uložená aj fotografia v elektronickej podobe každej osoby, ktorá dovŕšila plnoletosť. AFIS, uchovávajúci odtlačky prstov držiteľov identifikačných kariet, je prepojený s centrálnym registrom obyvateľov. [3]

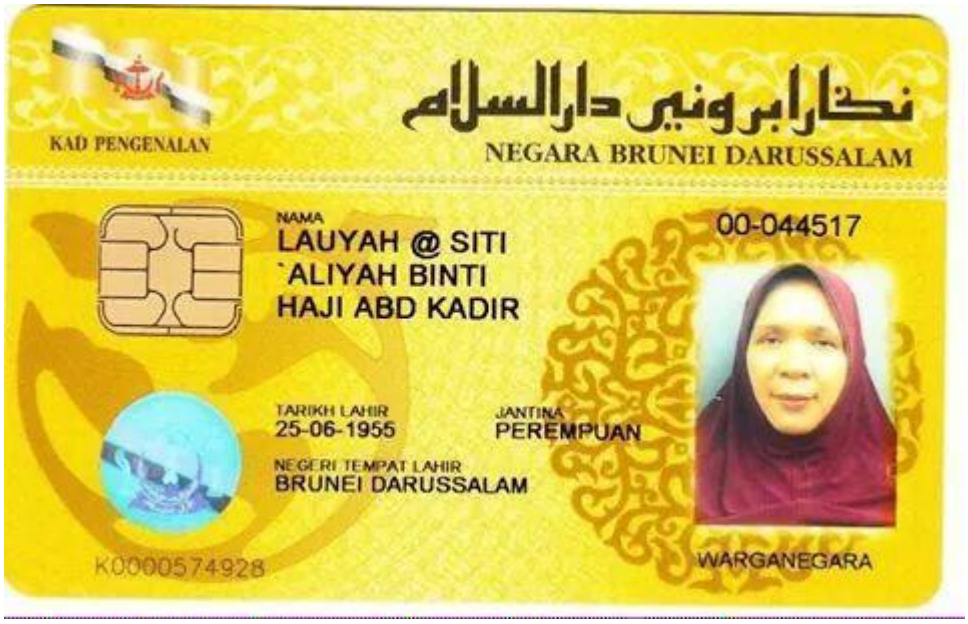
Obyvateľ žiadajúci o vydanie identifikačnej karty, je fyzicky preverovaný pomocou porovnania odtlačkov prstov a údajov uložených v AFIS. Vylúči sa tak neoprávnené vystavenie identifikačnej karty na základe sfalšovaných dokladov, rodnú listov osôb, ktoré sú už po smrti a pod. [3]

Na identifikačnú kartu je zaznačené iba meno a priezvisko, štátna príslušnosť, dátum narodenia a fotografia majiteľa (údaje, ktoré sa tak často nemenia). Všetky ostatné údaje sú uložené na čip. Takže pri zmene bydliska osoby sa iba prepíšu údaje na čipe a nie je potrebné meniť celý doklad. Ak štátny orgán potrebuje detailnejšie informácie, pomocou identifikačnej karty, slúžiacej ako primárny kľúč do systému registra obyvateľov, sa ku

konkrétnym detailným informáciám dostane. Na čipe tejto karty sú elektronicky uložené aj biometrické šablóny odtlačkov dvoch prstov a fotografia držiteľa. [3]

Identifikačná karta využíva elektronický podpis, je chránená privátnym a verejným kľúčom, RSA a DES šifrou a ďalšími modernými zabezpečovacími prvkami, ako UV značky, mikrotlač, giloše a hologram. Karta využíva biometrickú autentizáciu užívateľa – na základe porovnania odtlačku prsta. Biometrický prvok znemožňuje prenosnosť karty. Vyhodnocovacie zariadenie sa skladá z dvoch prvkov a to z čítačky karty a snímača daktyloskopického odtlačku prsta. Po zosnímaní odtlačku prsta sú porovnané biometrické šablóny živej osoby a šablóny načítané z identifikačnej karty. K bezpečnosti identifikácie osoby prispieva fakt, že porovnanie prebieha lokálne a teda žiadne osobné údaje nie sú prenášané sieťou. Umožňuje to aj rýchle rozmiestnenie vyhodnocovacích zariadení, ktoré v bežnej prevádzke nie sú závislé na centrálnych evidenciách. Tieto zariadenia môžu byť integrované do peňažných či platobných automatov, zariadení, ktoré regulujú prístup do objektu a pod. [3]

