Primjena biometrijske zaštite u inteligentnim transportnim sustavima

Huđek, Darko

Undergraduate thesis / Završni rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:011986

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-11-27**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Darko Huđek

PRIMJENA BIOMETRIJSKE ZAŠTITE U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

ZAVRŠNI RAD

Zagreb, 2015.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

PRIMJENA BIOMETRIJSKE ZAŠTITE U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

Mentor: dr. sc. Pero Škorput
Student: Darko Huđek, 0016078918

Zagreb, 2015.

Umjesto ove stranice uvezuje se zadatak diplomskog rada

Sažetak

Biometrija predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi temeljeno na jednoj ili većem broju njihovih fizičkih i ponašajnih karakteristika. Cilj završnog rada je da se pokaže primjena biometrije u inteligentnim transportnim sustavima. U uvodu se objašnjavaju pojmovi biometrija i ITS, te se nakog toga povezuje u cjelinu.

Arhitektura ITS-a, kao temeljna organizacija sustava, omogučava nam svaku nadgradnju sustava i prati svaku promjenu u tehnologiji koja omogućuje napredak. Napretkom tehnologija povećavaju se prijetnje i propusti, pa se uz napredak tehnologije javlja i veća potreba za sigurnošću informacija. Kao najbolja zaštita informacija pokazuju se biometrijske metode koje bez potrebne autentikacije ne dopuštaju ulaz i korištenje tih podataka. Na primjerima koji su prikazani u završnom radu dolazi se do zaključka kako biometrija prati napredak tehnologije te u korak sa vremenom povećava sigurnost sustava i smanjuje opasnosti koje svakodnevno prijete informacijskom sustavu.

Ključne riječi: biometrija; ITS; informacijska sigurnost

Abstract

Biometrics is a set of automated methods for uniquely recognizing humans based upon one or more of their physical and behavioral characteristics. The aim of this dissertation is to show the application of biometrics in intelligent transportation systems. The introduction explains the core concepts of biometrics and ITS, which are then expanded upon and presented as a whole.

ITS architecture, as a basic organization system, allows us to upgrade each system and monitors any change in technology that enables progress. Advances in technology increase the number of threats and chance of oversight, and so with them comes a greater need for information security. Biometrics present the best security measures that prevent access unless strict authentication of users' identity is accomplished. The examples in this final assignment lead us to the conclusion that biometrics follows advancements in modern technology and is in step with the ever growing need for better security in information systems.

Keywords: biometrics; ITS; information security

Sadržaj

Uvod

Početkom 21. stoljeća prometni se stručnjaci slažu da uspješno rješavanje rastućih problema odvijanja prometa i obavljanja transporta više nije moguće bez primjene cjelovitog koncepta i tehnologija ITS-a (Inteligentnih transportnih sustava).

ITS je upravljačka i informatičko-komunikacijska nadogradnja klasičnog prometnog i transportnog sustava, tako što se postiže bitno veća propusnost, sigurnost, zaštićenost i ekološka prihvatljivost u odnosu na rješenja bez ITS aplikacija. To ne znači da prije ITS-a nije postojala inteligencija u prometu, nego da se kroz stvarno vremensko prikupljanje i obradu podataka te umreženu distribuciju informacija postiže znatno smanjenje zagušenja, čekanja, prometnih nesreća, neučinkovitosti prijevoza, ekoloških onečišćenja itd.

Predmet završnog rada je prikazati mogućnosti primjene biometrijske zaštite u inteligentnim transportnim sustavima.

Cilj završnog rada je prikazati učinkovitost i korisnost primjene ITS-a u svim aspektima.

Završni rad sastoji se od šest funkcionalno povezanih dijelova ili teza:

1. Uvod,
2. ITS arhitektura i informacijska sigurnost,
3. Analiza informacijsko-sigurnosnih rizika u inteligentnim transportnim sustavima,
4. Pregled biometrijskih sustava,
5. Primjena implementacije biometrijskih rješenja u inteligentnim transportnim sustavima,
6. Zaključak.

Prvo poglavlje završnog rada je *Uvod* u kojem se iznosi predmet rada, cilj, svrha te njegova struktura.

Drugo poglavlje pod nazivom *ITS arhitektura i informacijska sigurnost* odnosi se na arhitekturu i sigurnost, te učinke ITS-a. U poglavlju će se za početak objasniti što je to ITS arhitektura te kako utječe na sami sustav, koje su karakteristike samog sustava kada u sebi ima elemente ITS-a. Nadalje, govorit će se o sigurnosti informacijskih sustava te koje su najčešće prijetnje u informacijskim sustavima.

U trećem poglavlju rada pod nazivom *Analiza informacijsko-sigurnosnih rizika u inteligentnim transportnim sustavima* prikazati će se kako poboljšati sigurnost i učinkovitost kroz provedbu poboljšane identifikacije tehnologije.

U četvrtom poglavlju pod nazivom *Pregled biometrijskih sustava* biti će navedene vrste biometrisjkih sustava i metoda. Za svaku od metode objasnit će se princip djelovanja te kako bi se neki od sustava moga primijeniti u ITS-u.

Peto poglavlje pod nazivom *Primjena implementacije biometrijskih rješenja u inteligentnim transportnim sustavima* vezano je za praćenje sudionika u automobilima tijekom raznih uvijeta.

Šesti dio rada je *Zaključak* koji je donesen na temelju istraživanja i vlastitih promišljanja. Sadržaj ovog poglavlja je rezime napisanog rada te je donesen zaključak koji uvodi u budućnost primjene biometrije u ITS-u, kako u informacijskoj domeni tako i u prometnoj. Na kraju rada se uz popis literature nalazi popis slika prikazanih u tekstu rada.

1. ITS ARHITEKTURA I INFORMACIJSKA SIGURNOST

ITS[1] se može definirati kao upravljačka i informacijsko-komunikacijska nadgradnja klasičnog sustava prometa i transporta kojim se postiže znatno poboljšanje performansi odvijanja prometa kroz učinkovitiji prijevoz putnika i robe, poboljšanje sigurnosti u prometu, udobnost i zaštita putnika, smanjenje onečišćenja okoliša, itd. ITS ima značenje novoga kritičnog pojma koji mijenja pristup i trend razvoja prometne znanosti i tehnologije transporta ljudi i robe tako da se učinkovito rješavaju rastući problemi zagušenja prometa, onečišćenja okoliša, učinkovitosti prijevoza, sigurnosti i zaštite ljudi i robe u prometu, u tom smislu inteligentna cestovna prometnica predstavlja upravljačku i informacijsko-komunikacijsku nadgradnju klasičnih cestovnih prometnica, tako da se osim osnovnih fizičkih funkcija ostvaruje bolje informiranje vozača, vođenje prometa, sigurnosne aplikacije itd. Paralelno teče i razvoj inteligentnih vozila, koja svojim novim svojstvima značajno unaprjeđuju sigurnost, učinkovitost i udobnost vožnje.

Konkretne koristi od ITS-a mogu se promatrati kroz različite skupine pokazatelja, odnosno kategorije ITS učinaka. U literaturi se ITS učinci povezuju uz sljedeće pokazatelje:

1. sigurnost,
2. učinkovitost protoka,
3. proizvodnost i smanjenje troškova,
4. koristi za okoliš.

ITS se sastoji od informacijskih sustava koji se moraju zaštititi kako bi ITS aplikacije bile pouzdane i raspoložive. Ovo je bitan aspekt sigurnosti te se odnosi na sve podsustave u nacionalnoj ITS arhitekturi. Ranjivost sustava temelji se na procjeni tehnologije koja se koristi, sigurnosnih službi na mjestu događaja i okruženju u kojem sustav djeluje. Sigurnosne analize nacionalne ITS arhitekture trebale bi biti na visokoj razini i one predstavljaju početnu sigurnosnu analizu koja se obavlja za bilo koji dio ITS-a.

[1] ITS- Inteligentni transportni sustavi

Ocjenjivanje nacionalne ITS arhitekture se obavlja u smislu tri povezujuća sigurnosna cilja:

1. Povjerljivost (osigurava da podaci budu nedostupni neovlaštenim osobama, procesima ili sustavima);

2. Integritet (osigurava točnost i pouzdanost sustava i podataka te definira razinu zaštite od neovlaštene namjerne ili nenamjerne promjene);

3. Raspoloživost (osigurava da sustavi i podaci budu dostupni ovlaštenim osobama).

ITS se kroz njegovo vrijeme korištenja, odnosno nadgradnjom sustava sa elementima ITS-a pokazao vrlo pozitivnim, tj. istraživanja su pokazala kako se primjenom ITS-a povećala ušteda energije, vremena i novaca, te se povećala sigurnost sustava. Informacijska sigurnost nije isto što i informatička sigurnost, informacijska sigurnost se bavi zaštitom informacija bez obzira u kojem obliku one postojale, dakle to uključuje informacije i u digitalnom i u papirnatom obliku (vrlo često upravo u papirnatom obliku postoje vrlo osjetljivi dokumenti).

1.1. ITS arhitektura

ITS arhitektura predstavlja temeljnu organizaciju sustava koja sadrži ključne komponente, njihove odnose i veze prema okolini te načela njihovog dizajniranja i razvoja, promatrajući cijeli životni ciklus sustava. Arhitektura znači stvarati sustav iz samih korjena, razmišljajući o budućnosti tog sustava i mogućoj nadgradnji kako bi taj sustav bio stabilan i otvoren na razvoj podsustava. To dolazi do izražaja kod velikih sustava kod kojih se očekuje proširenje te se zahtjevaju sljedeće temeljne karakteristike: kompatibilnost, proširivost, interoperabilnost, integrativnost i normiranost.

Ukoliko arhitektura nije dobro definirana, događa se to da se sustav u jednom trenutku više ne može širiti, a troškovi se eksplicitno povećavaju sa svakim novim zahtjevom. ITS arhitektura daje opći predložak (engl. general framework) prema kojemu se planiraju, dizajniraju i postavljaju integrirani sustavi prometa i transporta u određenom prostorno-vremenskom obuhvatu. Na ovaj način omogućeno je planiranje razvoja ITS-a na logičan način. [2]

Arhitektura ITS-a također specificira interakciju između različitih komponenti sustava u cilju rješavanja konkretnih prometnih problema te je konceptualni dizajn koji definira strukturu i/ili ponašanje integriranog inteligentnog transpornog sustava.

ITS arhitektura važna je iz više razloga, ona osigurava neophodne interopebilnosti različitih dijelova ITS-a, pruža cjelovite informacije o načinu funkcioniranja ITS-a, osigurava dosljednost informacija prema krajnjim korisnicima i uvjete neovisnosti primjenjenih tehnologija uz relativno laku integraciju novih tehnilogija. Arhitektura ITS-a također osigurava uvjete „slobodnog tržišta“ za usluge i opremu jer su sučelja dobro normirana, time se osiguravaju uvjeti povećane proizvodnje (ekonomija opsega) što za posljedicu ima smanjenje cijena za usluge i opremu. Takvim načinom, osiguranim uvjetima „slobodnog tržišta“, potiče se investiranje u ITS. S obzirom na sadržaj i obvezatnost, postoje tri osnovna tipa ITS arhitektura:

Okvirna ITS arhitektura (engl. *Framework Architecture*) primjerena je za nacionalnu razinu, a usmjerena je na iskazivanje potreba korisnika i šire funkcionalno gledište. Može se koristiti kao osnova za razvoj preostala dva tipa ITS arhitekture.

Obvezna ITS arhitektura (*Mandated Architecture*) uključuje fizičko, logičko i komunikacijsko gledište te neke dodatne analize (analizu troškova i koristi, analizu rizika itd.). Sadržaj joj je strogo utvrđen i ograničava mogućnosti opcija u pojedinim izvedbama.

