BIOMETRICKÉ ZABEZPEČENIE DÁT V BIOMEDICÍNE

Anna Horňáková, Milan Šárek

Anotácia

Táto práca analyzuje súčasný stav využitia biometrie v počítačovej bezpečnosti. Ponúka prehľad najčastejšie používaných anatomicko-fyziologických a behaviorálnych biometrických identifikačných metód. Výsledkom práce by mal byť nový komplex metód, ktorý umožní spoľahlivú identifikáciu užívateľa čo najkomfortnejšou formou. Výsledná aplikácia nových princípov zabezpečenia bude použitá pre zvýšenie ochrany špecializovaného zdravotného záznamu. Ďalej dôjde k rozšíreniu obecne pojatého konceptu EHR MUDR do ďalšej aplikačnej oblasti.

Kľúčové slová

Biometria, Bezpečnosť dát, DLP (Data Loss Prevention), ERPI (Electronic Record Personal Identification), EHR (Electronic Health Record)

1. Úvod

Biometria, biometrická identifikácia a verifikácia boli predmetom výskumu už od začiatku 80-tych rokov minulého storočia. Na konci 20-teho storočia sa začali nasadzovať prvé aplikácie a to hlavne v kriminalistickej praxi, kde sa jednalo o automatizované spracovanie odtlačkov prstov a dlaní nájdených na mieste trestného činu. V súčasnosti majú biometrické metódy nezastupiteľnú úlohu ako vo forenzných vedách, tak aj v komerčne využiteľných aplikáciách.

V tejto práci analyzujeme súčasný stav využitia biometrie v počítačovej bezpečnosti, hlavne možnosti využitia identifikácie na základe biometrických údajov. Biometrické charakteristiky môžeme rozdeliť na anatomicko-fyziologické a behaviorálne.

2. Anatomicko-fyziologické biometrické charakteristiky

Medzi najčastejšie používané anatomicko-fyziologické biometrické identifikačné charakteristiky v bežnej praxi patria napríklad odtlačky prstov a dlaní, geometria tvaru ruky a snímanie krvného riečiska dlane alebo chrbta ruky.

2.1 Odtlačky prstov a dlaní

Odtlačky prstov a dlaní sú založené na unikátnosti obrazcov papilárnych línií. Miniaturizácia snímacích prvkov aj špeciálnych procesorov umožnila rozšírenie využitia biometrickej identifikácie založenej na daktyloskopických poznatkoch aj pre široké komerčné využitie.

V komerčnej sfére prebieha vyhodnocovanie odtlačkov prstov trošku inak ako v kriminalistike. Jedná sa hlavne o dva rozdiely. Prvým je to, že prebieha buď verifikácia, tj. porovnávanie 1:1, alebo porovnávanie 1:N, kde N je veľmi malé číslo na rozdiel od rozsiahlych databáz v kriminalistike. Druhým rozdielom je to, že algoritmus sám vyslovuje záverečný verdikt, tj. povoliť alebo zamietnuť

prístup danému užívateľovi. Ak je porovnanie neúspešné, žiadateľ má možnosť pokus opakovať.

Medzi typické príklady použitia biometrických aplikácií v praxi patrí autentizácia osôb pre prístup k výpočtovým a komunikačným prostriedkom, na zvýšenie ochrany identifikačných alebo platobných kariet, pri autentizácii vstupu do objektov alebo pri ochrane drahých alebo nebezpečných zariadení pred ich neoprávneným použitím.

Pri počítačovom spracovaní odtlačkov prstov pre komerčné bezpečnostné účely môžeme rozlíšiť tri technologické fázy [9]:

1. snímanie odtlačku prsta (najrôznejšie technológie pre načítanie biometrických dát a ich prevod do elektronickej formy),
2. počítačové spracovanie odtlačku prsta (technologické postupy pre odstránenie šumu, nájdenie charakteristických znakov a vznik šablón, algoritmy pre porovnávanie načítaných a uložených biometrických šablón) a
3. záverečné vyhodnotenie (formulácia výsledku porovnania, tj. verifikácia, autentizácia či identifikácia).

Snímanie daktyloskopických odtlačkov sa dá rozdeliť do dvoch základných skupín, na klasické a bezprostredné.

Klasické snímanie daktyloskopických stôp sa používa hlavne v kriminalistike a tak sa mu nebudeme podrobne venovať. Jedná sa o snímanie odtlačkov pomocou tlačiarenskej černej farby a daktyloskopickej karty. Tá sa potom naskenuje a uloží v elektronickej podobe.

