Uporaba biometričnih sistemov v boju proti glokalnemu terorizmu

Robert Brumnik

Povzetek:

Namen prispevka:
Biometrija, je veda o prepoznavanju identitete, na principu fizičnih značilk telesa, kot so prstni odtis, obraz, glas, šarenica (statična biometrija) ali vedenjskih značilk telesa, kot je hoja, podpis, dinamika tipkanja (dinamična biometrija). Glavna domena biometrije je priskrbeti verodostojna in kvalitetna dokazila pri osebni identifikaciji/avtentikaciji. Prispevek je kot povzetek dispozicije doktorskega dela, orientiran v izhodišča smiselnosti uporabe biometričnih sistemov, v boju proti terorizmu.

Metodologija:
Prispevek vsebuje pregled metodoloških orodij, ki bodo uporabljena pri raziskavah v okviru izdelave doktorske naloge. Svoje mesto v prispevku pa najde tudi povzetek kontroverzne Rudminove[1] analize, po kateri iskanje in identifikacija teroristov na osnovi biometrične tehnologije ni učinkovita.

Ugotovitve:
Povečevanje mobilnosti populacije ter posledično s tem povezana globalizacija terorizma, zahteva povečanje razpoložljivosti globalnih informacij, s katerimi lahko identificiramo človeka na lokalnem nivoju (Jain, Bolle, in Pankanti, 1999). Trenutno predstavljajo na področju osebne identifikacije: Evropa 80 % tržišča pametnih kartic, 15% predstavlja Azija, Severna Amerika pa samo 5 % (ostalo biometrija). Vsled tega je pričakovati povečan trend uporabe biometričnih sistemov v EU.

Praktična uporabnost:
Motivov za temeljne in aplikativne raziskave na področju biometričnih sistemov, je več kot dovolj. V prispevku bomo izpostavili nekaj najpomembnejših:

1. Enostavnost ter varnost uporabe biometričnih sistemov, pri postopkih identifikacije.
2. Stroškovni aspekt (razpoložljivost, vzdrževanje).
3. Uporabnost izsledkov raziskave, v mnogih znanstvenih disciplinah Medicina, Informatika,..
4. Usklajenost raziskovalne tematike potrebam aktualnih EU projektov (SIS_II schengenski informacijski system).
5. Trend globalizacije.
   - Standard (NATO[2], MicroSoft[3], Biometrija-ByoScript[4]?).
   - Študija[5] Evropske komisije o vpeljavi biometrije v evropski "način življenja" in njenem vplivu na družbo kot celoto

[1] Floyd Rudmin (Rudminova analiza); original dostopen na URL: (http://www.lewrockwell.com/orig7/rudmin1.html). Statistična analiza, ki jo je opravil Rudmin (profesor psihologije in sociologije univerze Tromso-Norveška), postavlja pod vprašanje uporabnost identifikacijske opreme za množični nadzor.

[2] NATO; Organizacija severnoatlantskega sporazuma ali tudi Severnoatlantska pogodbena zveza (angleško North Atlantic Treaty Organisation; kratica Nato ali NATO) je mednarodna vojaško-politična organizacija držav za sodelovanje na področju obrambe, ki je bila ustanovljena leta 1949; url: http://sl.wikipedia.org/wiki/NATO (28.08.2008) in članicam zveze narekuje vojaške standarde.

[3] Microsoft Corporation, je ameriško računalniško podjetje s sedežem v Redmondu, Washington, ZDA, sta ustanovila leta 1975 Bill Gates in Paul Allen; url: http://sl.wikipedia.org/wiki/Microsoft (28.08.2008). Microsoft je največje softversko podjetje na svetu s preko 80.000 zaposlenimi in je preko programskega produkta Office prevzelo primat svetovnega monopolista ter tako narekovalo standard v računalništvu.

[4] BioScript; url: http://www.bioscrypt.com/solutions/home/ (28.08.2008), je podjetje na področju razvoja in prodaje biometričnih proizvodov, in lahko kot v primerih Microsoft in NATO, narekuje standarde in prevzame nadzor nad to tehnologijo in posledično nad identifikacijo ljudi.