Servisna ITS arhitektura (*Service Architecture*) slična je obveznoj arhitekturi, ali je isključivo vezana za pojedine usluge.

ITS arhitekturu možemo promatrati i u njena tri osnovna dijela. Kao najvažnija ITS arhitektura, javlja se fizička ITS arhitektura koja definira i opisuje dijelove funkcionalne arhitekture koji mogu biti povezani tako da formiraju fizičke entitete, zatim ne manje važna logička ITS arhitektura koja definira unutarnju logiku odnosa pojedinih entiteta, predstavljena je nazivom temeljne funkcije s informacijskim izvorima i odredištima, te komunikacijska ITS arhitektura gdje se definira oblik komuniciranja među entitetima.

Logička arhitektura obuhvaća procese i tijekove podataka među procesima, dok fizička obuhvaća fizičke entitete (elemente opreme) i tijekove podataka među njima. Uspješna ITS arhitektura razumijeva da je logička arhitektura nastala prije svega na temelju stvarnih korisničkih zahtjeva te vizije i ukupnog koncepta primjene, dok se fizička arhitektura razvija na temelju logičke.

Fizička arhitektura uključuje također i komunikacijsku arhitekturu. Pri definiranju fizičke arhitekture posebno treba voditi računa o normizacijskim zahtjevima, kao i strategiji implementacije.

Koncept "dobre" arhitekture uspoređuje se sa arhitektonskim dizajnom građevina. Arhitekt vidi rješenje na globalnoj razini fokusirajući se samo na aspekte koji su ključni za potrebe korisnika i okruženja, detalji sustava nisu razrađeni, ali postoje specifikacije svih svojstava bitnih za korisnika. Iz toga su proizašla 5 osnovna načela "dobre" arhitekture.

Konzistentnost označuje da uz djelomično znanje sustava moguće je predvidjeti ostatak sustava, ortogonalnost predstavlja međusobno neovisne funkcije koje su odvojene u specifikaciji, transparentnost zahtjeva da definirane funkcije moraju biti jasne korisnicima, općenitost da se funkcije mogu višestruko koristiti i kompletnost gdje se zahtjeva visoka razina zadovoljenja potreba korisnika uz postojeća ograničenja.

Kod informacijske sigurnosti jako je bitno da arhitektura sadrži elemente "dobre" arhitekture kako bi se, ukoliko dođe do problema, moglo u što manjem vremenskom periodu doći do adekvatnog rješenja uz što manje negativnog utjecaja na sustav. Zbog boljeg razumjenvanja i pravovremenog djelovanja na moguće probleme, ITS arhitektura se djeli na 4 osnovne razine kako bi se olakšalo rješavanja negativnih utjecaja na sustav. Za početak imamo razinu 0, koja nije dio arhitekture jer se odnosi na dizajn komponenata i ovisi o izabranoj tehnologiji. Tipično se odnosi na dobavljače koji razvijaju pojedine komponente ili podsustave prema fiksiranim ciljevima i standarnim razvojnim procedurama. Razina 1 je definira strukturu sustava te relacije između podsustava, sastoji se od nekoliko posebnih arhitektura, razina 2 definira svojstva i integraciju sustava koji djeluju unutar jedne organizacije (engl. single agency level) te zahtijevaju se multidisciplinarna znanja i primjenjuju različite nestandardizirane procedure, te razina 3 koja uključuje realna ograničenja i djelovanja prema drugim organizacijama, specificira se zahtijevna razina međusobnog povezivanja i interoperabilnosti, ali se uzbor tehnologije prepušta dizajnerima podsustava.

Kada se govori o tipu ITS arhitekture, Američka ITS arhitektura i Europska ITS arhitektura odskaču od ostalih. Glavna razlika između tih dviju arhitektura je u tome što američka ITS arhitektura, kao prva ITS arhitektura koja je predstavljena 1996. godine, ima težište na fizičkom gledištu, dok europska ima težište na potrebama korisnika te na funkcionalnom gledištu. Na temelju američke ITS arhitekture se temeljio razvoj ostalih ITS arhitekture kao i razvoj ITS-a.

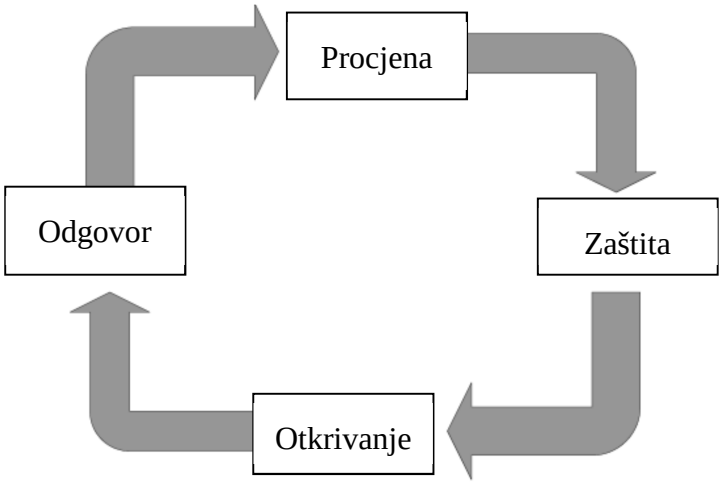
1.2. Informacijska sigurnost

Sigurnost je proces održavanja prihvatljivog nivoa rizika. Znači, sigurnost nije završno stranje nego je to proces koji traje, tj. nije konačni proizvod.

Kada se govori o sigurnosti i zaštiti informacijskih sustava, nekoliko principa danas važe kao osnovni aksiomi o sigurnostI. Sigurnost je proces, sigurnost nije proizvod, usluga ili procedura,već skup koji ih sadrži uz još mnogo elemenata i mjera koje se stalno provode. Ne postoji apsolutna sigurnost, te uz različite metode tehničke zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

Promatrajući sigurnost kao proces, ona sadrži četiri elementa:

- Procjena (engl. assessment)
- Zaštita (engl. protection)
- Otkrivanje (engl. detection)
- Odgovor (engl. response)

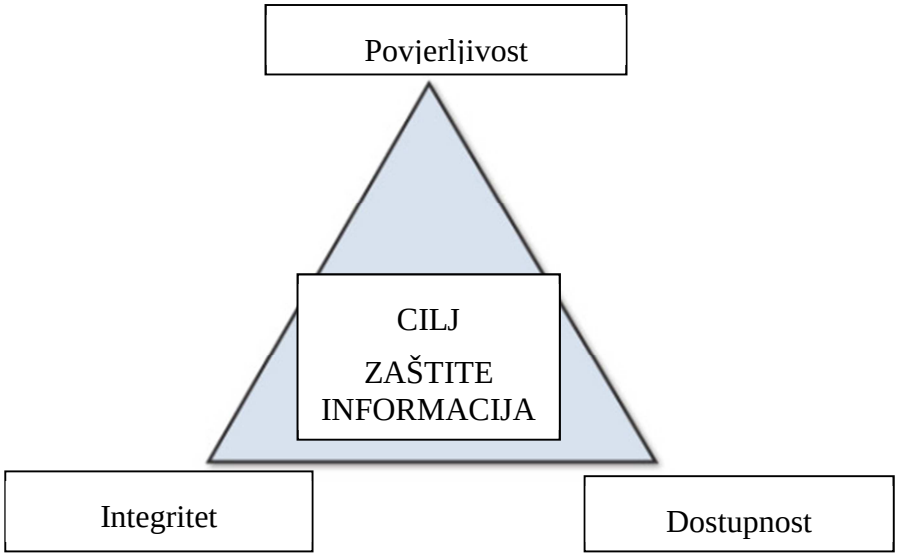


Slika 1: Sigurnost kao proces[17]

Slika prikazuje odnoste između gore navedenih elemenata kao povezanu cjelinu koja čini proces sigurnosti. Taj postupak se ponavlja kako bi se sigurnost sustava održala. Vrlo bitno je rano otkrivanje rizika kako bi se proces mogao nastaviti nesmetano i uz najmanje gubitke.

Informacija je imovina i kao takvu ju je potrebno prikladno zaštititi, kako bi se omogućilo normalno poslovanje neke organizacije. Taj zahtjev postaje sve važniji zbog distribuiranosti poslovne okoline, jer su u takvom okruženju informacije izložene većem broju prijetnji i ranjivosti. Informacije se javljaju u više oblika. Zapisane su na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, prenose se poštom ili elektroničkim putem. Bez obzira u kojem je obliku pohranjena informacija, ona bi uvijek trebala biti prikladno zaštićena. [16]

U današnje vrijeme informacija se predstavlja kao najvažniji resurs u poslovanju, može se reći i da je najskuplja jer ukoliko netko posjeduje informaciju u pravo vrijeme, te ako je ona ispravna i tajna, često je takva informacija od velike važnosti u poslovanju bilo koje organizacije.[17]



Slika 2:CIA triad

Izvor:[17]

Slika prikazuje kako je CIA (Central Intelligance Agency)[2] podjelila ciljeve pri izradi plana za zaštitu informacijskog sustava tako da čini trokut sigurnosti.

Svaki profesionalac koji se bavi zaštitom informacija mora u obzir uzeti ova 3 cilja kao prioritet te ih razmotriti svakog posebno prilikom izrade plana za zaštitu.

[2] CIA – hrv. Središnja obavještajna agencija SAD-a

Za kvalitetan rad i zaštitu informacije potrebno je osigurati:

1. Integritet (*engl. Integrity)* – zaštititi od neovlaštenih izmjena
2. Povjerljivost (*engl. Confidiality*) – zaštititi od objavljivanja tajnih informacija
3. Dostupnost (*engl. Availability*) – zaštitit od uskraćivanja dostupnosti informacija ovlaštenim korisnicima

Kontrola integriteta je temeljena na tri principa:

- dodjela samo nužnih prava pristupa (*engl. need-to-know basis*). Korisnicima se dodijeljuje pravo pristupa samo na one datoteke i programe koji su im potebni kako bi obavljali svoju poslovnu funkciju.
- odvajanje dužnosti (*engl. separation of duties*). Osigurati da ne može samo jedan zaposlenik izvoditi transakciju od početka do kraja. Odgovornost za izvođenje se djeli na dvoje ili više zaposlenika, npr. netko tko ima privilegiju kreiranja transakcije ne bi smio imati privilegiju za njeno izvođenje.
- rotacija dužnosti (*engl. rotation of duties*). Poslovni zadaci bi se trebali periodički mijenjati kako bi korisnicima bilo otežano zlonamjerno preuzimanje kontrole nad transakcijom. Učinkovit princip u kombinaciji sa odvajanjem dužnosti. Za male organizacije je to problem zbog manja osposobljenih zaposlenika. [10]

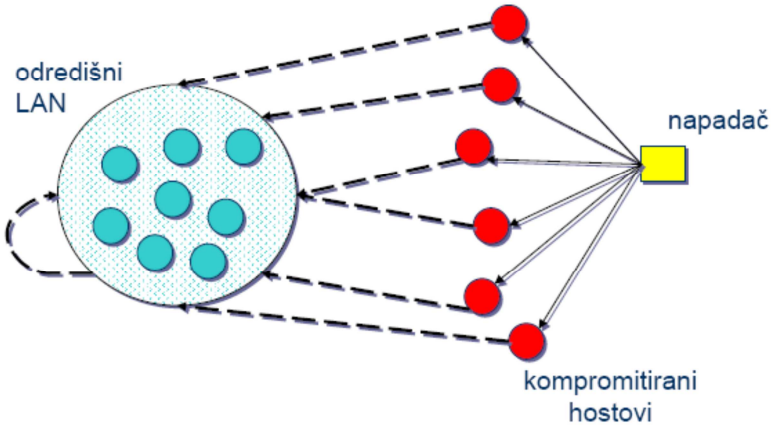
Aspekti povjeljivosti su korisnička identifikacija i autentifikacija. Identifikacije je nužna kako bi se osigurala učinkovitost politike neke organizacije koje za cilj imaju dodjeljivanje pristupa pojedinim podacima.

