

INTELIGENTNA BIOMETRIJA ZA NADZOR VSTOPA

Matjaž Gams, Tea Tušar

Odsek za inteligentne sisteme, Institut Jožef Stefan

Jamova 39, 1000 Ljubljana, Slovenija

Tel: +386 1 4773900; fax: +386 61 1251038

e-mail: matjaz.gams@ijs.si, <http://ai.ijs.si/mezi/matjaz.html>

Povzetek

V tem prispevku bomo opisali CIVaBiS - Celovit inteligentni varnostni biometrični sistem, tj. projekt ARRS in MORS z namenom nadzora vstopa in predvsem v zvezi z varnostnimi grožnjami. Sistem je zasnovan za preprečevanje groženj v zvezi s teroristi, vendar so varnostne komponente načeloma uporabne kjerkoli. Projekt se nahaja v ključni fazi testiranja in integriranja, vsebuje pa vrsto že izdelanih modulov za nadzor vstopa: biometrijo, integracijo, mikroučenje, makroučenje, ekspertni sistem in umetni vid. Ideja projekta je v tem, da se z integracijo več modulov in posebej z inteligentnim prilagajanjem na vsakega vstopajočega bistveno zmanjša možnost penetracije sistema. Sedanje izkušnje kažejo, da je integracija več modulov z inteligentnim sklepanjem pomembna izboljšava.

1 UVOD

Teroristični napadi in vse pogostejši vdori v varovane objekte (banke, poslovni prostori) so v splošni javnosti povišali zavest o pomembnosti **zagotavljanja varnosti oseb in varovanih prostorov**. Zato je pomembno, da se zagotovi učinkovit nadzor nad vstopom v varovane prostore. Zahteve po podobnih sistemih nadzora postajajo vse pogostejše in se uveljavljajo tudi na drugih področjih, kot so varovanje mejnih prehodov in pomembnih turističnih in poslovnih objektov.

Na področju avtentikacije ljudi postajajo čedalje bolj pomembne in razširjene biometrične identifikacijske metode, ki omogočajo višji nivo varnosti pri nadzoru vstopa. Taki prijemi lahko zagotovijo večjo stopnjo osebne varnosti, učinkovitejše izvajanje osebnih pravic in varnejšo državno in evropsko mejo. Po besedah M. Kirkpatricka, enega direktorjev FBI: "Teroristu je mogoče slediti edino s pomočjo biometrije." (angl. "The only way to trace a terrorist is through biometrics.")

Pri tem moramo upoštevati, da vse varnostne situacije niso enake, tudi znotraj istega sistema ne. En odgovor na potrebo po prilagajanju posameznim varnostnim situacijam je **kombiniranje različnih identifikacijskih metod**. Izbira, usklajevanje in uravnoteženje varnostnih prijemov, vključno z metodo identifikacije, je ključnega pomena, saj omogoča ustrezno prilagajanje varnostnim potrebam. Kombinirane metode identifikacije je bistveno težje pretentati kot eno

samo ne glede na to, da so nekateri sistemi izredno zanesljivi že sami zase.