6. Tržno-ekonomski aspekt.

Raziskave biometričnih sistemov v procesu identifikacije niso cilj, pač pa pot, ki se ne zaključi. Neprestano se spreminjajo tehnologija (strojna in programska oprema), ranljivost informacijskih sistemov ter grožnje in prijemi teroristov.

Izvirnost/pomembnost prispevka:
Prispevek v četrtem poglavju izpostavlja raziskovalna vprašanja, na katerih bodo bazirale hipoteze kot osnova za nadaljne raziskave.

Ključne beside: glokalno[6], terorizem[7], biometrija, učinkovitost, zanesljivost, razpoložljivost

1 UVOD

Biometrija, je veda o prepoznavanju identitete, na principu fizičnih značilk telesa, kot so prstni odtis, obraz, glas, šarenica (statična biometrija) ali vedenjskih značilk telesa, kot je hoja, podpis, dinamika tipkanja (dinamična biometrija). Glavna domena biometrije je priskrbeti verodostojna in kvalitetna dokazila pri osebni identifikaciji/avtentikaciji (Gates, 2004). Povečevanje mobilnosti populacije ter posledično s tem povezana globalizacija terorizma, zahteva povečanje razpoložljivosti globalnih informacij, s katerimi lahko identificiramo človeka na lokalnem nivoju. Zagotoviti moramo, verodostojne in hitro dosegljive informacije, ter upoštevati njihovo morebitno zaupnost. Posegi v človekove pravice in temeljne svoboščine so omejeni z načeli nujnosti, ustreznosti, določeni v zakonu. Posamezniku mora biti zagotovljeno zadostno varstvo pred posegi (represivnih) državnih organov v zasebnost.

O uporabnosti biometričnih sistemov v boju proti terorizmu, je dosti napisanega tako v strokovni literaturi kot znanstvenih člankih (Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism). "Teroristu je mogoče slediti edino s pomočjo biometrije" (Michael Kirkpatrick[8], 2002). Zavedati se je potrebno, da raziskave biometričnih sistemov v procesu identifikacije niso cilj, pač pa pot, ki se nikoli ne zaključi. Neprestano se spreminjajo tehnologija (strojna in programska oprema), ranljivost informacijskih sistemov ter grožnje in prijemi teroristov. Prispevek je orientiran v izhodišča smiselnosti uporabe biometričnih sistemov, v boju proti terorizmu.

---

[5] Študija, biometrics at the Frontiers: Assessing the Impact on Society Technical je pripravil Joint Research Centre za Evropski parlament url: http://www.google.si/search?hl=sl&q=biometrics+at+the+Frontiers%3A+Assessing+the+Impact+on+Society&btnG=Iskanje+Google&meta= (30.08.2008).

[6] Glokalizacija; (Glocalisation) termin izhaja iz leta 1980 (Japonska gospodarska praksa). Odnos globalno-lokalno=glokalno. Globalizem je odgovor na upočasnjeno rast multinacionalk koncem 20.stoletja. "Uniformiranost v različnosti" Pr.: Beneton v kreacijah, ki se prodajajo globalno so vključene specifičnosti nekega kraja. Družbe pridobijo večje tržišče, ko združijo podobnosti fragmentiranih in geografsko zelo oddaljenih trgov. Paradoks: globalizem podpira fragmentacijo in lokalizme. Kasneje (l.1990) se termin uporablja tudi za druge primere (marketing, kibernetika, fizika..)
Dr. Manfred Lange uporablja v interpretaciji lokalno-regionalo-globalnih interakcij termin "glokalno". Forum za glokalizacijo (l.2001) se fokusira na povezovanje lokalnih skupnosti in ostalih globalnih virov, s ciljem za dosego ojačanja lokalnih skupnosti, socialnega razvoja, rasti demokracije, miru in uravnoteženja med globalnimi priložnostmi ter zmožnostmi lokalizma.

[7] Terorizem; beseda, ki izhaja iz francoščine (terreur), kjer je označevala eno izmed faz revolucije v času jakobinske diktature (od leta 1794 do 1796). Koren besede izhaja iz latinščine (terror, terroris - močan strah), iz katerega izhaja beseda terrere, ki pomeni prestrašiti (Krunić, 1997).