Najčešće prijetnje povjerljivosti su:

- hakiranje – haker je netko tko preuzima kontroli nad sustavom
- maskiranje – to je proves kojim ovlašteni korisnik pristupa sustavu koristeći lozinke drugih korisnika i na taj način dolazi do pristupa datotekama kojima inače nema pristup
- neovlaštena korisnička aktivnost – pojavljuje se kad autorizirani korisnik dobije pristup datotekama kojima nema pravo pristupa
- nezaštićeno preuzimanje (*engl. download*) datoteka- ako se prilikom preuzimanja datoteka informacije prenesu iz sigurnog okruženja u nesigurno okruženje (npr. na server gdje svi mogu pristupiti)
- lokalne mreže (*engl. Loacal Area Networks*) – posebna prijetnja povjerljivosti informacija jer podaci koji putuju mrežom nigz biti kompromitirani u svakom čvoru mreže
- trojanski konji – mogu kopirati povjerljive datoteke u neovlaštena područja sustava, ukoliko korisnik koji ima pravo pristupa tim datotekama, ne znajući, izvrši takav program

Prijetnje dostupnosti se javljaju u obliku:

- uskraćivanja usluge (*engl. Denial of service – DoS*)



Slika 3: Uskraćivanje usluke (DoS)[17]

DoS je vrsta napada u kojem se obično namjernim generiranjem velike količine mrežnog prometa nastoji zagušiti mrežna oprema i poslužitelj tako da postaju toliko opterećeni da više nisu u stanju procesirati legitimni promet. Kao posljedica nastaje da korisnici ne mogu koristiti usluge poput maila, weba i sl.[18]

- distribuirano uskraćivanje usluge (*engl. Distributed Denial of Service*)- je oblik napada uskraćivanjem usluga u kojem su izvori zagušujuceg mrežnog prometa distribuirani na više mjesta po Internetu. Najčešće se radi o računalima na koja je prethodno provaljeno kako bi ih se iskoristilo za napad na druge mreže ili računala na Internetu.

- gubitak sposobnosti procesiranja podataka kao rezultat prirodnih katastrofa-informacijska sigurnost podrazumijeva zaštitu informacija od velikog broja prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija. Informacijska sigurnost se postiže primjenom odgovarajućih kontrola, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkcije sklopovske i programske opreme.

Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, pregledavati i poboljšavati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahtjeva organizacije.

Definiranje, implementacija, održavanje i poboljšavanje informacijske sigurnosti može biti od presudne važnosti kako bi se ostvarila i zadržala konkurentnost, osigurala profitabilnost, te kako bi se zadovoljile zakonske norme i osigurao poslovni ugled.

Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, špijunaže, sabotaže, vandalizma, požara, poplave i sl. Šteta nanesena organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge je sve prisutnija pojava.

Sigurnost informacijskih sustava može biti ugrožena na više načina. Prijetnje možemo podijeliti prema izvoru:

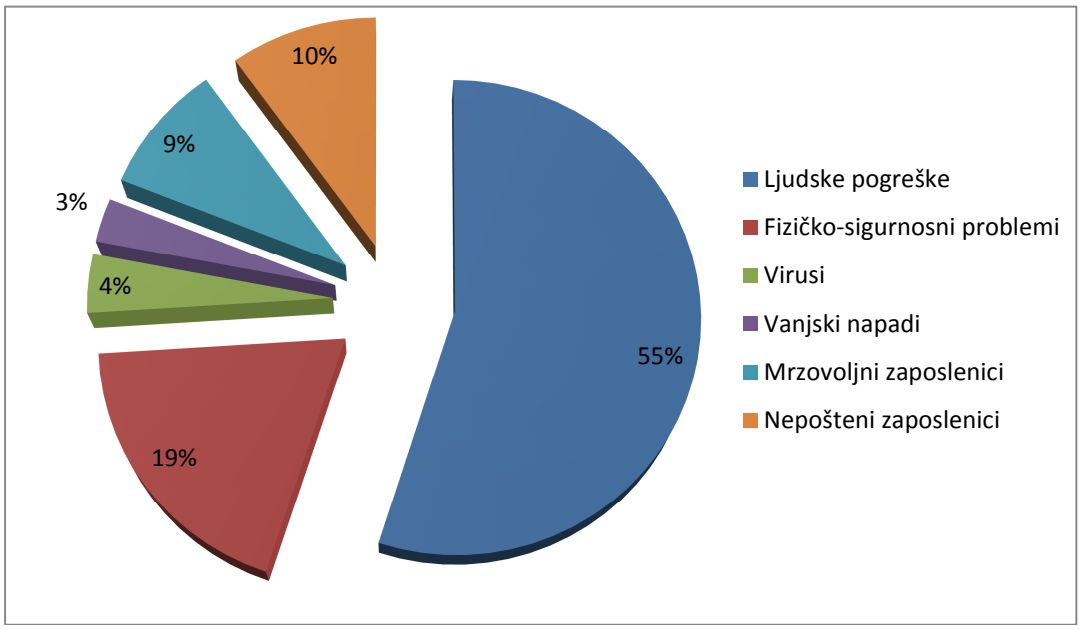
1. ljudi – namjerne prijetnje,
2. ljudi – nenamjerne prijetnje,
3. oprema,
4. prirodne nepogode.

Slika 4: Najčešći izvori prijetnji

Izvor: [19]

Slika prikazuje oblike prijetnji koje dolaze od najčešćih izvora, neke se događaju na svakodnevnoj razini te ih se sankcijama može riješiti dok neke su nepredvidime i na njih ne utječe čovjek tako da se na njih ponekad i teško pripremiti, odnosno riješiti ih ukoliko ne postoji dovoljno stručan i profesional tim ljudi koji su u obzir uzeli i taj segment.

Iako mnogi smatraju da prijetnje sigurnosti sustava naješe dolaze izvana (napadi hakera), istraživanja koja su obavljena i objavljena pokazuju sasvim suprotne činjenice.



Slika 5:Analiza prijetnji sigurnosti sustava

Izvor: [20]

Iz grafikona iznad koji je rezultat višegodišnjeg analiziranja prijetnji sigurnosnih sustava, došlo se do zaključka koji je na početku za neke bio dosta iznenađujući zbog uvida da ljudske pogreške nose najveću prijetnju sustavu. Kod iskusnih informatičara i osoba koje su zadužene za sigurnost sustava ova činjenica je bila opće poznata te su time samo potvrdili svoje zaključke. Vanjski napadi u koje spadaju hakeri su po istraživanjima najmanja prijetnja sigurnosnim sustavima te bi se organizacije, kojima je u cilju imati siguran sustav, ponajprije trebale unutar samih sebe provjeriti i otkloniti pretnje.

Organizacija za ekonomsku suradnju i razvoj (*engl. The Organisation for Economic Cooperation and Development - OEDC*) je ustanovila 9 principa sigurnosti informacijskih sustava:

1. Svijest o informacijskoj sigurnosti - važno je biti svjestan potrebe za sigurnošću informacijskih sustava i zaštitnim sigurnosnim mjerama

2. Odgovornost - svi članovi organizacije su odgovorni za sigurnost informacijskih sustava

3. Odziv - svi članovi organizacije trebaju pravovremeno i kooperativno sudjelovati u spriječavanju, detekciji i rješavanju sigurnosnih incidenata

4. Etika - svi članovi organizacije trebaju postupati respektivno prema legitimnim interesima ostalih

5. Demokracija - sigurnost informacijskih sustava treba biti u skladu s pravilima demokratskog društva

6. Procjena rizika - potrebno je provoditi procjene rizika

7. Dizajn i implementacija sigurnosnih mjera - sigurnosne kontrole trebaju biti sastavni dio informacijskih sustava

8. Upravljanje sigurnošću - organizacija treba uspostaviti jasan pristup upravljanju sigurnošću

9. Promjene - organizacija treba redovito nazdirati sustav informacijske sigurnosti i izvoditi potrebno modifikacije sigurnosnih politika, mjera, procedura i sl.

2. ANALIZA INFORMACIJSKO-SIGURNOSNIH RIZIKA U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

Nakon nesreće 11.9.2001. godine, prometna industrija je pod detaljnim nadzorom. Intenzivan trud od strane vlada, međunarodnih organizacija i komercijalnih interesa širom svijeta usmjeren je na identificiranje procesa, programa i tehnologija koje će spriječiti pojavu daljnjih terorističkih napada. Fokus dosadašnjih napora bio je na „prednjem kraju“ sektora za zračno putovanje, a to su putnici, prtljaga, zaposlenici aerodroma te posada.

Uz te napore, nastavit će se pružati inovacije koje povećavaju razinu sigurnosti diljem svijeta i iako bi bilo nerazborito ne nastaviti u smjeru pojačavanja sigurnosti, slabe točke u prometnoj infrastrukturi nisu ograničene samo na ovaj sektor prometne industrije. Zapravo je „stražnji kraj“ globalnog prometa koji obuhvaća teret, dostavu, logistiku i skladištenje komponente koje su puno podložnije napadu i imaju puno veći potencijal za ljudsku i ekonomsku štetu te zadaje još kompleksniji problem sigurnosti koji treba riješiti.

Pojačano pouzdanje u svjetsku trgovinu gura infrastrukturu globalnog prometa do krajnjih granica. Potreba za ubrzanjem i pojednostavljivanjem prometa tereta povećala je sigurnosne rizike u sve kompleksnijoj mreži međusobno povezanih prometnih usluga. Slabe točke postoje širom te mreže, posebno na „prolaznim točkama“, a to su luke, granice i prometna čvorišta koja omogućuju presudne veze u ovoj globalnoj mreži.

Mogli smo naučiti na primjeru nesreće 11.9. kako jedna razarajuća nesreća u prometnom sektoru može značajno utjecati na svjetsku trgovinu čak i kad se šteta ne dogodi u prijevoznom objektu. Jedan incident vezan uz prijenos tereta na ključnoj prolaznoj točki može uzrokovati rasulo u prometnoj infrastrukturi i dovesti svjetsku trgovinu na mrtvu točku. [5]

2.1. Sigurnosni rizici u prijevozu

Vlada i međunarodne organizacije trenutačno su fokusirane na procjenu sigurnosnih rizika u prometu. Mnoge od ovih inicijativa traže procjenu integracije biometrije za potvrdu identiteta pojedinaca koji imaju pristup kritičnom teretu, sigurnosnim područjima prijevoznih objekata i s time povezanim informacijskim sustavima. To bi trebalo dati ogroman poticaj za usvajanje biometrije u sektoru za prijevoz tereta.

Iako sama biometrija ne može potpuno objasniti sve slabe točke, ali kad bi bila integrirana u kvalitetne sigurnosne sustave mogla bi povećati kvalitetu zaštite te otežati upad počiniteljima terorističkih napada, sabotaža ili krađe, te u isto vrijeme omogućiti inteligentnom društvu više vremena za otkrivanje zavjera i sprječavanje katastrofe prije nego što bude prekasno.

Prilična je debata u prometnoj, sigurnosnoj i biometrijskoj industriji vezana uz razvoj kompleksnih sigurnosnih sustava. I predlagači i kritičari biometrijskih tehnologija ukazuju na visoku razinu zabrinutosti u razvoju i upravljanju centraliziranom vladom ili komercijalnim bazama podataka, vlasništvom, radom i održavanjem nužne infrastrukture informacijskih tehnologija i financijskih izvora za ove nove sisteme.