Voľný priestor, ktorý ostáva na čipe je možné využiť pre informácie o vodičskom preukaze, zdravotné a penzijné poistenie, pre políciu a pod. Identifikačná karta plne podporuje myšlienku tzv. e-government a e-commerce, čo v praxi znamená, že každý užívateľ karty má prístup ku orgánom a úradom štátnej správy. Identifikačná karta šetrí čas užívateľom aj štátnej správe, zjednodušuje a zefektívňuje identifikáciu osôb, zvyšuje komfort a popritom ešte zvyšuje bezpečnosť. [3]



Obrázok 12 Identifikačná karta [22]

4.2 Využitie daktyloskopickej identifikácie pre komerčné účely

Biometrické aplikácie, ktoré sú založené na vyhodnocovaní odtlačkov prstov, určené pre komerčné využitie majú oproti klasickým AFIS pre policajno-súdne účely svoje špecifiká. Tým prvým je fakt, že dochádza k porovnávaniu v pomere 1:1 alebo 1:N, kde N je veľmi malé číslo a používa sa označenie 1:*few*, čo znamená identifikáciu osôb z veľmi malého okruhu ľudí. Aplikácie AFIS slúžiace pre autentizáciu osôb, ktoré chcú získať prístup k chráneným objektom, nie sú tak veľké a nepotrebujú pracovať s miliónmi záznamov, ako je to v prípade aplikácií pre policajno-súdne účely. [3]

Druhým špecifikom je fakt, že po odňatí odtlačku výpočtový algoritmus sám určí, či žiadateľovi priradiť alebo odmietnuť prístupové práva do chráneného objektu. Pri neúspešnom porovnávaní má užívateľ ďalšiu možnosť zopakovať pokus. Nie je to práve užívateľsky príjemné, ale je to stále lepšie, ako pustiť neoprávneného užívateľa do chráneného objektu. Ďalším faktom je, že je vyvíjané úsilie o zníženie neúspešných pokusov oprávneného užívateľa. Snímacie a vyhodnocovacie zariadenia sú preto neustále zdokonaľované, aby splnili všetky vlastnosti, ktoré sa od nich očakávajú. [3]

Biometrické technológie odtlačkov prstov sa v praxi využívajú hlavne:

- pri autentizácií vstupu do fyzických objektov
- pri autentizácií osôb pre prístup ku komunikačným a výpočtovým prostriedkom
- ku zvýšeniu ochrany identifikačných, platobných alebo iných plastových kariet
- k ochrane drahých alebo nebezpečných zariadení, technológií alebo majetku pred neoprávneným použitím alebo zneužitím

Biometrické technológie sa neustále zdokonaľujú, vďaka čomu sa bude nepretržite zväčšovať aj oblasť ich praktického využitia. V ďalšom texte trochu podrobnejšie rozoberiem niektoré príklady. [3]

4.2.1 Autentizácia osôb pre prístup k výpočtovým a komunikačným prostriedkom

Je to najtypickejšia a najrozšírenejšia oblasť. Automatizované daktyloskopické porovnanie sa robí pomocou výpočtovej techniky a to nielen na bežných PC, ale aj pomocou jednoúčelových špecializovaných procesorov. Užívatelia PC pri svojej práci každodenne používajú klávesnicu a myš, ktorých sa dotýkajú končekmi svojich prstov a z tohto dôvodu nemajú obvyklé psychologické zábrany, dotýkať sa aj iných zariadení, v tomto prípade

snímacích daktyloskopických prvkov, slúžiacich ako vstupný prvok pre bezpečné prihlásenie užívateľa do počítača alebo iného zariadenia.