[8] Michael Kirkpatrick; direktor FBI 2002-2004; url: http://www.fbi.gov/congress/congress04/033004kirkpatrick.htm (28.08.2008)

2 BIOMETRIJA

Mnogi dejavniki in motivi, vodijo k uporabi sistemov osebne identifikacije, ki morajo biti varni, zanesljivi ter enostavni za uporabo. V okviru sistema za varovanje informacij, morajo biti natančno določene vloge in odgovornosti udeleženih v varnostnem sistemu neke države (Podbregar in Slapar; 2006). V fazi upravljanja s tveganji, je potrebno izvesti vse potrebne kontrolne postopke, ki bodo morebitno tveganje, zmanjšali na minimum ali ga odpravili.

3 AKTUALNOST TEMATIKE V SVETOVNEM PROSTORU

V globalnem prostoru, biometrija vse bolj pridobiva na pomenu kot znanstvena disciplina.

Identifikacijski sistemi, so namenjeni za uporabo kot varnostni mehanizem, pri vstopu v določen realen ali virtualen prostor, lahko pa tudi pri vstopu na ozemlje neke države, ko je potrebno potrditi avtentičnost ali identificirati osebo.

Problematika sistemov za avtentifikacijo (potrjevanje identitete) oseb, v zadnjih letih pridobiva na pomembnosti tako v Sloveniji, kot tudi v Evropski uniji, ter širše v svetu. Po eni strani gre za strateško vprašanje tako Slovenije kot geopolitičnih povezav, v katere je vključena (EU in NATO), saj je vprašanje varnosti ter potencialnih terorističnih napadov, čedalje pomembnejše. Hkrati pa je za Slovenijo pomembna tudi uskladitev standardov, ki jih uporablja, s tistimi standardi, ki jih na tem področju prevzemamo zaradi vključitve v NATO.

Na področju biometrije, obstaja tudi precejšnje število tujih raziskav. Slovenija na tem področju ne prednjači, saj se biometrija, zaenkrat v večini uporablja v zasebnem sektorju, za vstop v zgradbe. Na nacionalni ravni je edini dosedaj poznan projekt, uvedba biometričnih potnih listin. Nujno potrebno je, da se ohrani nadzor nad ključnimi tehnologijami, povezanimi z zagotavljanjem varnosti ter gibanjem državljanov. Strateški interes Slovenije, namreč ni samo v varnostnih vidikih uporabe biometričnih sistemov. Glede na to, da gre za svetovno tendenco, se pričakuje tudi silovit razmah trga na tem področju in s tem možnost, za doprinos k gospodarski rasti s komercializacijo tovrstnih sistemov.

4 RUDMINOVA ANALIZA

Glede učinkovitosti biometričnih metod identifikacije in množičnega nadzora ter njihove uporabe pri lovljenju teroristov, pa se pojavljajo tudi skeptiki. V predstavitev, navajam analizo na osnovi Bayesovega[9] teorema, ki jo je opravil prof. Floyd Rudmin. Izid raziskave, kot ga je interpretiral prof. Rudmin, bi nas moral zelo skrbeti saj nakazuje na neučinkovitost identifikacijskih sistemov. So torej visoka vlaganja investitorjev (varnostne službe, državne varnostne agencije, policija, vojska, itd.) v identifikacijske sisteme za nadzor in boj proti terorizmu nesmiselna?

Kakšna je torej verjetnost, da je posameznik res terorist, če ga množični nadzor identificira kot terorista (Rudmin, 2006)?
Če je verjetnost enaka 0, potem identificirani posameznik ni terorist. Če je verjetnost enaka 1, potem je vsak odkrit domnevni terorist tudi povsem zagotovo zares terorist. Če je verjetnost

[9] Bayesov teorem je preprosta matematična formula, ki se uporablja za preračun pogojne verjetnosti, pri potrjevanju (testiranju) subjektivnih trditev (hipotez); url: http://plato.stanford.edu/entries/bayes-theorem/ (28.08.2008).