Bez obzira na prepreke, konsenzus među naprednim industrijskim liderima planira napredak globalne trgovine na način koji će omogućiti uočavanje sigurnosnih prijetnji novog doba, a u napretku će značajnu ulogu igrati biometrija.

Slika 6:Biometrijska detekcija pospanosti vozača[21]

Pospanost vozača, koja je česta pojava na autocestama, te kod velikih teretnih vozila (autobusa, kamiona,..) koja prelaze velike udaljenosti u malo vremenskom periodu, uzrokuje velike probleme u prometu. Biometrijske tehnike koje će vjerovatno u budućnosti biti ugrađene u vozila imat će značajan utjecaj kako bi se izbjegle incidentne situacije. Npr., ukoliko se vozač primakne glavom prema upravljaču vozilo će zvučnim signalom obavjestiti da nešto nije po uputama.

Ukoliko vozač ne pomakne glavu, tj ostane u tom položaju vozilo će automatski oduzimati gas te uključit će se pračenje ceste koje je karakteristika ITS-a te zvučnim signalom “buditi“ vozača. Također postoje i mnoge druge biometrijske tehnike koje bi se mogle iskoristiti u tom slučaju, npr. širenje zjenica, otvorenost očiju, lice, oblik tijela, puls tijela i sl, te na taj način u kombinaciji sa ITS-om djelovati kako bi takva situacija prošla bez žrtava.

Pri analiziranju mogućih čimbenika opasnosti, određivanja prihvatljive razine rizika, dizajniranju adekvatnog i kompromisnog rješenja, kvara sustava ili njegovih komponenti i posljedica, inženjeri i menadžeri susreću se sa raznim problemima. Stvarni sustav nije u potpunosti siguran i bez neželjenih događaja kao što su nesreće. Iz tog razloga potrebno je dobro razumijevanje i sposobnost određivanja rizika kako bi se odredili učinci ITS rješenja.

Rizik je vezan sa nesigurnošću povezanu sa određenim događajima koji su nepoželjni. Inženjerski priručnici definiraju rizik kao potencijalni gubitak ili nagradu koja slijedi iz izlaganja opasnosti ili kao rezultat određenih nepredvidivih događaja. Rizik uključuje vjerojatnost pojavljivanja određenog događaja, posljedice tog događaja, značenje posljedica i populaciju izloženu riziku. Posljedice poput smrtnih stradanja nije odgovarajuće svoditi na financijske iskaze, u tom slučaju se rade posredne kalkulacije.

Pozornost treba usmjeriti na prevenciju pogrešnog ponašanja koji često izazivaju teške posljedice.

Primjeri pogrešnog ponašanja u prometu su:

- prevelike brzine vožnje
- nedovoljan razmak slijeđenja vozila
- oduzimanje prednosti prolaza
- nepoštovanje prometne signalizacije

. Povećani nadzor, detekcija i kažnjavanje prekršaja ne može u potpunosti ukloniti sva neželjena ponašanja zbog toga što svaki sudionik u prometu (pješak, vozač..) ima vlastitu percepciju rizika koji je određen vlastitim iskustvima.

Djelovanjem u realnom vremenu dobiva se sposobnost spriječavanja eskalacije prometnog problema koja kao prednost ima brže i lakše raščišćavanje i normalizaciju prometnog toka.

„Procjena rizika je niz stručnih i znanstvenih aktivnosti kojima se modelira i kvantificira rizik pojave nepoželjnih događaja u određenom sustavu uiz različite scenarije.“[1]

2.2. Prednosti biometrije

U današnjem društvu, napredak u tehnologiji čini nam život puno jednostavnijim i sigurnijim, nova saznanja iz svijeta znanosti sukcesivno njihovim otkrićima implementiraju se u svakodnevni život u vidu različitih izuma,tj. uređaja. Međutim, svaka tehnološka inovacija krije potencijalnu prijetnju korisnicima koja je često skrivena te ju je teško odmah prepoznati. Jedna od glavnih prijetnji je krađa osobnih podataka i privatnih informacija. Danas se ti osobni podaci, zbog napredka tehnologije, nalaze u digitalnom obliku koji je sve dominantniji.

Slika 7:ZET-ov uređaj za registraciju putnika[23]

ZET-ov (Zagrebački električni tramvaj) uređaj koji se koristi u tramvajima za registraciju putnika. Možemo slobodno reći kako je ZET među prvima u Hrvatskoj uveo biometriju u svoja vozila. Na uređaj se registrira preko “pametne kartice“ koja u sebi sadrži sliku, datum valjanosti od kad do kad, ime i prezime, status kartice (osnovnoškolska, srednjoškolska, studenska, radna, umirovljenička..) te ukoliko to netko želi i novčano stanje na toj samoj kartici kako bi se karta mogla kupiti onda kada se uđe u tramvaj. Preko uređaja se lako može provjeriti do kada vrijedi iskaznica, te do kada se koriste prava za prijevoz ukoliko je netko u obrazovnom programu što mu donosi neke benificije.

Biometrija se definira kao mjera neke jedinstvene fizičke osobine i ponašajne osobine osobe po kojoj će se moći identificirati samo ta jedna osoba i onemogućiti mogućnost kopiranja i krivotvorenja podataka. Te karakteristike i osobine se koriste za identifikaciju svakog čovjeka, tj. sve detalje o ljudskom tijelu koji se razlikuje od jednog čovjeka do drugog, će se koristiti kao jedinstvene biometrijske podatke koji će poslužiti kao jedinstvena identifikacijate osobe(ID). To je snimak: mrežnice, šarenice, otisak prsta, otisak dlana i DNK.

Kako se upotreba takvih podataka počela sve više koristiti tako i korisnici pokušavaju informacije osigurati sa šifriranim lozinkama, iskaznicama ili karticama s posebnim pinom. Međutim, pokazalo se da takva mjera zaštite nije najsigurnija s obzirom na porast krađa podataka i dokumenata. Propusti u sigurnosnim mjerama dozvolili su da se dogodi umnožavanje kartica ili krivotvorenja kartica koje se onda zlorabe. Kako bi se povećala sigurnost i dobila bitka protiv cyber kriminala počelo se sve više istraživati na tom području što je dovelo do stvaranja biometrijskih sigurnosnih sustava.

Slika 8: Budućnost biometrije u vozilu [23]

Kako se tehnologija razvija, i sustav zajedno sa okolinom napreduje, možemo očekivati da se u budućnosti neće koristiti ključevi kako bi se vozilo otključalo i pokrenulo. Stvari poput kartica, ključeva, mobitela i sl. vrlo brzo će zamjeniti jedan otisak prsta koji će umjesto toga svega obaviti taj isti posao ali sa puno većom sigurnošću i uz gotovo nimalo rizika. Gledajući tako, krađe će biti gotovo nemoguće, svako vozilo će imati jedinstveni ključ kao što je otisak prsta ili neka druga biometrijska metoda.

Poboljšavanje procesa je ključ usvajanja novih tehnologija diljem svijeta. Suočeni sa ozbiljnim nedostatcima procesa poslovanja, te tehnologijama koje dokazano uklanjaju nedostatke, pobornici "*mainstreama*" integriraju nove tehnologije u postojeću infrastrukturu.

Sigurnosni rizici poslije 11.9. natjerali su transportne opskrbljivače da pomnije pregledaju nedostatke i ulože znatne resurse na procjenu i smanjenje rizika. Biometrija kao takva grana ima i veliki utjecaj na ITS, upravo iz tog razloga što povećava sigurnost, tj. diže se na viši nivo. U teoriji, ITS je definiran kao nadgradnja klasičnog prometnog sustava, a u praksi se to može interpretirati i kao potpuno novo vođenje sustava.

Korištenjem biometrijskih sustava na prometnicama ili u samom vozilu može se puno toga učiniti kako bi se smanjilo čekanje na nekim djelovima gdje je to moguće smanjiti i osigurati da se vozilom upravlja u "normalnom" stanju (ne pod utjecajem alkohola, opijata, kroničnog umora i sl.)

Na kraju će poboljšanje procesa biti ono koje će potaknuti prometna poduzeća na prihvaćanje novih tehnologija, uključujući biometriju. To je posebno dobro i točno s obzirom da dinamika u vrlo promjenjivom prometnom tržištu zahtijeva kontinuiran napredak procesa i vezano je uz smanjenje troška da bi ostali konkurentni na tržištu.

Ova dinamika uključuje neprekidnu regulaciju industrije, ubrzanje globalne trgovine, komunikacije diljem svijeta, intenzivno natjecanje unutar i između prometnih sektora, niske operativne marže i suprotstavljene sile fragmentacije i konsolidacije u pojedinim industrijskim sektorima.

2.3. Biometrijski sustavi u praksi

Usvajanje biometrijskih tehnologija za primjenu prijevoza tereta traje već godinama. Projekti temeljeni na biometriji koji su korišteni u sljedećim studijama, uz iznimku idejnog koncepta graničnog prijelaza SAD/Kanada, dugo su bili u tijeku prije nesreće 11.9.

Pojačanje sigurnosti je bilo samo dio razloga za odabir biometrije. Jednak, ili u nekim slučajevima veći naglasak je bio na potencijalu za povećanu operativnu učinkovitost postignutu pomoću ubrzavanja kretanja tereta i smanjenja papirologije i obrade dokumenata.

Zagovornici biometrije poboljšano osiguranje vide kao velik potencijal za korištenje ove tehnologije za rješavanje mnogih hitnih sigurnosnih pitanja, uključujući krađe, otmice i onečišćenje kritičnog tereta. Kritičari biometrije (i drugih sigurnosnih tehnologija) ukazuju na SAD-ov rat protiv droge kao primjer ozbiljnog neuspjeha velikih industrijaliziranih nacija u sposobnosti kontrole protoka nedopuštene robe preko granica usprkos velikoj predanosti resursima.

3. PREGLED BIOMETRIJSKIH SUSTAVA

Pojam biometrija potječe od grčkih riječi: bios=život i metron=mjera. Prednost biometrijske autentifikacije jest da se fiziološka obilježja ne mogu zaboraviti ili izgubiti, a njihova raznolikost smanjuje mogućnost otuđenja. Svojstvo jedinstveno biometriji je u tome što povećava uporabljivost: sustav je jednostavniji za korištenje jer korisnici više ne trebaju pamtiti lozinke i PIN-ove ili sa sobom nositi kartice i ključeve.

S obzirom na porast sigurnosnih zahtjeva i pad pouzdanosti pobrojenih metoda nadzora ulaska i izlaska iz štićenog prostora, s vremenom su se kao najpouzdanije i najprimjenljivije identifikacijske metode iskristalizirale upravo biometrijske metode,

te daktiloskopija i metoda identifikacije na temelju analize DNK koje također možemo svrstati među metode biometrijske identifikacije. [6]

3.1. Biometrijski sustavi

Biometrijski sustav djeluje u jednom od sljedećih načina a to su registracija biometrijskih podataka, identifikacija i verifikacija te pogreške, koje će detaljno biti objašnjene u nastavku rada.

Četiri osnovna zahtjeva pri izgradnji biometrijskog sustava su:

1. Točnost

- Ne može se točno izmjeriti niti postoji mjerna jedinica u kojoj bi se ona izrazila te ju je moguće samo procijeniti
- Ta procjena se vrši sa razinama pogrešaka koje između ostalog uvršćuju vjerojatnost da će lažni korisnik biti prihvaćen (engl. *False Accept Rate*) ili vjerojatnost da će legalni korisnik biti odbijen (engl. *False Reject Rate*)
- Ove razine pogrešaka često se koriste kao procjena za korisničku populaciju koju ne zanima manipulacija iznimkama.