Pre aplikácie komerčne-bezpečnostného charakteru je dnes bežnejšie používanie bezprostredného snímania daktyloskopických odtlačkov. Pod týmto pojmom rozumieme snímanie odtlačkov z prikladaných prstov alebo dlaní živých a bezprostredne prítomných osôb k snímaču (senzoru).

Interaktívne snímanie odtlačkov prstov, ktoré je dnes často implementované do najrôznejších technických zariadení, je realizované pomocou senzorov. Tieto senzory môžu byť kontaktné alebo bezkontaktné a môžu pracovať na rôznych fyzikálnych princípoch [2].

2.1.1 Kontaktné senzory na snímanie odtlačkov prstov

Medzi kontaktné senzory patria senzory optické, elektronické, optoelektronické, kapacitné, tlakové a teplotné. Niektorým typom týchto senzorov sa budeme v nasledujúcom texte venovať podrobnejšie.

2.1.1.1 Optické kontaktné senzory

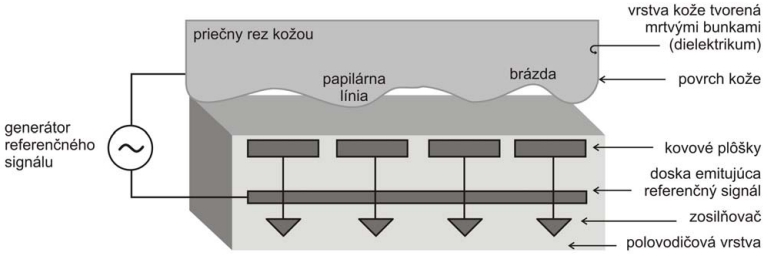
Optické senzory pracujú na technológii FTIR (Frustrated Total Internal Reflection). Táto technológia funguje na princípe, že laserový lúč zospodu osvetľuje povrch prsta ktorý sa dotýka priehľadnej dosky senzora. Odrážaný svetelný tok je snímaný CCD (Charge-Coupled Device) prvkom. Množstvo odrazeného svetla závisí od hĺbky papilárnych línií a brázd (výstupky a zárezy na prste alebo dlani). Papilárne línie odrážajú svetlo viac, brázdy menej.

Iné optické snímače využívajú hustý zväzok optických vlákien, ktoré sú

postavené kolmo k rovine snímacej plochy senzora. Tu sa opäť uplatňuje metóda osvitu a odrazu svetelného toku. Ďalším typom sú potom senzory využívajúce technológiu CMOS (Complementary Metal–Oxide–Semiconductor).

2.1.1.2 Elektronické kontaktné senzory

Elektronické senzory pracujú na princípe vzniku elektrického poľa medzi dvoma paralelnými vodivými a elektricky nabitými doskami (Obrázek 1). Ak zmeníme pôvodne plochý tvar hornej dosky na vlnitý (tvorený povrchom daktyloskopických papilár a brázd) zmení sa aj tvar elektrického poľa, ktorý je na ňom závislý. Hornú dosku elektronického senzora tvorí povrch kože, do ktorého sa púšťa riadiaci elektrický signál.



Obrázek 1 – Schéma princípu elektronického senzora (podľa [8])

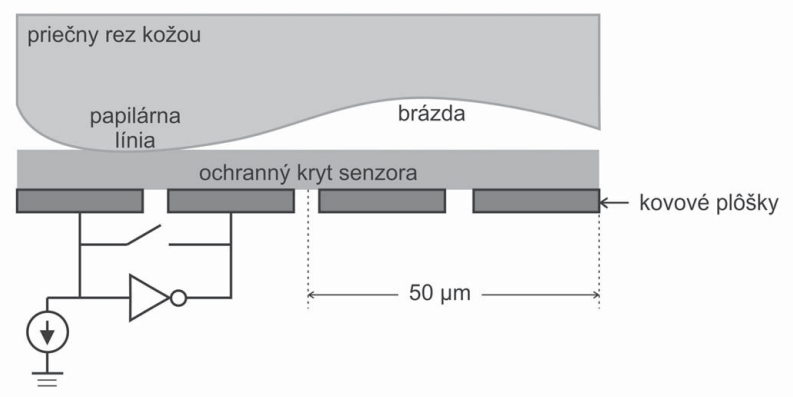
Výhodou tohto senzora je to, že nesníma len povrch kože ale preniká hlbšie pod povrch. Tým sa stáva odolný voči znečisteniu alebo poškodeniu povrchu kože.