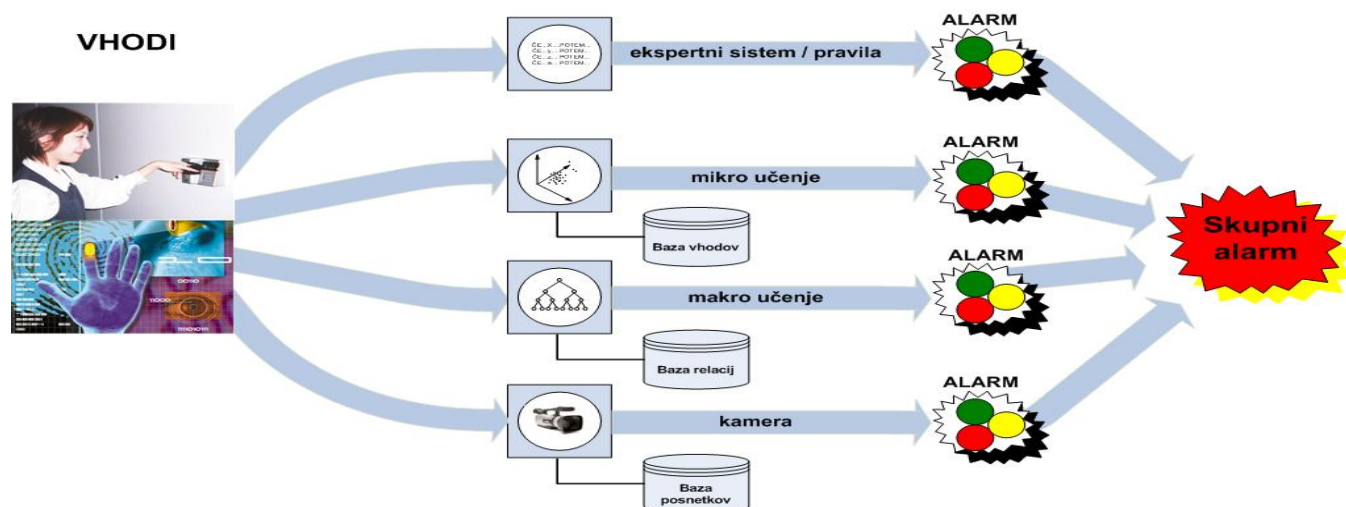
Posebej po terorističnih napadih v ZDA in drugod po svetu je izredno poskočilo vlaganje v raziskave in razvoj na področju inteligentnih sistemov za biometrični nadzor oseb. Danes v razvitem svetu velja, da je najučinkovitejše sredstvo v boju proti terorizmu inteligenca. ZDA so zato sprejele vrsto zakonov, ki omogočajo obširnejše zbiranje (osebnih) podatkov in elektronski nadzor. Z več podatki tako postaja eden ključnih mehanizmov v boju proti terorizmu **uporaba inteligentnih metod za nadzor oseb** (Gams 2001, Luštrek idr. 2006, Reddy 2006). Z novimi metodami lahko inteligentni sistemi opazijo **sumljivo ali deviantno obnašanje posameznika**, ki je lažne identitete ali pa celo prave identitete (ali neznane), vendar iz kakršnihkoli razlogov odstopa od običajnega za znanega posameznika (npr. pod vplivom opojnih substanc ali s porušenim duševnim ravnotežjem) ali izstopa od običajnega za posameznika svojega tipa (npr. glede na starost, videz itd.). Metode biometrične identifikacije omogočajo zbiranje podatkov o osebah, ki jih nato obdelamo z inteligentnimi sistemi, kar nam omogoča višji in bolj poglobljeni nivo ugotavljanja morebitnih varnostnih vdorov (Kolbe idr. 2005).

Primer vstopne kontrole na dejanskem vhodu je predstavljen na Sliki 1. Zaposleni približa kartico čitalniku kartic in položi prst v čitalnik prstnih odtisov. Sistem v primeru pozitivne identifikacije odpre vrata.



Slika 1: Primer vstopne kontrole. Na desni sta čitalnik prstnih odtisov in čitalnik kartice.

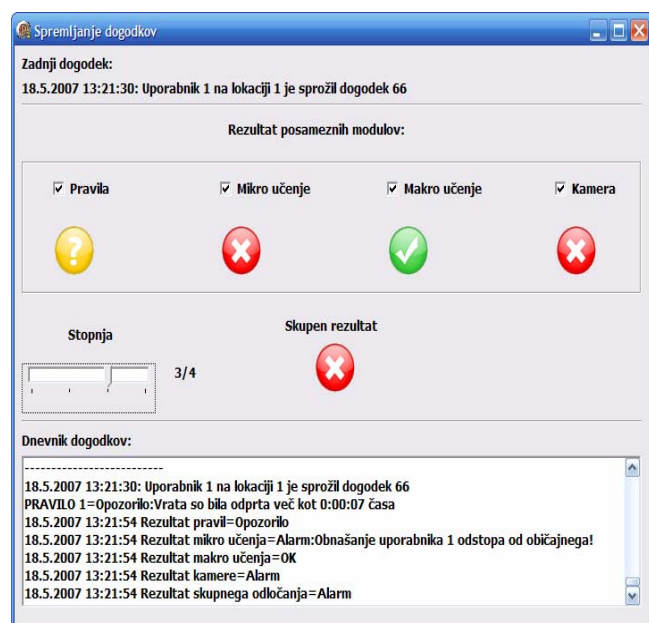
2 CiVaBiS – zgradba



Slika 2: Struktura sistema CiVaBiS.