2. Brzina računanja

- Vrlo je važan faktor koliko brzo sustav može donijeti odluku
- Važno je znati i mogućnosti brzine sustava posebice kada postoji mogućnost povećanja broja korisnika

3. Cijena sustava

- Uključuje cijene svih komponenti sustava

4. Manipulacija iznimkama

- Svaki će biometrijski sustav prije ili poslije doći do problema koji se mora riješiti u procesu manipulacije iznimkama a koji uključuje osobe vještake iz određenih područja
- Može se dogoditi da korisnik ne želi koristiti biometrijski sustav ili spada u populaciju kojoj se ne može izuzeti karakteristika ili jednostavno korisnik ima loš biometrijski dan
- Ti se događaji nazivaju greškama u korištenju (engl. *Failure to Use*), greškama u izuzimanju (engl. *Failure to Enroll*) i greškama u stjecanju (engl. *Failure to Acquire*)

Uz četiri osnovna zahtjeva pri izgradnji biometrijskih sustava potrebno je voditi računa i o:

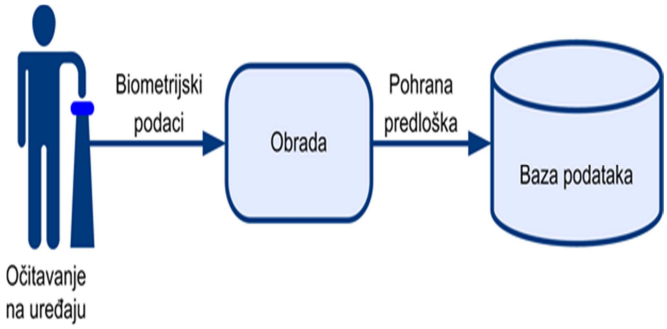
1. Sigurnost
    - Činjenica da odluku donosi biometrijski sustav može se iskoristiti za dokaz autorizacije ili prisutnosti kod senzora, a što postavlja pitanje integriteta biometrijskog sustava
    - Važno je znati i mogućnosti brzine sustava posebice kada postoji mogućnost povećanja broja korisnika

2. Privatnost
    - Postoji bojazan da se biometriju može iskoristiti kao alat za uspostavljanje totalitarnog režima jer je moguće povezivanje lažnih identiteta sa realnim karakteristikama [7]

3.1.1. Registracija biometrijskih podataka

Svaki biometrijski sustav ima svoje posebnosti implementacije koje ovise o primjeni sustava i metodama koje se koriste. Postoje i općenita svojstva zajednička svim sustavima.

Za korisnika prvi susret sa sustavom znači registraciju njegovih biometrijskih podataka (engl. *enrollment*) i upis u bazu podataka. Ovaj se proces može podijeliti u nekoliko faza prikazanih na slici 10.

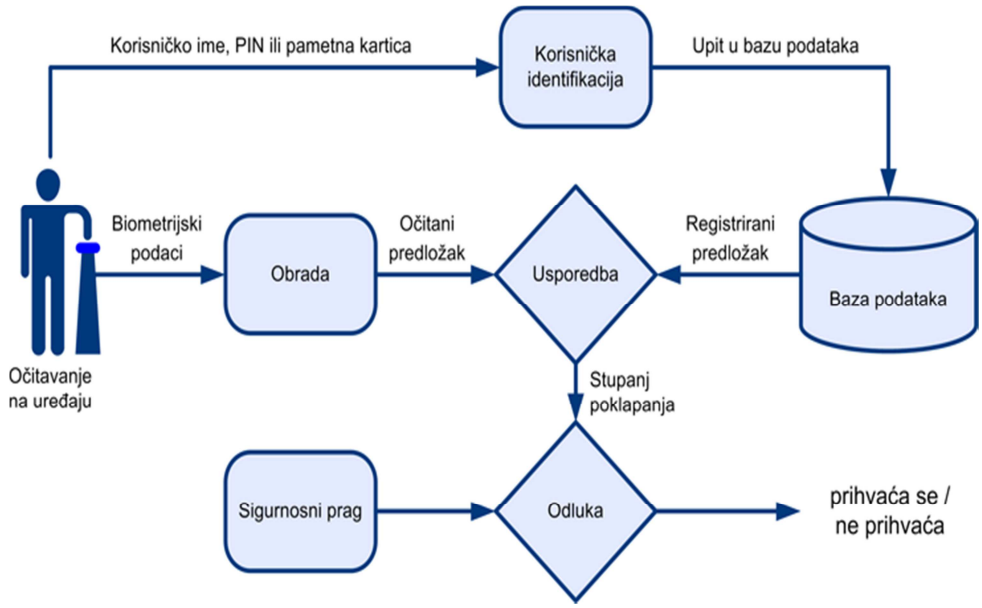


Slika 9: Registracija biometrijskih podataka [6]

Slika 2 prikazuje postupak registracije biometrijskih podataka. Prvo se očitava na uređaju, zatim se obrađuju biometrijski podatci te zatim pohranjuju u bazu podataka. Baza podataka ne može biti izbrisana niti se podaci ne mogu izgubiti te ju to čini puno sigurnijim od ostalih sustava.

3.1.2. Identifikacija i verifikacija

Proces verifikacije sastoji se od usporedbe upravo očitanih podataka sa onima iz korisnikovog predloška. Korisnik mora priložiti identifikacijski podatak pomoću kojeg sustav pronalazi odgovarajući predložak. Taj se podatak može isporučiti u vidu korisničkog imena, PIN-a ili pametne kartice. Proces verifikacije prikazan je na slici 2.



Slika 10: Proces verifikacije korisnika [6]

Identifikacijski podatak može isporučiti i sam sustav pomoću procesa biometrijske identifikacije. U tom se slučaju uneseni biometrijski podatak uspoređuje sa svim podacima iz baze postojećih korisnika. Očito je da ovakav proces može biti neprecizan i dugotrajan, a njegova implementacija skupa i zahtjevna, ali razvojem tehnologije ta dugotrajnost se danas mjeri u sekundama što je ustvari dosta brže nego kod utipkavanja pina na uređaju.

Istraživanja pokazuju kako se očekuje porast brzine učitavanja i do nekoliko stotina puta, što u konačnici znači kako će za jedan takav proces učitavanja. cijelu bazu podataka taj upit proći u samo nekoliko mili sekundi te će se na izlazu dobiti da li se ulaz prihvaća ili ne prihvaća. U samo 10-ak godina tehnologija je napravila velike pomake.

Gledajući memorijske kartice koje su se 2005. godine pojavile za pohranu podataka su imale samo 128 MB-a, što danas prosječnom čovjeku ne dolazi na pamet ni razmišljati o kupnji takve, danas te brojke o memoriji dolaze do prosječnih 128 GB-a. Naravno, nisu samo memorijske kartice osjetile *blitzkrieg* na tržištu u zadnjih 10-ak godina, ima tu i puno ostalih tehnologija. ITS kao takav se nije mogao ni zamisliti prije par godina.

3.1.3. Pogreške

Brzina, upotrebljivost i pouzdanost sustava biometrijske autentifikacije ovise o metodama koje se koriste, stoga je pri projektiranju jako važno temeljito proučiti njihova svojstva i performanse. Kod analize metoda često se proučavaju stope pogrešaka. Dvije su vrste pogrešaka koje se javljaju kod biometrijskih sustava:

1. Pogrešno prihvaćanje (engl. *False Acceptance*), pogreška I. tipa – sustav pogrešno prihvaća osobu kao legitimnog korisnika jer je u bazi pronašao predložak dovoljno sličan unesenom.
2. Pogrešno odbijanje (engl. *False Rejection*), pogreška II. tipa – legitiman korisnik se odbija jer sustav nije pronašao dovoljno podudaranje očitanih podataka s predloškom iz baze. Pogrešno odbijanje predstavlja neugodnost za korisnika, ali smatra se prihvatljivijim od I. tipa jer korisnik može ponovno pokušati s autentifikacijom.

Kako bismo bolje opisali pogreške koje se javljaju uvodimo dva faktora: udio pogrešnih prihvaćanja (engl. *False Acceptance Rate* – FAR) i udio pogrešnih odbijanja (engl. *False Rejection Rate* – FRR).

FAR i FRR ovise o sigurnosnom pragu (engl. *Security Threshold*) koji može biti parametar algoritma usporedbe ili vrijednost s kojom se uspoređuje rezultat dobiven algoritmom. Viši sigurnosni prag znači da će sustav rigoroznije obavljati usporedbu trenutno unesenih podataka s predloškom što će smanjiti broj pogrešnih prihvaćanja i vrijednost FAR-a, ali će povećati broj pogrešnih odbijanja i proporcionalno FRR. Analogno zaključujemo u slučaju smanjivanja sigurnosnog praga gdje će se FRR smanjiti, a FAR povećati.

3.2. Biometrijske metode i mogućnosti njihove primjene u prometu

Metode tjelesne biometrije temelje se na individualnosti i nepromjenjivosti dimenzija pojedinih dijelova ljudskog tijela i njihovih međusobnih odnosa.

Brojni sigurnosni sustavi temelje se na identifikaciji osoba biometrijskim metodama, da bi se utvrdilo je li neka osoba ta za koju se predstavlja. Takva provjera mora biti jeftina, brza, pouzdana, te ne smije zadirati u tjelesni integritet osobe.

U biometrijske metode spadaju:

- otisak prsta,
- šarenica oka,
- mrežnica oka,
- glas,
- prepoznavanje lica,
- termogram lica,
- dinamika potpisa.

Sve metode biti će detaljno objašnjene u nastavku rada.

3.2.1. Otisak prsta

Otisak prsta je najstarija i najpoznatija metoda autentifikacije. Kao metodu sigurne identifikacije poznavali su ga još u staroj Kini, od 1896. godine se koristi za kriminalnu identifikaciju. Zbog toga je identifikacija otiskom prsta dugo korisnicima predstavljala neugodnost. Prihvaćenost se postupno povećava popularizacijom ove metode.

Dvije su vrste čitača danas u upotrebi:

1. Optički čitač otiska prsta reagira na promjene u refleksiji svjetla na mjestima gdje papilarni grebeni dodiruju površinu. Optički senzori su relativno jeftini, rade pouzdano i generiraju sliku zadovoljavajuće kvalitete. Njihov glavni nedostatak su prašina i nečistoća koja se nakuplja na dodirnoj površini.

Ukoliko se radi o ekstremnoj površinskoj nečistoći ona može poprimiti oblik pravog otiska prsta i uzrokovati pogrešno prihvaćanje. Zato ovakav uređaj ima kratak vijek trajanja i treba ga redovito održavati. Optički čitač reagira na pritisak i može se lako zavarati korištenjem trodimenzionalnog modela prsta, stoga se u njih često ugrađuje detektor živosti prsta.

2. Silicijski čitač otiska prsta zasniva se na kapacitivnosti prsta. Sastoji se od mreže površinom malih kapaciteta, gdje je njegova površina jedna, a prst druga ploča. Čitač registrira grebene prsta koji prelaze iznad uređaja zbog većeg kapaciteta od udubljenih dijelova. Ovakvi čitači su mali, jeftini i brzi, a nedostatak im je preosjetljivost kapacitivnosti na vlagu i znoj.

Slika 11- Otisak prsta [6]

Slika 12 prikazuje primjer otiska prsta. Čitače otiska prstiju danas nalazimo posvuda, a ugrađuju se čak i na osobna računala, pametne telefone, ulaze u zgradu i sl. Prije tehnološkog razvitka otisak prstiju se davao na način tako da se prst, jedan po jedan, umočio u tintu te ostavljao trag na nekom papiru koji se poslije spremao u registratore kao identifikator. Danas su te metode puno praktičnije te nema zamazanih prstiju nego sve ide preko digitalnog čitača koji radi sliku otiska u puno boljoj rezoluciji od onog ručnog jer u slučaju povrede na prstu digitalno će po jednom malom djeliću prsta moći prihvatiti ili odbiti upit.