2.1.1.3 Optoelektronické kontaktné senzory

Optoelektronické senzory sa skladajú z dvoch základných vrstiev. Horná vrstva je v kontakte s kožou a je schopná emitovať svetlo. To je zachytené v druhej sklenenej vrstve do ktorej sú zatavené fotodiódy. Tie potom transformujú svetelný impulz na elektrický.

2.1.1.4 Kapacitné kontaktné senzory

Kapacitné senzory snímajú odtlačok prsta pomocou merania elektrickej kapacity (Obrázek 2). Snímací senzor je zložený z veľkého množstva snímacích plôch, ktoré sú od seba odizolované. Dotykom kože papilárne línie premosťujú jednotlivé vodivé plôšky v závislosti na papilárnej kresbe a brázdy sa chovajú ako izolant. Meria sa napätie a kapacitné úbytky medzi jednotlivými vodivými plôškami. Tak vzniká digitalizovaný obraz papilárnej kresby. Tieto senzory sú veľmi náchylné na rôzne druhy znečistenia, ktoré môžu podstatne meniť vodivosť kože.



Obrázek 2 – Schéma princípu kapacitného senzora (podľa [8])

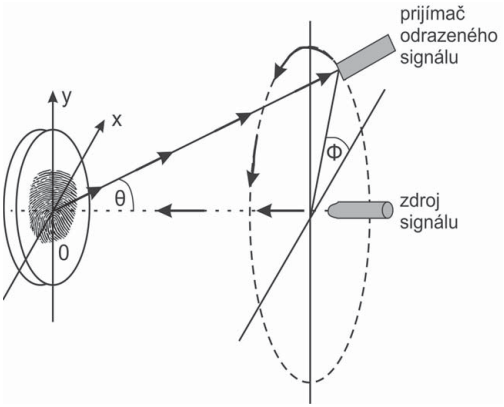
2.1.1.5 Tlakové kontaktné senzory
Tlakové senzory reagujú na tlak papilárnych línií na povrchu snímacieho senzora. Povrch senzora je tvorený elastickým piezoelektrickým materiálom, ktorý tlak transformuje na elektrický signál a vytvára tak daktyloskopický obraz.

2.1.1.6 Teplotné kontaktné senzory
Teplotné senzory reagujú na teplotné rozdiely medzi papilárnymi líniami a brázdami. Veľkou výhodou tohto senzora je to, že teplota je dôležitým faktorom, ktorý môže napovedať, či snímaný odtlačok patrí živej osobe.

2.1.2 Bezkontaktné senzory na snímanie odtlačkov prstov
K najznámejším skupinám bezkontaktných senzorov patria optické a ultrazvukové.

2.1.2.1 Optické bezkontaktné senzory
Pri optických senzoroch je princíp práce podobný dotykovým optickým senzorom iba s tým rozdielom, že svetelný lúč umožňuje snímať daktyloskopický odtlačok zo vzdialenosti 3 až 5 cm. Najväčšou prednosťou tohto snímača je to, že zabraňuje jeho znečisteniu v dôsledku dotyku špinavými prstami.

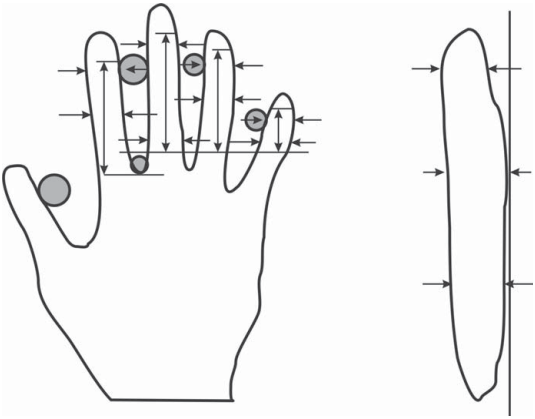
2.1.2.2 Ultrazvukové bezkontaktné senzory
Ultrazvukové senzory sú tiež založené na princípe podobnom optickým, akurát na povrch kože dopadá namiesto svetelného lúča zväzok krátkych vĺn (Obrázek 3). Tento typ senzora odstraňuje všetky nedostatky uvedené pri predchádzajúcich typoch senzorov [1].