Shema sistema je prikazana na sliki 2. Po registraciji z eno ali več napravami inteligentni sistem preveri vstop še s štirimi koduli: ekspertni sistem, mikroučenje, makroučenje in umetni vid. Vsak od modulov oceni verjetnost pravilne identitete ter zaključek grafično sporoči z ustrežno barvo. Odgovori modulov se integrirajo.

barvo, medtem ko v primeru makroučenja ni bilo nobenih dvomov v pravilno identiteto vstopajočega. Vhodne signale sistem pobira z naprav komercialnih dobaviteljev podjetja Špica, integriranje pa poteka preko izvirno razvitega HW (Slika 4).



Slika 3: Sporočilo sistema ob vstopu.

Na Sliki 3 vidimo sporočilo sistema ob vstopu. Prvi modul, ekspertni sistem, ni prepričan ne o alarmu, ne o pravilni identiteti, zato sporoči svojo neodločnost z rumeno bravo. Modula mikroučenje in kamera sporočita resen sum z rdečo



Slika 4: Integracija vhodnih naprav poteka s sistemom DOGS, razvitim v podjetju Špica.

SW celotnega sistema razvijajo vsi trije partnerji, poleg Špice še Fakulteta za elektrotehniko (kamera, vid) in Inštitut Jožef Stefan (inteligenca, integracija).

3 CiVaBiS – opis modulov

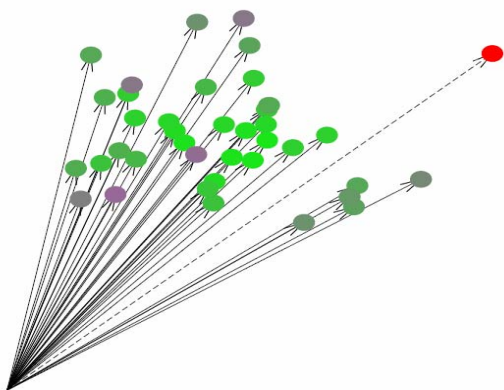
3.1. Ekspertni sistem

Sistem pravil, imenovan tudi ekspertni sistem, je nakazan na Sliki 2. Ob vhodu sistem testira pravila in glede na vzorec sproži alarm ali ne. Pravila so naslednje oblike:

- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če uporabnik PARAM2 sproži dogodek med časom PARAM3 in časom PARAM4 na dan PARAM5 (PON, TOR, SRE, CET, PET, SOB, NED ali VSAK_DAN).
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če uporabnik PARAM2 sproži več kot PARAM3 dogodkov v času PARAM4.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če uporabnik PARAM2 po vstopu ne izstopi v času PARAM3.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če med časoma PARAM2 in PARAM3 zapustijo prostor uporabniki PARAM4 (napišite uporabnike, ločene z vejico), ki so prišli noter.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če se vrata po odprtju ne zaprejo v času PARAM2.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če se pred dogodkom PARAM2 ni zgodil dogodek PARAM3 (KARTICA, PRSTNI_ODTIS, ODPIRANJE_VRAT ali ZAPIRANJE_VRAT) v času PARAM4.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če se pred dogodkom PARAM2 ni zgodil dogodek PARAM3 (KARTICA, PRSTNI_ODTIS, ODPIRANJE_VRAT ali ZAPIRANJE_VRAT) v času PARAM4.
- Pravilo sproži PARAM1 (OPOZORILO ali ALARM), če uporabnik PARAM2 ni odšel iz prostora do časa PARAM3.

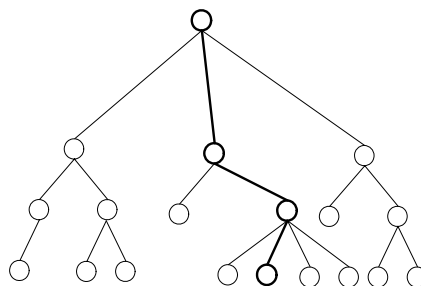
3.2. Mikroučenje

Modul mikroučenja za vhodne podatke uporabi čase med čitalnikom kartice in čitalnikom odtisov, med čitalnikom in odprtjem vrat ter med odprtjem in zaprtjem vrat. Skupno imamo 3 čase, torej 3D prostor, na katerem se učimo glede na učne primere – prejšnje vhode določene osebe. Ko vstopi nova oseba, npr. terorist, primerjamo njene časovne podatke s podatki tiste osebe, za katero se terorist izdaja. V naših testih se je pokazalo, da se ljudje registrirajo dokaj stabilno, zato se običajno hitro in jasno pokaže, kadar vstopa nekdo drug z lažno identiteto.