Užívatelia väčšinou pracujú s počítačmi v kancelárskom alebo domácom prostredí, kde je čisto. Je teda možné počítať s určitými hygienickými návykmi a z nich vyplývajúca čistota prstov, ktorá je predpokladom pre opakovanie daktyloskopického vyhodnocovania. Povrch snímača musí totiž ostať čistý, alebo musí byť jednoduché ho znova dostať do čistého stavu. [3,7]

Limitujúcim faktorom pre automatizované vyhodnotenie odtlačku je nepoškodený povrch končekov snímaných prstov. Osoby, ktoré pracujú s počítačmi, majú väčšiu pravdepodobnosť prijateľnej kvality odtlačkov ako osoby, ktoré pracujú fyzicky. Osoby vykonávajúce remeselnú profesiu majú kresbu papilárnych línií mechanicky vybrúsenú, zjazvenú alebo chemicky poškodenú, čo potom v niektorých prípadoch býva problematické pri snímaní a vyhodnocovaní pomocou automatizovaných technologických prvkov. Kvalita odtlačkov môže byť tiež u niektorých osôb ovplyvnená rôznymi ochoreniami kože, používaním liečivých alebo ochranných krémov a pod. Negatívne môžu byť aj stresové situácie, pri ktorých sa niektoré osoby viac potia, čoho výsledkom je tzv. mokrý odtlačok. [3,7]

Snímacie prvky sú integrované do klávesníc stolových počítačov, do korpusov notebookov alebo sú tiež vyrobené ako samostatné zariadenia, pripojiteľné na port počítača. Známe sú aj snímače integrované do klasických myší a na podobnom spôsobe je možné biometrickú identifikáciu integrovať aj do mobilných telefónov. [3,7]

Obrázok 13 Prvok pre snímanie odtlačku prsta [23]

4.2.2 Karty s biometrickým prvkom

Čip plastovej karty má v sebe uložené informácie v elektronickej podobe (napr. meno, priezvisko, dátum narodenia, číslo konta, sociálneho poistenia, fotografia držiteľa atď.) a zároveň je na čipe uložená biometrická šablóna držiteľa karty.

Pri preverovaní identity vsúva držiteľ kartu do čítacieho zariadenia a zároveň prikladá prst na snímací senzor. Vykoná sa porovnanie vzoru uloženého v čipe s práve odňatým odtlačkom a tým potvrdenie identity. Porovnanie je realizované na základe biometrických šablón. Týmto spôsobom je garantovaná personálna neprenosnosť karty. Výhoda, že biometrická šablóna je uložená v čipe je tá, že biometrické dáta nie je nutné prenášať sieťou a sú vyhodnocované v lokálnom zariadení. Z hľadiska bezpečnosti bývajú dáta v čipe aj tak šifrované. [3]

V praxi sa tieto karty používajúce biometrickú identifikáciu používajú v štátnom alebo finančnom sektore, ale aj v oblasti rôznych klubov, záujmových združení atď. Používajú sa všade tam, kde je potrebné zabezpečiť neprenosnosť karty. Karty s biometrickým prvkom sú vydávané aj niektorými leteckými spoločnosťami v spolupráci s pasovými orgánmi. Karta potom na letisku nahrádza štandardný pas. Pri kontrolných prepážkach je potom podstatne urýchlené odbavovanie pasažierov. V tomto príklade je veľmi dôležitý psychologický moment. Pasažier sám žiada o vydanie čipovej karty a tým súhlasí s budúcim preverovaním odtlačkov prstov, čo je podmienka získania výhody rýchleho prejdenia letiskovými kontrolami. [3]

Obrázok 14 Karta s biometrickým prvkom [24]

4.2.3 Autentizácia vstupu osôb do fyzických objektov

Identifikácia na základe daktyloskopického porovnania je podobná ako v prípade kontroly prístupu k počítačovým technológiám. Snímacie zariadenie spolu s ďalšími technologickými prvkami sú umiestnené do krytov, ktoré sú pripevnené na stenu v priestore dverí alebo dokonca do dverných kľučiek. Porovnanie býva obvykle nastavené na pomer 1:few (jeden k niekoľkým), pretože do niektorých objektov majú prístup aj desiatky oprávnených osôb. [3]