Obrázek 3 – Schéma princípu práce ultrazvukového senzora (podľa [8])2.2.

Geometria tvaru ruky

Ďalšou často používanou metódou je geometria tvaru ruky, ktorej podstatou je meranie dĺžok alebo šírok prstov, kostí alebo kĺbov ruky (Obrázek 4). Táto metóda bola prvou, ktorá bola použitá na počítačovú verifikáciu pre komerčné účely. Moderné trojrozmerné skenery snímajú geometrické charakteristiky v desiatkach bodov za sekundu. Ruka sa prikladá na horizontálnu plochu skenera, ktorá má špeciálne fixačné kolíčky, aby bola ruka priložená vždy v rovnakej polohe. Skener sníma jeden obraz zhora kolmo na rovinu snímacej dosky a druhý z boku. Vzniknú dva čiernobiele snímky „siluety" ruky.



Obrázek 4 – Základný princíp metódy geometrie ruky (podľa [8])

Užívateľ, ktorý požaduje potvrdenie svojej identity, zadá najprv svoj identifikačný kód (PIN) na klávesnici, alebo priloží na čítačku magnetický prúžok, čip alebo čiarový kód ID karty. Následne priloží ruku na stanovenú pozíciu podľa vizuálneho návodu, ktorý je na každej klávesnici [5]. Skenery geometrie ruky sú dnes už bežné v mnohých oblastiach vrátane zdravotníctva.

2.3 Snímanie krvného riečiska dlane alebo chrbta ruky

Ďalšou metódou podobnou snímaniu geometrie ruky a vhodnou pre použitie v počítačovej bezpečnosti je snímanie krvného riečiska dlane alebo chrbta ruky. Pri tejto metóde sa pomocou CCD kamier sníma špecifický obraz ciev na povrchu ruky. Jedná sa o snímanie celkového plošného obrazu rozloženia všetkých ciev v blízkosti povrchu chrbta ruky.

Nespornou výhodou tejto metódy je to, že zároveň overuje, či je preverovaný objekt živý. Snímanie totiž prebieha v infračervenom pásme ktoré je citlivé na teplotu. Cievy sú v tele teplejšie než ich okolie. Ďalšie spracovanie nasnímaného obrazu je už potom podobné ako pri odtlačku prsta (porovnávajú sa tvary ciev). Ďalšou výhodou oproti snímaniu geometrie ruky je to, že nie je nutné ruku prikladať vždy v tej istej polohe.

Ďalšími možnosťami u tejto metódy je snímanie krvného riečiska dlane, alebo bezkontaktné snímanie (ako dlane tak aj chrbta ruky), ktoré zaisťuje vysokú hygienickú čistotu na rozdiel od snímania geometrie ruky alebo kontaktného snímania odtlačkov prstov [5].

2.4 Rozpoznávanie tváre a jej častí

Namiesto ruky môže na identifikáciu človeka poslúžiť napríklad aj jeho tvár alebo jej časť. Existujú počítačové programy, ktoré dokážu rozpoznávať ľudské tváre podobne ako človek. Rozpoznávanie tvárí je v súčasnosti typické najmä pre kriminalistiku a existuje mnoho rôznych metód a algoritmov, ktoré sa pre tieto účely používajú.

Veľmi jednoduché môže byť však aj použitie pri zabezpečovaní bežných výpočtových a telekomunikačných systémov. Na nasnímanie obrazu tváre postačuje bežná videokamera, ktorú má mnoho obrazoviek už integrovanú do seba. Takto je vlastne klasické zadávanie hesla nahradené nasnímaním tváre. Tento postup je veľmi výhodný z hľadiska toho, že nie je potrebný vôbec žiadny priamy kontakt užívateľa so snímačom [10].

V tejto oblasti však určite výskum nie je na konci. Rozpoznávanie tváre sa dá ešte v mnohých smeroch zdokonaľovať. Ako príklad sa dajú uviesť prejavy rôznych emócií.

Zaujímavou aplikáciou s ohľadom na kontrolu bezpečnosti v IT by bolo určite priebežné snímanie tváre človeka pri práci na počítači a vyhodnocovanie, či s citlivými dátami pracuje stále tá istá oprávnená osoba. Iným príkladom by mohlo byť zaznamenávanie tvárí všetkých, ktorý sa do daného systému nie len

dostali ale s ním aj pracovali. (Niekto môže nechať otvorenú aplikáciu a na malú chvíľku odísť, čoho môže využiť nepovolaná osoba.)