Slika 12:Uređaj za očitavanje otiska prsta [23]

Otisak prsta je dosta korištena biometrijska tehnika te je ona u zadnje vrijeme počela imati primjenu i na pametnim telefonima za otključavanje. Ovakvih uređaja u budućnosti će biti sve više, gdje god da ovakav uređaj nađe svoju primjenu, imat će pozitivne strane. Npr., na ulasku na aerodrom, ovak uređaj bi osigurao da se blokira ulaz osobama kojima je zabranjen odlazak iz države i razloga koji su poznati njemu ili sudu, zabrana ulaska na stadion ukoliko nije kupljena karta ili je već odprije poznat policijskim snagama te mu je izrečena kazna zabrane odlaska na koju se odlučio oglušiti i mnoge druge.

Pojavom ITS-a očitavanje prstiju dobilo je sasvim novu dimenziju, biometrijski gledano čitači prstiju se koriste već duže vrijeme i uz napredak tehnologije otisci kao identifikatori se nalaze na gotovo svakom osobnom dokumentu, ali očitavanje prsta se koristi za mnoge uporabe, npr. ulaz u zgradu, ulaz na pametni telefon, ulaz u automobil i sl. Svakim danom uporaba čitača otisaka se povećava.

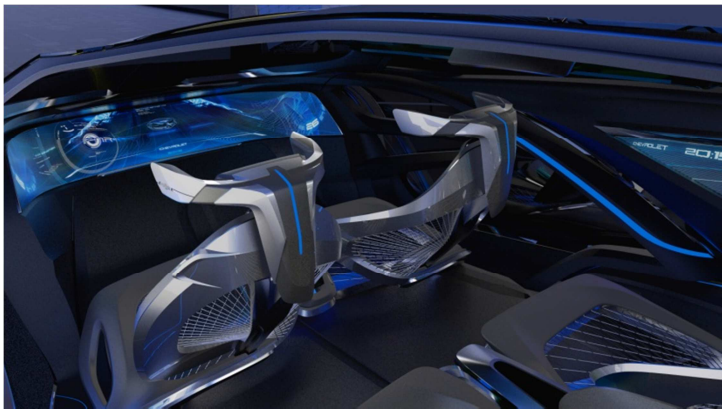
3.2.2. Šarenica oka

Šarenica (engl. *Iris*) je obojeni dio oka koji okružuje zjenicu, a sastoji se od prstena, brazdi i pjega u različitim bojama, koji čine jedinstveni vremenski nepromjenjiv kompleks boja i šara kod svakog pojedinca.

Šarenica ispunjava pretežiti broj zahtjeva koji se traže za identifikacijska obilježja. Univerzalna je, trajna (svoj izgled poprima u najranijem djetinjstvu i ne mijenja se tijekom vremena), nemoguće ju je mijenjati bez velikog rizika od gubitka vida.

Sustav za identifikaciju na temelju šarenice ne može se prevariti lećama, staklenim ili pravim okom odstranjenim s mrtvog čovjeka. Naime, kad je riječ o lećama postoje algoritmi koji registriraju leće, a kod staklenog oka ili oka mrtve osobe nema očekivane kontrakcije ili širenja zjenice pri obasjavanju oka. Ova tehnika identifikacije vrlo je jednostavna i pouzdana, neinvazivna je jer nije potreban fizički kontakt osobe sa skenerom. Može se obaviti i snimanjem šarenice oka s običnom kamerom s udaljenosti i do pola metra. Za pregled baze potrebno je par sekundi.

Prepoznavanje osoba skeniranjem šarenice (irisologija) jedna je od najpouzdanijih biometrijskih metoda, ponajviše zbog prirodnih karakteristika šarenice. Metoda je pogodna kako za provjeru tako i za utvrđivanje identiteta.



Slika 13- Prikaz uređaja u vozilu koji reagira na šarenicu oka [8]

Slika 14 prikazuje što se u budućnosti može očekivati, te što ćemo sa svojom šarenicom oka moći učiniti. Na šarenici je definirano oko 200 karakteristika, koje su pogodne za identifikaciju. To je ravna struktura i svaka šarenica je jedinstvena u svojoj boji, uzorku i strukturi. Vaše dvije šarenice vas mogu identificirati kao što to mogu otisci prstiju. Boja šarenice se tokom prvih godina života mijenja, a do promjena može doći čak do desete godine života. Boja ovisi o količini pigmenta kojeg šarenica sadržava.

U šarenici se nalaze dva mišića:

- **Sfinkter**, mišić koji stišće zjenicu i ograničava količinu svjetla koje može ući u oko, te putovati kroz očnu leću do mrežnice. Što je zjenica manja, to je šarenica veća.

- **Dilatator**, mišić koji proširuje zjenicu pri slabom osvjetljenju, kako bi se povećala količina svjetla koje ulazi u oko. Širenje zjenice smanjuje veličinu šarenice.

Boja šarenice se može bolje izraziti ili potpuno promijeniti kontaktnim lećama u boji. Šarenica oka je podijeljena na 12 segmenata i 7 koncentričnih krugova sa središtem u zjenici oka.

Smatra se da šarenica desnog oka odražava zdravlje desne strane našeg tijela, dok šarenica lijevog oka lijeve strane.

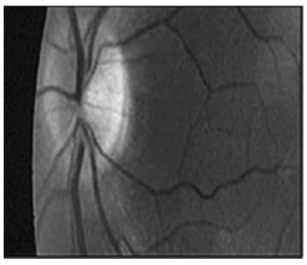
Parni organi mogu se naći i u jednoj i drugoj šarenici sa jednom iznimkom: srce se pojavljuje u obje šarenice.

3.2.3. Mrežnica oka

Mrežnica je tanki sloj stanica, splet krvnih žila koji se nalazi u stražnjem dijelu oka. Njena struktura je individualna, jedinstvena karakteristika svake osobe.

Za uspješno skeniranje mrežnice oka potrebno je skinuti naočale i oko približiti skeneru, te fokusirati pogled na određenu točku. Proces skeniranja traje između 10 i 15 sekundi i oko se za vrijeme skeniranja osvjetljava blagim snopom svjetlosti, zbog čega ova metoda spada u neugodnije i nametljive biometrijske metode.

Zbog visoke cijene, ali i visoke pouzdanosti ova metoda koristi se u područjima i objektima visokog stupnja sigurnosti gdje cijena opreme nije odlučujući čimbenik.



Slika 14- Prikaz mrežnice oka [8]

Slika prikazuje mrežnicu oka. To je jedno od najsigurnijih biometrijskih identifikacijskih obilježja, jer nije moguće promijeniti ili replicirati unutarnju strukturu oka, niti se ona mijenja tijekom čitavog života, a mrežnica mrtve osobe toliko brzo propada da nisu neophodne dodatne mjere utvrđivanja znakova smrti.

Mrežnica (lat. *retina*) je unutarnja ovojnica oka. Smještena je na stražnjem dijelu očne jabučice i njezin je najvažniji dio. Sadrži vidne stanice, štapiće i čunjiće koji pomažu u osjetu svjetla i raspoznavanju boja. Povezane su sa živčanim vlaknima koja se udružuju u vidni živac. Kod odraslog čovjeka mrežnica čini 72% kruga i ima oko 22mm u promjeru.

Dio mrežnice čini optički disk koji se ponekad naziva i slijepom pjegom jer u tom području nema fotoreceptora. U presjeku nije deblja više od 0,5mm. Ima tri sloja živčanih stanica i dva sloja sinaptičkih spojeva.

Skeniranje mrežnice uz napredak tehnologije možemo u budućnosti očekivati na graničnim prijelazima gdje ćemo ostavljati svoju skeniranu sliku u bazu podataka te po povratku potvrditi svoj povratak kako bi se omogućilo lakše pronalaženje ukoliko to bude potrebno.

3.2.4. Glas

Cilj autentifikacije glasom jest utvrditi tko je govornik uspoređujući pohranjeni uzorak s trenutnim. Oslanja se na karakteristike glasa, a ne na izgovor pojedinih riječi. Karakteristike glasa ovise o građi glasnica, grla i usne šupljine, ali i o naučenim karakteristikama (tempu i stilu govora). Kako bi se mogla obaviti usporedba, potrebno je pri registraciji od korisnika zatražiti da izgovori neku frazu. Kada korisnik obavlja autentifikaciju najčešće treba izgovoriti istu tu frazu. Takav sustav je vrlo podložan prijevarama u kojima se glas legitimnog korisnika snimi i kasnije reproducira pri autentifikaciji. Veća sigurnost postiže se tako da sustav zatraži od korisnika da svaki put izgovori drugi tekst, koristeći neku vrstu pitalice na koju korisnik treba odgovoriti. Budući da je broj pitanja i odgovora pohranjenih u sustavu ograničen prijevare su i dalje moguće. Postoje i sustavi kod kojih se zadaje tekst čiji izgovor prethodno nije pohranjen od strane korisnika. Iako to donekle rješava problem s varalicama sustav mora prepoznavati govor da bi zaključio je li izgovorena fraza zbilja pravi odgovor na pitanje.

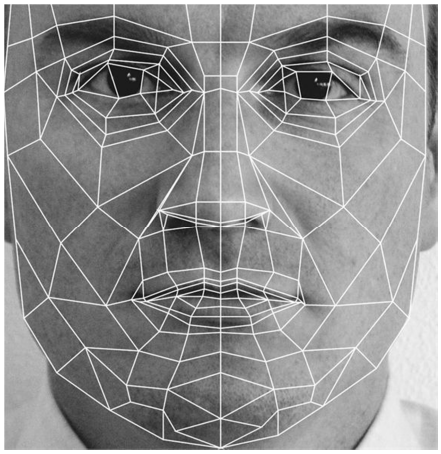
Slika 15:Prepoznavanje glasa na središnjem računalu vozila [14]

Vrlo zanimljiva metoda koja će nam u budućnosti puno vremena uštedjeti, možda neće naći primjenu u prometu, ali u nekim izoliranim prostorima će imati široku uporabu. Glas je specifičan jer iako ima ljudi koji zvuče dosta slično, opet postoje naglasci na neke riječi koje ih razlikuju u podpunosti. Nemoguće je "prekopirati" nečiji glas te tako zaobići tu zaštitu. U prometu bi veliki utjecaj imala buka i vanjski zvukovi tako da primjena ovakvog sustava bi bila otežana i gotovo nemoguća.

Prednost ovakvih sustava je što koriste uobičajenu, jeftinu i lako nabavljivu hardversku opremu – mikrofon i zaslon. Sustav je vrlo prihvatljiv i nenametljiv za korisnike. Nažalost, performanse i mogućnosti zaobilaženja nisu tako dobre. Sustav je osjetljiv na pozadinsku buku, a glas varira ovisno o dobi i raspoloženju korisnika.

3.2.5. Prepoznavanje lica

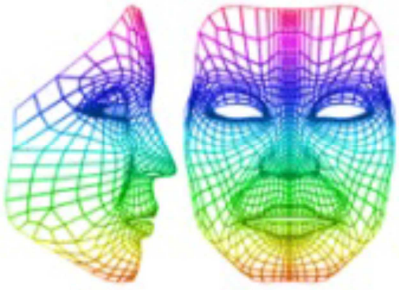
Prepoznavanje lica najprirodniji je način prepoznavanja među ljudima. U novije vrijeme koristi se kao metoda biometrijske autentifikacije gdje računalo uspoređuje korisnikovu trenutno dohvaćenu sliku lica s pohranjenom. Postoje dvodimenzionalni i trodimenzionalni algoritmi za usporedbe lica.