Zavedením čipovej karty alebo personálnym kódom (PIN) môže byť zvýšená bezpečnosť tejto biometrickej technológie. Pre potrebu druhej možnosti je v blízkosti snímacieho senzoru umiestnená malá mechanická klávesnica, umožňujúca zadávať PIN. [3]

Zadávanie PIN má dvojitý význam: [3]

- Bezpečnostný
  - Pri autentizácií je požadovaný ďalší doplnkový prvok k overeniu.
- Technologický
  - Keď je procesorovej jednotke známy PIN, prebieha iba verifikácia (porovnanie 1:1). Porovnáva sa jeden odňatý odtlačok s jedným vzorom, ktorý je jednoznačne určený pomocou PIN. V režime verifikácie je porovnávací proces veľmi urýchlený a realizovaný takmer v reálnom čase. V opačnom prípade sa realizuje porovnávací proces 1:n, ktorý je z hľadiska času na vyhodnotenie zdĺhavejší.

Vstupné zariadenia do objektov sú často spájané s ďalšími prvkami, umožňujúcimi evidovať a vyhodnocovať napríklad dochádzku, dobu strávenú v chránenom priestore atď. [3]

Obrázok 15 Biometrický zámkový systém [25]

4.2.4 Ochrana drahých alebo nebezpečných zariadení, technológií alebo majetku pred ich neoprávneným použitím alebo zneužitím

Ako ukážkový príklad si môžeme uviesť ochranu luxusného osobného automobilu pred jeho neoprávneným použitím. Aby mohol vodič vozidlo naštartovať, najskôr musí priložiť svoj prst ku snímaciemu senzoru a po pozitívnom vyhodnotení odtlačku je vozidlo pripravené vykonávať ďalšie funkcie. V pamäti procesorovej jednotky môže byť uložené odtlačky prstov viacerých osôb, oprávnených používať vozidlo. . [3,7]

Obdobne je možné chrániť akékoľvek ďalšie technologické zariadenia. V súčasnej dobe je vedený vývoj miniatúrnych, odolných a spoľahlivých komponentov, ktoré bude možné integrovať ako ochranné prvky do osobných strelných zbraní, pričom sa zabráni veľkému množstvu zbytočných úmrtí spôsobených neoprávnenou manipuláciou so zbraňou. Tým je zároveň znemožnené, aby ktokoľvek použil zbraň proti jej vlastníkovi. Umiestnenie daktyloskopického snímacieho senzoru je predpokladané na puzdre zbrane, alebo pri vysokom stupni miniaturizácie v okolí spúšte zbrane. [3,7]

5 NOVÉ TRENDY

V tejto poslednej kapitole, ktorá sa bude venovať novým trendom v oblasti použitia snímačov odtlačkov prstov budú uvedené snímače odtlačkov prstov, ktoré sú zabudované do samotných displejov zariadení, snímače zabudované do mobilných telefónov pre zabezpečenie prístupu k obsahu telefónu a platby pomocou odtlačkov prstov.