Slika 5: Mikroučenje išče "outlierje" glede na 3 čase (2 čitalnika in vrata) ter glede na prejšnje vstopo.

3.3. Makroučenje

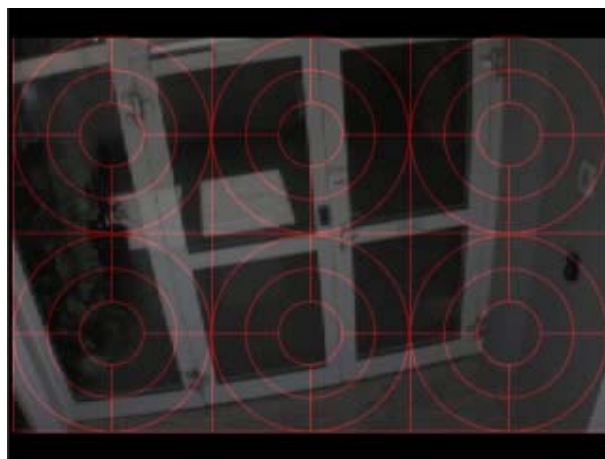


Marko in Tea vsak ponedeljek vstopita v razmaku 30 sekund (92%, 34)

Slika 6: Makroučenje išče globalne zakonitosti glede na istočasne vhode, običajno uro itd.

Makroučenje za razliko od mikroučenja išče bolj globalne zakonitosti, npr. kdo vstopa običajno kdaj in s kom ... Tu gre za klasično rudarjenje podatkov.

3.4. Kamera / umetni vid



Slika 7: Vektorji gibanja so osnova za analizo identitete vstopajočega.

Zadnji modul se podobno kot prejšnji dve učenji skuša naučiti vzorcev vstopajočega, konkretno dinamiki oseb, opazovani preko kamere. Nastali vektorski premiki služijo prepoznavanju vstopajočega (Perš idr. 2002).

4 ZAKLJUČKI

Varnost postaja v svetu vedno pomembnejše področje, zato mora tudi Slovenija slediti temu trendu. Med ključnimi elementi varnosti je zagotavljanje nadzora vstopa v prostore z omejenim dostopom ter nadzor varovanih odprtih prostorov, kot je na primer prestop državne meje. Tak nadzor se najučinkoviteje izvaja z biometričnimi metodami, integriranimi z metodami inteligentnih sistemov.

V okviru projekta CIVaBiS smo razvili **celovit inteligentni varnostni biometrični sistem za avtentikacijo oseb za**

potrebe obrambnega sistema in boja proti terorizmu. V sistem je moč vključiti poljubno kombinacijo biometričnih senzorjev. Poglavitna novost je v inteligentni komponenti sistema, ki je na osnovi znanja in sprotnega učenja iz zbranih podatkov sposobna opozoriti na nenavadno obnašanje pri kontroli vstopa.

Zahvala: Zahvaljujemo se MORS in ARRS za financiranje projekta CiVaBiS. Zahvaljujemo se tudi g. M. Štruklju za pripombe in nadzorovanje izvajanja sistema. Zahvaljujemo se tudi sodelavcem: Mitji Kolbetu, M. Luštreku, E. Dovganu, B. Kaluži in Robertu Blatniku.

Literatura

- [1] Gams, M. Weak intelligence: Through the principle and paradox of multiple knowledge, Advances in computation: Theory and practice, Vol. 6, Nova sc. Pub., inc., NY, 2001.
- [2] Kolbe, M., Gams, M., Kovačič, S., Perš, J. Sistem za avtomatsko razpoznavanje obnašanja z metodami računalniška vida. V: Zbornik 8. mednarodne multikonference Informacijska družba IS 2005, 11. do 17. oktober 2005, (Informacijska družba). Ljubljana: Institut "Jožef Stefan", 2005, str. 357-361.
- [3] Luštrek, M., Gams, M., Bratko, I. Is real-valued minimax pathological?. Artif. intell., 2006, vol. 170, str. 620-642.
- [4] Reddy, R. Robotics and Intelligent Systems in Support of Society, Intelligent Systems, pp. 24-31, May/June 2006.
- [5] Perš, J., Bon, M., Kovačič, S., Šibila, M., Dežman, B. Observation and analysis of large-scale human motion. Hum. mov. sci., July 2002, vol. 21, str. 295-311.