Slika 16:Prepoznavanje lica [12]

Slika prikazuje crte lica čovjeka pomoću kojeg bi se vrlo lako mogao napraviti fotorobot. Metoda koja u budućnosti neće imati preveliku ulogu, ali će u nekim slučajevima biti od pomoći. Po nekim određenim točkama lica koje su različite kod svake osobe, spraja sa slikom iz baze podataka te sužuje krug potrage za pravom osobom. Metoda bi se mogla korisititi u slučaju nekih prometnih nesreća gdje se zbog težine ozlijeda neke druge metode neće moći ni probati korisititi.

Među dvodimenzionalnim, najpoznatiji su algoritmi svojstvenih lica i facijalne metrike. Algoritam svojstvenih lica uspoređuje lice korisnika s unaprijed unesenim slikama ljudskih lica (engl. *eigenface*) – najčešće s njih 100 do 150. Za svako ljudsko lice izračunava se stupanj poklapanja s korisnikovim licem, a potom se matrica sa stupnjevima poklapanja pohranjuje kao korisnikov predložak koji zauzima vrlo malo diskovnog prostora. Algoritam facijalne metrike analizira položaje i relativne udaljenosti između dijelova korisnikovog lica (nosa, usta i očiju) te informacije o njima zapisuje u predložak. Dvodimenzionalni algoritmi se lako mogu zavarati podmetanjem slike legitimnog korisnika. Kvaliteta prepoznavanja ovisi o kutu upada svjetlosti na lice korisnika i promjeni kuta gledanja u kameru. Problem predstavlja i promjenjivost lica starenjem, mijenjanje frizure, šminke, izraza lica i brade ili nošenje naočala. Zbog toga dvodimenzionalne metode imaju visok EER i nisu upotrebljive za identifikaciju.



Slika 17: Biometrijski uzorak prepoznavanja lica [12]

Trodimenzionalni algoritmi analiziraju i pohranjuju 3D karakteristike i veličine dijelova lica. Time se izbjegavaju problemi koji karakteriziraju dvodimenzionalne metode jer svojstva trodimenzionalnog modela ne zavise o izrazu lica, nošenju šminke ili zakrenutosti glave. Svojom točnošću metoda 3D analize konkurira skeniranju šarenice.

Algoritmi za usporedbu lica brži su od onih za usporedbu šarenica, a kamere za dohvat slike lica jednostavnije za rukovanje. Ova biometrijska tehnologija je jedna od relativno jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu. Dovoljno je osobno računalo i video kamera. U praksi je dovoljno da osoba prođe pored kamere i da ju sustav zabilježi, dok se prepoznavanje osobe obavlja pomoću prepoznavanja oblika.

Jedna varijanta biometrijske metode koja je slična metodi prepoznavanja lica, je metoda prepoznavanja uha. Naime, oblik uha i struktura hrskavog tkiva na površini uha različiti su među osobama, ali to nije velika jedinstvenost pa ova metoda nije često korištena. Pristupi prepoznavanju uha temelje se na poklapanju vektora duljine izbočenih točaka na površini od lokacije graničnih znakova na uhu.

3.2.6. Termogram lica

Termogram lica je nova i perspektivna biometrijska metoda koja još nije našla komercijalnu primjenu. Lice svakog čovjeka prožeto je razgranatim mrežama krvnih žila. Jedinstvenost dobivenih uzoraka je velika i za razliku od metode prepoznavanja lica slike se mogu prikupljati bez obzira na osvjetljenje u okolini.

Prednost je nenametljivost prema korisniku od kojeg se traži samo da pogleda u kameru. Prepoznavanje funkcionira neovisno o dobi, izrazu lica i estetskim modifikacijama. Zbog visoke točnosti i brzine metoda je pogodna za identifikaciju. Razlog zašto još nije ušla u komercijalnu primjenu je skupoća potrebne opreme, odnosno infracrvene kamere.

Slika 18- Termogram lica [6]

Slika prikazuje termogram lica. Mreža je jedinstvena za svakog čovjeka, čak i za blizance. Iz nje se širi toplina koja se može očitati infracrvenom kamerom. Identifikaciju je moguće obaviti pod različitim svjetlosnim uvjetima i u mraku.

Ova metoda omogućuje prepoznavanje osobe bez njezine suradnje te snimanje s veće udaljenosti, zbog toga pripada skupini neinvazivnih metoda identifikacije.

S pomoću termovizijskih kamera metoda se često primjenjuje u nadzoru državnih granica.

3.2.7. Dinamika potpisa

Prepoznavanje dinamike potpisa zasniva se na načinu na koji nastaje potpis i obično ne uzima u obzir izgled samog potpisa.

Postoje dva načina da se dohvate ti podaci:

Ploča osjetljiva na dodir (engl. *tablet*) registrira pokrete i pritisak olovke na površinu.

Pametna olovka funkcionira kao svaka druga olovka – ima tintni uložak kojim se korisnik potpisuje na papir. U pametnoj olovci se bilježe pokreti u sve tri dimenzije kao i pritisak na površinu.

Prednost ispitivanja dinamike potpisa je što se ne može krivotvoriti proučavajući zapisani potpis korisnika. Krivotvorenje može uspjeti samo ako zlonamjerna osoba proučava način na koji se korisnik potpisuje. Pokazuje se da to i nije tako teško jer se sposobnost lažiranja povećava već i nakon nekoliko proučavanih potpisivanja korisnika. Veličina podataka dobivenih iz svakog potpisa je oko 20 kB, obrazac dobiven iz 3 do 10 potpisa zauzima od 90 B do 1 kB. Usprkos veličini obrasca EER za ovu metodu je jako visok i metoda nije pogodna za identifikaciju.

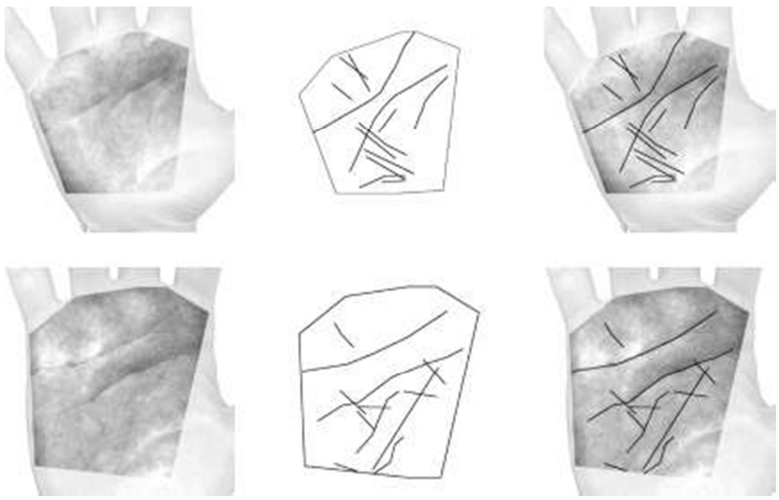
Ova tehnologija koristi dinamičku analizu potpisa kako bi autentificirala osobu. Tehnologija je bazirana na mjerenju brzine, pritiska i kuta koje koristi osoba kada se potpisuje ili kada piše nespecificirani tekst. Jedno od smjerova prema kojima se je usredotočila ova tehnologija su i e-business aplikacije, ali i druge aplikacije gdje je potpis prihvaćen kao metoda osobne autentifikacije.

Svoju primjenu nalazi na svim osobnim dokumentima te je jedan od najstarijih načina dokazivanja identiteta. Potpis je kao ime i prezime te ga je praktički nemoguće 100% iskopirati.

3.2.8. Ostale metode

1. Geometrija dlana

Metoda geometrije dlana oslanja se na različitost oblika dlana i prstiju u malim i srednje velikim skupinama. Može se analizirati sjena ruke ili trodimenzionalni oblik.



Slika 19:Primjer izlučenih linijskih segmenata [13]

Slika prikazuje geometrijske oblike koje nastaju prislanjanjem dlana o ravnu površinu te uz taj geometrijski oblik postoje linije koje se presjecaju kod svakog čovjeka drugačije. Za ovu metodu je teško očekivati njeno korištenje kao prioritetno zbog toga što pogreška može vrlo lako doći do izražaja. Npr. ukoliko dođe do porezotine, linije više neće imati isti broj preklapanja nego će svaka linija dobiti još jednu točku preklapanja te bi odmah time odbilo pristup. U nekim slučajevima bi ova metoda možda bila i jedina moguća za korisiti tako da ju ne treba umanjivati, ali napredkom tehnologije, druge metode su puno brže i prihvaljivije.

2. Termogrami dlana i tijela

Termogrami dlana i tijela imaju vrlo slična svojstva termogramu lica. Snimke dobivene infracrvenom kamerom govore o položajima krvnih žila i vena koji su jedinstveni za svakog čovjeka. Za razliku od termograma lica, istraživanje metoda termograma dlana i tijela je još u začecima.

3. DNA

Metoda usporedbe uzoraka DNA još nije sasvim pogodna za automatiziranu upotrebu. Postupci prikupljanja tkiva su vrlo nametljivi za korisnike. Usporedbe uzoraka traju 5-10 minuta, stoga se metoda usporedbe DNA zasad koristi isključivo u forenzici. Čitanje jedinstvenog DNK - deoksiribonukleinske kiseline (eng. DNA – Deoxyribonucleic Acid) je grana biometrije koja se bavi prepoznavanjem DNK osobe.

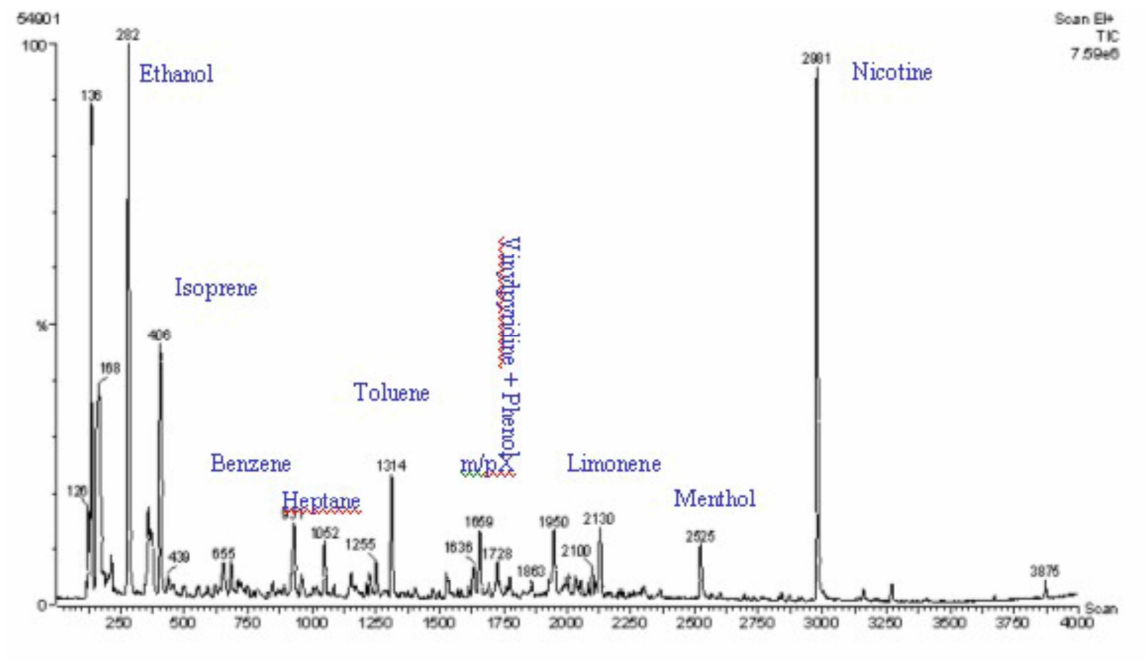
S pretpostavkom da svaka osoba sadrži sebi svojstveni DNK, pristupilo se mogućnosti izrade svojevrsnog čitača DNK zapisa. Pošto se očita DNK neke jedinke, isti se uspoređuje s pohranjenih zapisom u bazi podataka i na taj je način moguće provoditi autentikaciju korisnika prilikom pristupa nekom sustavu ili prostoru.