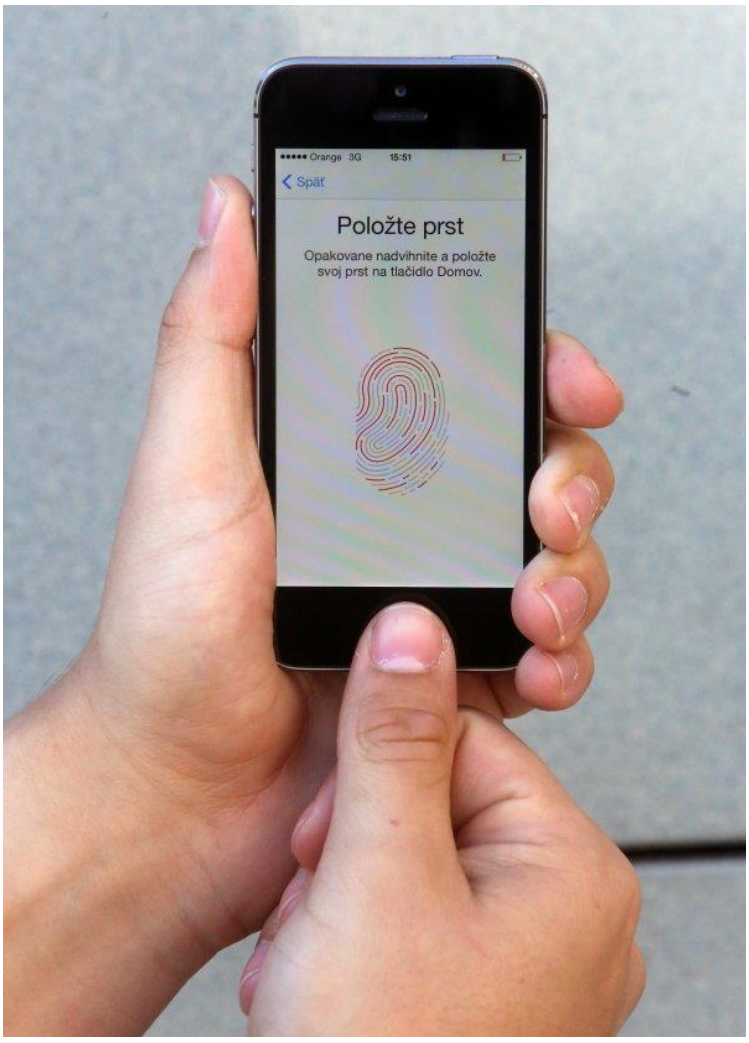
5.1 Snímače odtlačkov prstov zabudované v displejoch

Technológiu, ktorá umožňuje zabudovať snímač odtlačkov prstov priamo do zariadenia si nechala patentovať Kórejská biometrická spoločnosť CrucialTek. Výrobcovia tým pádom nemusia umiestňovať skener samostatne, prípadne ho riešiť iným spôsobom ako je napríklad zabudovanie do tlačidiel. Táto technológia by mala pomôcť šetriť miesto, prípadne ho využiť efektívnejšie. Na uvedenie prvého zariadenia so zabudovaným snímačom odtlačkov v displeji si bude ešte treba pár mesiacov počkať. Prvým zariadením tejto novej technológie by mal byť mobilný telefón spomínanej Kórejskej biometrickej spoločnosti. Telefón by mal mať unikátne špecifikácie, vrátane snímača odtlačkov prstov, ktorý by nemal byť zabudovaný v tlačidle, ale v samotnom displeji. Podobnú technológiu si dal patentovať aj známy výrobca Apple a je len otázkou času, kedy sa táto technológia objaví aj v mobilných telefónoch iPhone. Nový iPhone by tak mohol ponúknuť väčší displej v rámci rovnakého tela telefónu, avšak na úkor toho že by sa vzdal svojho hardvérového tlačidla.[8]

5.2 Snímač odtlačkov prstov v mobilnom telefóne iPhone

V predchádzajúcej podkapitole bolo už spomínané hardvérové tlačidlo mobilného telefónu iPhone. Toto tlačidlo má v sebe zabudovaný senzor nazývaný „*Touch ID*“, ktorý predstavuje jednoduchý spôsob používania odtlačku prsta namiesto hesla, pretože odtlačok prsta je jedným z najlepších hesiel na celom svete. Nachádza sa totiž stále pri svojom majiteľovi a neexistuje žiadny taký, ktorý by bol rovnaký. Postačuje jediný dotyk a senzor „*Touch ID*“ prečíta odtlačok prsta a automaticky odomkne zariadenie. Za pomoci tohto senzoru je dokonca možné autorizovať nákupy v obchodoch iTunes Store, App Store či iBooks Store a pomocou systému Apple Pay aj nákupy. Táto technológia, ktorá sa skrýva v senzore „*Touch ID*“ je asi tým najpokročilejším hardvérom a softvérom aké boli kedy vložené do mobilných zariadení. Hardvérové tlačidlo je vyrobené zo zafírového kryštálu, ktorý je jedným z najčistejších a najtvrdších materiálov. Zafírový kryštál chráni