0.5 (50% - 50%), potem je nadzor enako učinkovit kot metanje kovanca oz. povsem naključno odločanje o tem ali je nekdo terorist ali ne.
Za izračun na podlagi Bayesovega teorema so potrebne tri ocene:

- delež teroristov v populaciji;
- verjetnost, da bo množični nadzor identificiral dejanske teroriste;
- verjetnost, da bodo nedolžni državljani napačno identificirani kot teroristi.

Po podatkih ameriškega popisa v ZDA živi 300 milijonov ljudi. Prof. Rudmin je predpostavil, da je v ZDA 1000 teroristov, kar je po njegovem mnenju precej visoka ocena. To pomeni en terorist na 300.000 ljudi. Naslednja predpostavka je, da je učinkovitost množičnega nadzora 0.4, kar pomeni, da bo množični nadzor identificiral 40% pravih teroristov. Tudi ta predpostavka je po mnenju prof. Rudmina previsoka, saj se teroristi izogibajo nadzoru in jih je zato z množičnim nadzorom težje ujeti. Tretja predpostavka pa je, da je stopnja napačne identifikacije enaka 0.0001, da bo torej 0.01% nedolžnih prebivalcev napačno spoznanih za teroriste, čeprav to niso. V številki je to 30.000 nedolžnih posameznikov in 400 pravih teroristov.

S temi predpostavkami na podlagi Bayesovega izračuna ugotovimo, da je verjetnost, da so posameznik terorist, če ga množični nadzor identificira kot terorista le 0.0132. To pa je zelo blizu ničli in zelo daleč od 1. Na podlagi teh predpostavk in tega izračuna prof. Rudmin zaključuje, da je množični nadzor za lovljenje teroristov neustrezen.

Kaj pa ob drugačnih predpostavkah?
Predpostavimo torej, da je učinkovitost množičnega nadzora 0.7 kar pomeni, da bo množični nadzor identificiral 70% pravih teroristov. V tem primeru je verjetnost, da so posamezniki teroristi če jih množični nadzor identificira kot teroriste še vedno le 0.0228. Tudi to je zelo blizu 0 in zelo daleč od verjetnosti 1.

Pa predpostavljajmo naprej. Učinkovitost množičnega nadzora naj bo 0,9, kar pomeni, da bo množični nadzor identificiral 90% pravih teroristov, stopnja napačne identifikacije pa 0.00001(FAR[10]-False Acceptance Rate), kar v konkretnem ameriškem primeru pomeni da bo samo 3000 nedolžnih napačno identificiranih za teroriste. S temi predpostavkami je verjetnost še vedno le 0.2308, kar je slabše, kot če bi metali kovanec.

Kdaj je torej množični nadzor učinkovit? Le v primeru, da je dejanski delež teroristov v populaciji dovolj visok. Namesto 1000 dejanskih teroristov v ZDA bomo torej predpostavili, da je teroristov milijon. V tem primeru je delež dejanskih teroristov 0.00333, verjetnost, da je posameznik zares terorist, če ga množični nadzor identificira kot terorista pa je 0.99. To pa je že zelo blizu gotovosti.

Sklep:
Na podlagi tega, prof. Rudmin zaključuje, da so sistemi množičnega nadzora za lovljenje teroristov neuporabni.
Uporabni so le v primeru nerealnih, paranoičnih predpostavk (milijon teroristov v ZDA). In, če te paranoične predpostavke niso izpolnjene, bo dejansko veliko nedolžnih posameznikov neupravičeno identificiranih za teroriste (mimogrede, v ZDA se to očitno že dogaja, primer za to so seznami nezaželjenih letalskih potnikov - "No Fly" seznami, itd.).

[10] FAR (False Acceptance Rate); predstavlja uspešno registracijo neavtoriziranega oz. neobstoječega uporabnika v sistemu.