2.5 Snímanie očnej dúhovky alebo sietnice

V poslednej dobe sa vďaka jednoduchému použitiu bežných videosystémov stáva čoraz viac rozšírenou metódou aj snímanie očnej dúhovky alebo sietnice. Rozpoznávanie dúhovky je možné bez ohľadu na veľkosť, umiestnenie a orientáciu ale je na to potrebný zložitý algoritmus. Táto aplikácia sa zatiaľ používa väčšinou len na zaistenie vysokej úrovne bezpečnosti [5].

Na zmapovanie krvného riečiska očnej sietnice sa používa svetelný lúč, ktorého časť sietnica pohltí a časť odrazí. Špeciálna kamera potrebná na snímanie je pomerne drahá a samotné snímanie nie je pre užívateľa príjemné (mnoho ľudí sa tejto technológie dokonca bojí) [5].

3. Behaviorálne biometrické charakteristiky

Pre využitie v počítačovej bezpečnosti by mohla byť zaujímavá aj jedna behaviorálna biometrická charakteristika, ktorá ešte nie je bežne používaná, a to dynamika stisku počítačových kláves.

3.1 Dynamika stláčania počítačových klávesov

Dynamika stláčania počítačových klávesov umožňuje takzvanú kontinuálnu (dynamickú) verifikáciu, ktorá vychádza z použitia klávesnice ako prostriedku neustálej interakcie užívateľa a počítača. To ponúka možnosť priebežnej kontroly v priebehu celej práce s počítačom. Možnosti použitia sú hlavne tam, kde hrozí riziko zneužitia na chvíľu opusteného počítača [3].

Najbežnejšie zisťovanou charakteristikou je čas stlačenia jednotlivých klávesov alebo doba trvania stlačenia jednotlivého klávesu. Ďalšími možnými prístupmi je zisťovanie celkovej rýchlosti písania, frekvencia chýb, štýl písania veľkých písmen alebo sila použitá na stlačenie klávesu. Na posledný zmienený typ je už potrebná špeciálna klávesnica, ktorá je schopná silu stlačenia merať. Všetky ostatné spôsoby sa dajú vyhodnotiť len pomocou špeciálneho programu [4, 6].

4. Porovnanie metód z hľadiska použiteľnosti v IT

V súčasnej dobe sú prevažne využívané systémy zabezpečenia dát, ktoré sa spoliehajú na preukázanie oprávnenosti užívateľa k prístupu do systému a otázka identifikácie užívateľa je riešená len na základe niektorých biometrických údajov. Väčšinou sa využíva overenie len jedného biometrického prvku.

Budeme preferovať metódy, ktoré boli uvedené v úvode a ktoré sa dlhodobo osvedčili ako stabilné, poprípade čo najmenej obťažujúce personál. Z pohľadu užívateľa musí ísť navyše o metódu dostatočne rýchlu (Tab.1). Ďalšími parametrami výberu budú požiadavky na hardvérovú náročnosť a potrebný výpočtový výkon.

metóda	stálosť biometrickej vlastnosti v čase	časová náročnosť snímania	overovanie živosti
odtlačok prsta	stredná	nízka	len u teplotných senzorov
geometria tvaru ruky	stredná	priemerná	nie
snímanie krvného riečiska	stredná	priemerná	áno
snímanie tváre	nízka	vysoká	áno
snímanie očnej dúhovky alebo sietnice	vysoká	vysoká (najmä u sietnice)	nie
dynamika stláčania počítačových klávesov	nízka	–	nie

Tabulka 1 – Porovnanie vybraných biometrických metód

5. Využitie vybraných metód v elektronickom zázname

Cieľom tejto práce je navrhnúť viacfaktorový systém, ktorý bude overovať niekoľko biometrických prvkov zároveň a zabezpečí tak väčšiu spoľahlivosť identifikácie. Takto navrhujeme chrániť prístup k pacientskym dátam v elektronickom zázname personálnej identifikácie ERPI, ktorý koncepčne vychádza z návrhu Universal Electronic Health Record MUDR, podrobne popísaný v literatúre [7].