senzor a súčasne funguje ako šošovka umožňujúca presné zaostrenie na prst. Na zistenie prstu slúži oceľový prstenec, ktorý dáva senzoru „*Touch ID*“ pokyn pre začatie snímania odtlačku. Pomocou pokročilej kapacitnej dotykovej technológie je vytvorený obraz s vysokým rozlíšením, zaznamenávajúci malé časti odtlačku prsta. „*Tocuh ID*“ následne analyzuje informácie pozoruhodne detailne a presne. Mapované sú aj jednotlivé detaily v brázdach, ktoré sú tak malé, že ich nie je možné vidieť voľným okom. Kontrolované sú dokonca aj drobné odchýlky v smere brázd, spôsobené štruktúrami okrajov a pórmi. „*Touch ID*“ je schopný prečítať viaceré odtlačky prstov s 360-stupňovou orientáciou a následne vytvára matematické vyjadrenie odtlačku prsta, ktorý porovnáva s údajmi zaregistrovaného odtlačku, na základe čoho identifikuje zhodu a odomyká zariadenie. Senzor pridáva do údajov registrovaného odtlačku nové časti odtlačku, čím postupne zvyšuje presnosť rozpoznávania a pomocou všetkých týchto údajov hľadá presnú zhodu a dosahuje veľmi vysokú úroveň zabezpečenia. [9]



Obrázok 16 Snímač odtlačku prsta – iPhone [26]

5.3 Snímač odtlačkov prstov v mobilnom telefóne Samsung Galaxy S6

Podobný dotykový snímač odtlačku prsta, ktorý používa výrobca mobilného zariadenia iPhone mieri do novo pripravovaného modelu mobilného zariadenia výrobcu Samsung, ako uviedol server SamMobile. Senzor tohto nového modelu bude mať väčšiu snímaciu plochu, čím sa predpokladá nárast hlavného tlačidla pod displejom, v ktorom bude snímač integrovaný. Predchádzajúci typ mobilného zariadenia od spomínaného výrobcu má hlavné tlačidlo príliš úzke, čím je poskytnutá malá snímacia plocha a to sa odráža v nižšej spoľahlivosti snímania. Pre úspešné rozpoznanie odtlačkov je často nutné prechádzať opakovane cez snímač. Typ snímača spolu s väčším hlavným tlačidlom v novom type mobilného zariadenia by mal eliminovať uvedené mínusy. Nový typ snímača by okrem funkcie odomknutia telefónu mohol nahradiť aj zadávanie hesiel v rozličných službách Samsungu, zadávanie hesiel na webových stránkach a dokonca by mohol umožniť platbu cez platobný systém PayPal. [10]

Obrázok 17 Snímač odtlačku prsta – Samsung Galaxy S6 [27]

5.4 Platby potvrdzované odtlačkami prstov

Marcel Gajdoš, regionálny manažér Visa Europe pre Českú republiku a Slovensko hovorí: *„Keďže očakávame, že všetky platobné terminály budú do konca roka 2017 bezkontaktné, tak pomocou biometrie bude technicky možné zaplatiť viac-menej kdekoľvek. Nové mobilné zariadenia, ako napríklad iPhone alebo Samsung Galaxy S5, už dokonca majú zabudované*

snímače na odtlačok prstov a je teda možné takto autorizovať bezkontaktné transakcie na termináli. Dá sa očakávať, že biometrické senzory začnú byť štandardnou súčasťou nových smart zariadení ako sú mobily, hodinky a rôzne náramky a autorizáciou platieb biometriou vďaka svojej bezpečnosti a jednoduchosti postupne nahradia autorizáciu PINom." [11]

Zo všetkých nových platobných metód, ktoré sú už spotrebiteľom dostupné, generácia „Z“ (vo veku od 16 do 24 rokov) inklinuje k verifikácii prostredníctvom skenovania odtlačkov prstov. [11]