Rudmin navaja še drugo možnost. Množični nadzor morda ni namenjen iskanju teroristov, pač pa iskanju posameznikov, ki niso tako redki kot so teroristi. Prof. Rudmin ugotavlja, da je anketa na Fox News[11] 19. maja 2006 pokazala, da 30% anketirancev v ZDA želi odpoklic Busha (ti. Impeachment). Če bi NSA[12] množično nadzorovala vse Američane z namenom identifikacije vseh posameznikov, ki si želijo odpoklic Busha in, če bi bila verjetnost, da bo množični nadzor identificiral dejanske Busheve nasprotnike enaka 0.9, verjetnost, da bodo Bushevi podporniki ali neopredeljeni napačno identificirani kot njegovi nasprotniki pa 0.01, je verjetnost, da si posameznik ki ga množični nadzor identificira kot Bushevega nasprotnika zares želi Bushevega odpoklica enaka 0.98.

Iskanje teroristov med 300 milijoni Američanov je torej po mnenju prof. Rudmina matematično nemogoče. Izvajanje množičnega političnega nadzora pa je matematično lahko zelo učinkovito.

Obstaja pa še tretja možnost. Tajne službe samo zapravljajo davkoplačevalski denar in opravičujejo svoj obstoj. Ali pa denar porabljajo za kaj drugega. In če jih kdo vpraša po rezultatih njihovega dela, se lahko vedno skrijejo za "nacionalnimi interesi".

5 RAZISKOVALNA VPRAŠANJA-IZHODIŠČA

1. Ali je lovljenje teroristov z uporabo biometričnih metod za množični nadzor, res (matematično) nemogoče in nesmiselno?
2. Ali množični nadzor celotne populacije lahko učinkovito odkrije teroriste?
3. Kaj o tem pravi matematična znanost na podlagi statističnih rezultatov pridobljenih v realnih okoljih delovanja?
4. Ali lahko biometrične metode za množični nadzor uspešno odkrijejo globalno-znanega terorista (zavedenega v vseh svetovnih bazah), ki pa se uspešno (lokalno) skriva in izmika sofisticiranim identifikacijskim sistemom?
5. Kako je z varnostjo osebnih podatkov glede na ostale sisteme?
6. Ali je strogo-matematični pogled psihologa-filozofa na uporabo biometričnih identifikacijskih sistemov v boju proti terorizmu edini smiselen, ki lahko verodostojno dokaže funkcionalno (ne)uporabnost sistemov?

V kolikor se odločamo za statistično-matematično oceno uporabnosti sistema bi bilo smiselno v obzir vzeti še naslednje parametre:

- statistična zanesljivost sistema-Reliability
- statistično-stohastična učinkovitost sistema (strežbe)-Efficacy
- karakteristika trenutne pogostosti odpovedi λ(t)
- frekvenca opravljenih pregledov z biometričnim sistemom v primerjavi z ostalimi razpoložljivimi sistemi (kartični, ID[13] card..)
- razpoložljivost biometričnega sistema napram ostalim sistemom identifikacije, ki so na voljo (kartični, ID card)
- napaka identifikacije-možnost (FAR, FRR[14]..)
- ponarejanja biometričnih identifikatorjev
- hitrost identifikacije

[11] Fox News je TV in radijski (satelitski) medij v lasti Fox Entertainment Group, url: http://en.wikipedia.org/wiki/Fox_News_Channel (30.08.08).
[12] NSA; Ameriški varnostna agencija (National Security Agency).
[13] ID Card; osebne identifikacijske izkaznice
[14] FRR (False Recection Rate); pomeni neuspešno registracijo uporabnika z obstoječo avtorizacijo.

- možnost in hitrost "kloniranja" identitete (identity theft).

Analiza, ki jo je predstavil prof. Rudmin, je tako za oceno uporabnosti biometričnih sistemov po mojem mnenju zelo sociološko pristranska, saj ne zajema mnogih učinkov uporabnosti, ki so z implementacijo biometričnih sistemov v boju proti terorizmu prisotni. Potrebno je namreč izpostaviti pomembnost celovitosti prikaza kvalitativnih in kvantitativnih parametrov oz. kazalcev učinkovitosti in varnosti biometričnega identifikacijskega sistema. Vprašanje varnosti biometričnega sistema, pa je seveda nujno obdelati tudi s stališča varovanja osebnih podatkov.