Zabezpečenie pacientskych dát je jednou z kľúčových otázok telemedicíny. V našom prípade sa môže javiť, že sa jedná o štandardné riešenie s využitím princípov elektronického záznamu EHR MUDR. Uvedená koncepcia záznamu je však riešená s ohľadom na bežné pacientske dáta, s ktorými sa stretávame v prevádzke bežnej nemocnice.

V prípade elektronického záznamu personálnej identifikácie ERPI by sa malo jednať o omnoho citlivejšie dáta, ktoré súvisia s identifikáciou jedinca z rôznych pohľadov. Z tohto dôvodu vzniká tiež požiadavka na vyššiu úroveň identifikácie osôb, ktoré budú k dátam pristupovať.

S ohľadom na charakter takýchto dát sa javí ako potrebné použitie niektorej sady DLP (Data Loss Prevention), ktorá umožňuje identifikovať riziká súvisiace so stratou citlivých dát a prípadne tieto riziká dynamicky znižovať. Navyše s ohľadom na typ citlivých identifikačných dát je vhodné mať k dispozícii prostriedok, ktorý umožní následný audit týchto dát.

Komerčné riešenia sú dostupné napríklad od RSA nebo Websense. Tieto sady sú navrhnuté tak, aby znižovali vplyv potenciálnych rizík nežiaduceho úniku dát z informačného systému bez ohľadu na to, či sú dáta uložené v datacentrách, prenášané cez sieť (sieťové DLP), alebo spracovávané užívateľom v koncovom zariadení (DLP koncového bodu). Toto riešenie je zaujímavé hlavne z dôvodu, že v ČR ešte nebolo v podobnom kontexte nasadenie systému DLP publikované [9].

6. Záver

Výsledkom by mal byť nový komplex biometrických identifikačných metód, ktorý umožní spoľahlivú identifikáciu užívateľa čo najkomfortnejším spôsobom. Výsledná aplikácia nových princípov zabezpečenia bude použitá pre zvýšenie ochrany špecializovaného zdravotného záznamu. Ďalej dôjde k rozšíreniu obecne pojatej koncepcie EHR MUDR do ďalšej aplikačnej oblasti.

Poďakovanie

Práca vznikla v rámci CBI (Centrum biomedínské informatiky), ktoré je riešené v rámci projektu 1M06014 MŠMT.

Literatúra

[1.] Bicz, W. et al. (2005). Fingerprint structure imaging based on an ultrasound camera, http://www.optel.com.pl/article/english/article.htm

[2.] Cravotta N. (2000). Looking under the surface of fingerprint scanners, EDN, http://www.edn.com/article/507025-Looking_under_the_surface_of_finger_print_scanners.php

[3.] Gunetti, D., Pikardi, C. (2005). Keystroke analysis of free text. In ACM Transactions on Information and System Security, sv. 8, č. 3, str. 312-347.

[4.] Ilonen, J. (2003). Keystroke Dynamics. In Advanced Topics in Information Processing, Lappeenranta University of Technology, http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf

[5.] Jain, A., Bolle, R., Pankarti, S. (1999). Biometrics: personal identification in networked society, Kluwer Academic Publisher, Norwell, Massachusetts, USA.

[6.] Monrose, F., Rubin, D. (2002). Keystroke dynamics as a biometric for authentication. In Future Generation Computer Systems, sv. 16, č. 4, str. 351-359.

[7.] Nagy, M. et al. (2008). Applied Information Technologies for Development of Continuous Shared Health Care. In CESNET Conference 08, CESNET, z.s.p.o., Prague, http://www.ces.net/events/2008/conference/cesnet08-proceedings.pdf

[8.] Rak, R.; Matyáš, V.; Říha, Z. (2008). Biometrie a identita člověka: ve forenzních a komerčních aplikacích, Grada, Praha.

[9.] RSA, The Security Division of EMC: Security Solutions for Business Acceleration [online]. 2010 [cit. 2010-10-28]. RSA Data Loss Prevention (DLP) Suite. WWW: <http://www.rsa.com/node.aspx?id=3426>.

[10.] Zhang, D. (2000). Automated biometrics: technologies and systems, Kluwer Academic Publisher, Boston.

Kontakt:

Ing. Anna Horňáková
Oddělení medicínské informatiky
Ústav informatiky, AV ČR, v.v.i.
Pod Vodárenskou věží 2
182 07 Praha 8
tel: +420 26605 3291
e-mail: *hornakova@euromise.cz*