ZÁVER

Cieľom bakalárskej práce bolo rozobrať problematiku snímania odtlačkov prstov v oblasti bezpečnosti. Práca je rozdelená na teoretickú a praktickú časť. V úvode teoretickej časti boli opísané jednotlivé pojmy ako biometria, čím sa tento vedný odbor zaoberá a na základe akých rysov prebieha rozpoznávanie ľudských jedincov, odtlačok prsta a jeho charakteristika, čo znamenajú pojmy identifikácia a verifikácia, pre aké aplikácie sú tieto činnosti typické a aký je medzi nimi rozdiel a v poslednej časti kapitoly boli uvedené chyby, ktoré môžu vzniknúť pri snímaní odtlačkov prstov, aká je pravdepodobnosť ich vzniku a ako je možné túto pravdepodobnosť vypočítať. V druhej kapitole teoretickej časti boli opísané jednotlivé typy snímačov odtlačkov prstov, ich klasifikácia podľa kategórie, do ktorej zapadajú, boli opísané fyzikálne princípy na ktorých sú založené a na ktorých pracujú. V tretej kapitole bolo popísané spracovanie dát zo snímačov odtlačkov prstov, boli uvedené doplňujúce biometrické pojmy ako biometrický vzor, čoho je odrazom, biometrické charakteristiky a z čoho sa získavajú, biometrické markanty, na čo sú potrebné a kde ich je možné nájsť, biometrická šablóna, čoho je výsledkom, kde sa ukladá a aká je jej veľkosť. Ďalej bol v tretej kapitole popísaný spôsob zberu dát, čo musí biometrická aplikácia spĺňať aby bola schopná vymieňať si svoje údaje s inou aplikáciou, prenos dát a čo je potrebné vykonať pred prenosom dát a po ich prenose, spracovanie signálu a jeho formálne delenie na extrakciu jedinečných biometrických charakteristík zo vzoru, kontrolu kvality a vyhľadávanie v databáze porovnaním s ďalšími vzormi markantov, čo jednotlivé formálne časti obsahujú a čo je ich úlohou, proces rozhodovania, čo je v ňom potrebné stanoviť a spôsob uloženia dát. V úvode praktickej časti boli uvedené a popísané jednotlivé oblasti využitia snímačov odtlačkov prstov. Bola popísaná oblasť administratívno-správnej sféry a využitie identifikačných kariet pre identifikáciu a verifikáciu obyvateľov, v komerčnej oblasti využitie snímačov odtlačkov prstov pre vstup osôb do chránených objektov a pridelenie im konkrétnych vopred určených práv a prístup k výpočtovým a komunikačným prostriedkom. Ďalej boli popísané oblasti, v ktorých sa využívajú karty s biometrickým prvkom a poslednou uvedenou oblasťou bola ochrana drahých alebo nebezpečných zariadení, technológií alebo majetku pred ich neoprávneným použitím alebo zneužitím. V závere praktickej časti boli uvedené nové trendy využitia snímačov odtlačkov prstov a bol vysvetlený stručný princíp ich fungovania.

ZOZNAM POUŽITEJ LITERATÚRY

[1] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. Brno: Computer Press, 2011, 294 s. ISBN 9788025489796

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV.: teorie a praxe ochrany majetku a fyzické bezpečnosti*. 1. vyd. Zlín: VeRBuM, 2014, 390 s. ISBN 978-80-87500-57-6.

[3] 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. obr. příl. Profesionál. ISBN 978-80-247-2365-5.

[4] CHIRILLO, John a Scott BLAUL. *Implementing biometric security*. Indianapolis, IN: Wiley Pub., 2003, xvii, 414 p. ISBN 0764525026.

[5] BOLLE, Ruud. *Guide to biometrics*. New York: Springer, c2004, xxix, 364 p. ISBN 0387400893.

[6] ASHBOURN, Julian. *Practical biometrics: from aspiration to implementation*. New York: Springer, c2004, xiv, 159 p. ISBN 1852337745.

[7] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902938-2-4.