Pričakovani prispevek znanosti

Raziskava v okviru doktorskega dela, obravnava problematiko družbene sprejemljivosti, identifikacijskih sistemov za množični nadzor. Gre za tendenco vzpostavitve varnosti, z minimalnim vplivom na svoboščine državljanov. Prisotnost zavedanja, da se že dotikamo vprašanja družbene sprejemljivosti takšne tehnologije, pa je ob vsem tem nujno potrebna. Tehnologija, ki je v prvi vrsti namenjena iskanju teroristov ter avtomatizaciji procesa osebne identifikacije, namreč posega tudi v našo zasebnost in življenje.

Raziskava v okviru izdelave doktorske disertacije temelji na:

1. kvantitativnih metodah statistične analize (anketiranje, statistična obdelava podatkov SPSS[15],..), v raziskavi družbene sprejemljivosti identifikacijskih sistemov. Raziskavo želim opraviti na populaciji različnih starostnih skupin ter stopenj izobrazbe v vezi s poznavanjem tehnologije za množični nadzor ter zavedanjem učinkov nadzora za ceno varnosti,
2. raziskovalno znanstvenem delu na področju inženiringa zanesljivosti ter statističnem vrednotenju rezultatov aplikativno razvitega biometričnega sistema, v smislu učinkovitosti in varnosti. Predstavil, ter izdelal bom raziskavo parametrov: FAR, FRR, zanesljivost (Reliability), učinkovitost (Efficacy) in karakteristike trenutne pogostosti odpovedi $\lambda(t)$ ter v okviru tega, pripravil kvalitativno statistično oceno parametrov, ki vplivajo na varnost in učinkovitost biometričnega sistema. Predstavljen bo njihov medsebojni vpliv, v realnih sistemih delovanja.

Sistemi za identifikacijo in potrjevanje identitete oseb na podlagi več značilk, naj bi v končni fazi, pripomogli k optimalnejšemu identifikaciji/avtentifikaciji oseb in preprostejšemu omejevanju dostopa do prostora (realen-virtualen prostor, zgradbe, lahko tudi države) ali varnostno zaščitenih informacij. Raziskovalno delo, naj bi doseglo večplasten pozitivni učinek pri uporabi biometričnih sistemov, ki ga lahko nakažemo v praktičnem in teoretičnem prispevku znanosti. Rezultati raziskave pa bodo lahko podpora odločitvam pri spremembi zakona o uporabi biometričnih sistemov.

6 OMEJITVE

V raziskavi bomo upoštevali zakonodajo (Zakon o varovanju osebnih podatkov, itd.) ter predpisane mednarodne standarde tega področja (BS7799, JTC1/SC17: Cards & Personal ID, JTC1/SC37: Biometrics, JTC1/SC27: IT Security, TC68: Financial Services, ISO/IEC 19794-2 Finger Minutiae Data, ISO/IEC 19794-4 Finger Image Data).

[15] SPSS Statistični paket sodi med najbolj razširjene "statistične" programske pakete v svetu. Namenjen je predvsem statistični obdelavi podatkov z osebnimi računalniki.

7 PREDVIDENE METODE RAZISKOVANJA

- Raziskava literature.
- Eksplorativni raziskovalni pristop, zaradi interdisciplinarnosti tudi multimetodski.
- Temeljni del raziskave, bo zasnovan na raziskovalno-strokovnem študiju identifikacijskih sistemov množičnega nadzora.
- Eksperimentalni pristop primerjalnega testiranja identifikacijskih sistmov.
- Statistična orodja za dokazovanje povezanosti dejavnikov ter pojavov (SPSS).
- Oblikovanje prioritetnih modelov sprejemanja biometrčnih sistemov na podlagi strukturiranega procesa (intervju, anketiranje, faktorska analiza) z vgrajenimi dejavnki, družbene sprejemljivosti biometričnega sistema.
- Ocenjevanje s pomočjo anketnega vprašalnika, oblikovanega na podlagi Likertove lestvice.