[8] *TouchIT* [online]. [cit. 2015-06-02]. Dostupné z: http://touchit.sk/skenery-odtlackov-prstov-budu-coskoro-zabudovane-priamo-v-displejoch/1612

[9] *Zabezpečenie pomocou senzora Touch ID v iPhone a iPade* [online]. [cit. 2015-06-02]. Dostupné z: https://support.apple.com/sk-sk/HT5949

[10] *Nový Samsung Galaxy S6 bude snímať odtlačky prstov ako iPhone* [online]. [cit. 2015-06-02]. Dostupné z: http://style.hnonline.sk/digital-132/novy-samsung-galaxy-s6-bude-snimat-odtlacky-prstov-ako-iphone-642384

[11] *Generácia Z chce platby potvrdzovať odtlačkami prstov* [online]. [cit. 2015-06-02]. Dostupné z: http://www.retailmagazin.sk/spotrebitel/prieskumy/533-generacia-z-chce-platby-potvrdzovat-odtlackami-prstov

[12] *FINGERPRINT RECOGNITION ROBOT* [online]. [cit. 2015-06-02]. Dostupné z: http://students.iitk.ac.in/projects/roboticsclub/fingerprint

[13] *Fingerprint sensing techniques* [online]. [cit. 2015-06-02]. Dostupné z: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.htm

[14] *Biometrické metody pro aplikace v biomedicíně* [online]. [cit. 2015-06-02]. Dostupné z: http://www.ejbi.org/img/ejbi/2011/1/Schlenker_cs.pdf

[15] KONČICKÝ, Martin. *Biometrický snímač otisku prstů*. Zlín, 2013. Bakalárska práca. UTB ve Zlíně. Vedoucí práce Ing. Rudolf Drga.

[16] *Biometrics Brings High Technology To The Identification Game* [online]. [cit. 2015-06-02]. Dostupné z: http://electronicdesign.com/archive/biometrics-brings-high-technology-identification-game

[17] *Co je to FingerChip®* [online]. [cit. 2015-06-02]. Dostupné z: http://www.hw.cz/teorie-a-praxe/co-je-to-fingerchipr.html

[18] *BerkeLana Di dUnia mayA* [online]. [cit. 2015-06-02]. Dostupné z: http://berkelanadiduniamaya.blogspot.sk/2011/08/4-sistem-pembacaan-sensor-sidik-jari.html

[19] *INTELLICHECK MOBILISA, INC. (IDN) SPO* [online]. [cit. 2015-06-02]. Dostupné z: http://www.nasdaq.com/markets/spos/company/intellicheck-mobilisa-inc-6340-77278

[20] *Biometric* [online]. [cit. 2015-06-02]. Dostupné z: http://www.methode.com/sensors-and-switches/biometric.html#.VW2DKkbj8WE

[21] *A Tutorial on Fingerprint Recognition* [online]. In: . [cit. 2015-06-02]. Dostupné z: http://www.cedar.buffalo.edu/~govind/CSE666/fall2007/FP_Tutorial.pdf

[22] *Nigeria launches new biometric ID card - brought to you by Mastercard* [online]. [cit. 2015-06-02]. Dostupné z: http://www.redicecreations.com/article.php?id=31569

[23] *Nové myši i klávesnice od Microsoftu vrátane snímania odtlačkov prstov* [online]. [cit. 2015-06-02]. Dostupné z: http://www.zive.sk/clanok/17187/nove-mysi-i-klavesnice-od-microsoftu-vratane-snimania-odtlackov-prstov

[24] *Biometrické systémy v praxi* [online]. [cit. 2015-06-02]. Dostupné z: http://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[25] *Kam směřuje biometrie* [online]. [cit. 2015-06-02]. Dostupné z: http://www.ceskestavby.cz/clanky/kam-smeruje-biometrie-21323.html

[26] *Najlepší Samsung bude skenovať odtlačky prstov ako iPhone* [online]. [cit. 2015-06-02]. Dostupné z: http://style.hnonline.sk/digital-132/najlepsi-samsung-bude-skenovat-odtlacky-prstov-ako-iphone-605600

[27] *Android M bude natívne podporovať snímače odtlačkov prstov* [online]. [cit. 2015-06-02]. Dostupné z: http://www.pda.sk/2015/05/android-bude-udajne-nativne-podporovat-snimace-odtlackov-prstov/

ZOZNAM OBRÁZKOV