8 RAZPRAVA

Pri pregledu svetovne literature, lahko zasledimo množico raziskav, ki se ukvarjajo s sodobnimi identifikacijskimi tehnologijami v kontekstu zasebnosti. Raziskave, temeljijo na predpostavkah, pravice do zasebnosti, vendar le redko katera, rezultate utemeljuje s kvalitativnimi ali kvantitativnimi znanstvenimi pristopi. Z raziskovalnim delom na področju kriminologije, želim določiti stopnjo poznavanja tehnologije za množični nadzor ter pripadajoče zakonodaje na tem področju. Zaradi nepoznavanja biometrije ter neustrezne zakonodaje na področju uporabe biometričnih tehnologij pri osebni identifikaciji, zamujamo mnoge priložnosti, tako v ekonomskem kot raziskovalnem smislu v javni upravi in gospodarskem segmentu.

9 VIRI

- Gates, K. A. (2004) Our biometric future: The social construction of an emerging nformation technology, University of Illinois at Urbana-Champaign, United States 2004.
- Hicklin, A., Watson , C., Ulery, B. (2005) The Myth of Goats: How many people have fingerprints that are hard to match?, NIST Interagency Report 7271.
- Hicklin, A., Khanna, R. (2006) The Role of Data Quality in Biometric Systems, National Institute of Standards and Technology, U.S. Department of Interior, Contract NBCH-D-02-0039.
- Huvanandana, Sanpachai (2002) A framework for a fast fingerprint identification using a hybrid system , University of Washington, United States
- Huey, L., Rosenberg, R. S. (2004) Thoughts on Expanding Police Surveillance Opportunities under the Cyber - Crime Convention. V: Canadian Journal of Criminology and Criminal Justice, Volume 46, no. 5. 597–606.
- Jain, A. K., Bolle, R. and Pankanti S. (1999) BIOMETRICS: Personal Identification in Networked society, Kluwer Academic Publishers.
- Janbandhu, P. K. and Siyal, M. Y., (2001) Novel biometric digital signatures for Internet-based applications, Inf. Management and Computer Security, vol. 9.1.
- Khanna, R., Ratha, N. (2004) Systems Engineering for Large-Scale Fingerprint Systems, Automatic Fingerprint Recognition Systems, Springer Verlag, New York, 2004.
- Kirkpatrick, M., (2002) http://www.fbi.gov/congress/congress04/033004kirkpatrick.htm

- Maltoni, D., Maio, D., Jain A. K. and Prabhakar, S. (2003) Handbook of Fingerprint Recognition, Springer Verlag. Meagher, S., Hicklin, A. (2005) Extended Fingerprint Feature Set, ANSI/NIST ITL 1-2000 Standards.
- Meško, G. (2000) Pogledi na preprečevanje kriminalitete v pozno modernih družbah, Teorija in praksa let. 37, 4/2000; str. 716-727
- Nadel, L. (2006) On the Future of Biometrics – Research, Applications, and Social Challenges, IEEE CVPR 2006.
- National Institute of Standards and Technology, (DES) Data Encryption Standard, Federal Information Processing Standards Publication 46-2, 1993.
- Podbregar, I., Slapar, M. (2006) Razsežnosti gospodarskega vohunstva v 21. Stoletju-primer gospodarskega vohunstva s pomočjo trojanskega konja, Bled, Dnevi varstvoslovja
- Praprotnik, T. (2003) Skupnost, identiteta in komunikacija v virtualnih skupnostih. Ljubljana: ISH - Fakulteta za podiplomski humanistični študij (Knjižna zbirka Documenta).
- Ratha, N. K., Connell, J. H., Bolle, R. M. (2001) An analysis of minutiae matching strength, Proc. 3rd AVBPA, Halmstad, Sweden,
- Rudmin, F. (2006) The Politics of Paranoia and Intimidation, Why Does the NSA Engage in Mass Surveillance of Americans When It's Statistically Impossible for Such Spying to Detect Terrorists? http://www.counterpunch.org/rudmin05242006.html
- Snelick, R., Indovina, M., Yen, J. and Mink, A. (2000) Multimodal Biometrics: Issues in Design and Testing, in Proceedings of Fifth International Conference on Multimodal Interfaces, Vancouver, Canada