U kombinaciji s drugim biometrijskih tehnikama može se osigurati vrlo visoki stupanj zaštite i prepoznavanje ukoliko se doista radi o osobi kojoj su pridodana izvjesna ovlaštenja.

Ova tehnika se može upotrijebiti i u vojne i civilne svrhe, a postoji velika vjerojatnost da će se u budućnosti podaci o osobnoj DNK pohranjivati i u osobnoj iskaznici. DNK analiza se danas koristi u brojnim sferama kao što su dokazivanje očinstva ili rodbinske povezanosti ili u pravosuđu u kojem su na taj način identificirani brojni kriminalci, ali su i brojni neopravdani osuđeni zatvorenici pušteni na slobodu.

4. Miris

Miris se zasniva na skupu kemijskih izlučevina ljudskog tijela i jedinstven je za svakog čovjeka. Analizom mirisa mogu se ustanoviti podaci o aktivnostima pojedinca što uzrokuje zabrinutost korisnika za vlastitu privatnost, npr. kod alkoholiziranih vozača miris je puno intenzivniji nego kod normalnih vozača.



Slika 20: Krivulje koje opisuju dinamiku mirisa za različite spojeve[7]

Svaki objekt u prirodi ima svoj miris koji je karakterističan za njegov kemijski sastav. Biometrijski sustavi koji detektiraju mirise rade na principu upuhivanja zraka preko kemijskih senzora od kojih je svaki osjetljiv na određenu grupu mirisa, tj. na njegova kemijska svojstva. Miris se opisuje mjerenjima obuhvaćenom od senzora i u njegovom intenzitetu na svakome od njih.

Pošto miris ima više funkcija u prirodi kao što su komunikacija, privlačenje partnera, zaštita okoliša ili obrana, onda se može upotrijebiti i u civilne, ali i u vojne svrhe.

Pretpostavljajući da svaka osoba sadrži karakterističan miris, moguće je po parametrima svakog od senzora odrediti o kojoj se osobi radi i odrediti glavnu notu mirisa od sporedne. Posebno je važno razlikovati miris osobe od parfema na njoj pa je u tom polju potrebno još istraživanja kako bi se odijelili mirisi.

5. Dinamika tipkanja

Svaki korisnik ima svoj jedinstveni način tipkanja definiran vremenom potrebnim da napravi prijelaz između kombinacije tipki i duljinom pritiska. Softverski sustav može kontinuirano pratiti dinamiku tipkanja i obavljati autentifikaciju korisnika. Nedostatak je što dinamika tipkanja spada u naučeno ponašanje i mijenja se s vremenom. [9]

Ova tehnika se razvila tijekom drugog svjetskog rata u primjeni kod radiotelegrafista jer je uočeno da se po brzini tipkanja mogu razlikovati pošiljatelji poruka. Ako se danas govori o dinamici tipkanja onda se podrazumijeva dinamika tipkanja po tipkovnici.

Kao tehnika je vrlo nenametljiva jer nije potrebno uvoditi nikakve dodatne uređaje za detektiranje, osim zvučne kartice. Eventualno je moguće posjedovati i specijalizirani program koji bi na razini operacijskog sustava pratio korisnikovo tipkanje.

Glavna karakteristika na kojoj se ova tehnika bazira je vremenski razmak između korisnikovog pritiskanja na tipkovnicu.

3.2.9. Usporedba biometrijskih tehnika

U sljedećoj tablici prikazana je paralelna usporedba više biometrijskih tehnologija s obzirom na sljedeće karakteristike:

- univerzalnost - opisuje u kojoj mjeri se tehnika može primijeniti u svakodnevici,
- jedinstvenost - opisuje u kojem postotku je navedena kategorija jedinstvena s obzirom na pojedinca,
- trajnost - opisuje promjenjivost s obzirom na vrijeme tj. koliko pojedinac zadržava navedenu karakteristiku,
- prikupljivost - opisuje s kojom lakoćom se dobiva uzorak navedene kategorije,
- izvedivost - opisuje u kojoj mjeri je moguće u praksi implementirati navedene biometrijske metode i
- prihvatljivost - opisuje u kojoj mjeri je moguća implementacija, a da se ne naruše ljudska prava.

Tablica 1: Usporedba biometrijskih tehnika prema univerzalnosti, jedinstvenosti i trajnosti, prikupljivosti, izvedivosti i prihvatljivosti

BIOMETRIJE METODE	UNIVERZALNOST	JEDINSTVENOST	TRAJNOST	PRIKUPLJIVOST	IZVEDIVOST	PRIHVATLJIVOST
Lice	Visoka	Niska	Srednja	Visoka	Niska	Visoka
Otisak prsta	Srednja	Visoka	Visoka	Srednja	Visoka	Srednja
Geometrija dlana	Visoka	Srednja	Srednja	Visoka	Srednja	Srednja
Šarenica	Visoka	Visoka	Visoka	Srednja	Visoka	Niska
Mrežnica	Visoka	Visoka	Srednja	Niska	Visoka	Niska
Termogram	Visoka	Visoka	Niska	Visoka	Srednja	Visoka
Uho	Srednja	Srednja	Visoka	Srednja	Srednja	Visoka
DNK	Visoka	Visoka	Visoka	Niska	Visoka	Niska
Potpis	Niska	Niska	Niska	Visoka	Niska	Visoka
Glas	Srednja	Niska	Niska	Srednja	Niska	Visoka
Dinamika tipkanja	Niska	Niska	Niska	Srednja	Niska	Srednja
Miris	Visoka	Visoka	Visoka	Niska	Niska	Srednja
Hod	Srednja	Niska	Niska	Visoka	Niska	Visoka

Izvor: [5]

U Tablica 1 se nalazi rezime biometrijskih tehnika koje su nastale na temelju istraživanja i testiranju na ljudima. U tablicama su iskazane mjerljive veličine koje utječu na njihovu adaptaciju i korištenje u svakodnevnom životu, mnoge od njih se još uvijek testiraju, ali vrlo brzo će postati praksa da se u djeliću sekunde može identificirati svaki čovjek na nekoj virtualnoj karti gdje će se moći pratiti i kretanje, a i stanje organizma pomoću tih biometrijskih tehnika. U prometu bi se moglo iskoristiti dosta tehnika u samom vozilu kako bi se spriječile krađe, ali i incidentne situacije što bi u konačnici u kombinaciji sa ITS-om uveliko smanjilo broj nezgoda i učinilo transport sigurnijim.

4. PRIMJERI IMPLEMENTACIJE BIOMETRIJSKIH RJEŠENJA U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

Od kasnih 90-ih, nepoželjni ili neuobičajeni uvjeti vožnje su jasno identificirani kao primarni uzrok automobilskih nesreća i smrti na cesti. Taj je problem privukao pažnju znanstvene zajednice koja je počela proučavati razvoj inteligentnih i prilagodljivih sustava, primarno naprednih voznih pomoćnih sustava ADAS (engl. *Advanced Driver Assistane Systems*) prikladnih za nadzor vozačeve budnosti i davanje potpore za izbjegavanje nesreće u pravom vremenu.

Liang i *Lee* u svome radu iz 2014. godine kažu: „Priroda vozačeve nepažnje varira. Umor i povezani simptomi kao što je pospanost i često klimanje glavom su vrlo česti u realnim situacijama, ali distrakcije od sigurne vožnje mogu također imati vizualne ili kognitivne uzroke.“ [26]

Vizualna ometanja često su vezana uz prisutnost elektroničkih uređaja kao što su mobiteli, navigacijski i multimedijski sustavi koji zahtijevaju aktivnu kontrolu od strane korisnika (vozača) kao npr. pritiskanje gumba ili okretanje ručica. Vizualne smetnje također mogu biti povezane s prisutnošću istaknute vizualne informacije dalje od ceste, koja uzrokuje spontano svraćanje pogleda s ceste i kratkotrajno okretanje glave.

Kognitivne smetnje nastaju kad vozač nije dovoljno fokusiran na svoj kritični zadatak odnosno sigurnu vožnju. Simptomi kognitivnih smetnji su manje vidljivi i teže uočljivi i mjerljivi pomoću objektivnih pokazatelja. Stoga se u većini slučajeva analiza kognitivnih smetnja bazira na dužem vremenskom praćenju ponašanja i sofisticiranim statističkim tehnikama.

S fokusom na umoru i vizualnim distrakcijama, istražuje se dizajn i razvoj potpuno automatiziranog sistema pomoći vozaču baziranog na naprednim tehnologijama koje se bave analizom slika i srodnih polja kao što su prepoznavanje obrazaca i biometrija. [10]

U prethodnim studijama, tehnike kompjuterskog vida često su bile predložene za detekciju pažnje vozača sa standardnim i dnevno-noćnim infracrvenim kamerama. Drugim riječima, ove tehnike usvojene su da otkriju znakove vizualne distrakcije, kao što je smjer pogleda izvan ceste i često okretanje glave te promjene u izrazu lica koje su karakteristične za osobe sa smanjenom opreznošću kao posljedicom umora. Dulje trajanje treptanja, sporiji pokreti kapaka, smanjeno otvaranje očiju, klimanje glavom, zijevanje te pogrbljeniji stav neki su od najzanimljivijih simptoma uhvaćenih pomoću vizualnih tehnika.

Česta shema obrade vozačevih karakteristika uključuje sljedeće korake:

- Lokalizaciju lica,
- Lokalizaciju dijelova lica (npr. očiju ili usta),
- Procjena specifičnih znakova koji pokazuju opću razinu pozornosti.

Nastanak male baze podataka bio je nužan uvjet za potvrđivanje predloženog pristupa. Dostupno je više važnih baza podataka za testiranje tehnika prepoznavanja izraza lica i pozicija glave te video isječaka koji prikazuju vozača tijekom vožnje snimljenih pomoću kamera u automobilu.

Postavke eksperimenta smišljene su imajući na umu potrebu sakupljanja slika tijekom efektivne vožnje. U tu svrhu, USB kamera je postavljena na vjetrobran auta na poziciju prikladnu za ugodnu vožnju. Kamera omogućuje snimanje nekoliko minuta videa tijekom uobičajenih situacija u vožnji.

Za svakog vozača skupljeni su podaci iz dvije sesije prikupljanja podataka, u različitom trenutku dana i s različitim osvjetljenjem. Korisnici su vozili i s naočalama i bez njih, bez zamaranja pozicijom sjedala i kamerom.

Svaka sesija sastoji se od trominutne video snimke, ručno podijeljene kako slijedi:

- Oko jedne minute normalnog ponašanja u vožnji: vozač prati cestu ispred sebe i u retrovizorima,
- Oko jedne minute simuliranih znakova umora: vozač zatvara oči i simulira klimanje glavom,
- Oko jedne minute dekoncentriranog ponašanja: vozač gleda prema gore, dolje ili sa strane u osam fiksiranih oznaka oko auta.

Trenutačno, baza podataka sastoji se od 15 registriranih korisnika koji voze isti auto tijekom ukupno 30 sesija i oko 90 minuta video zapisa. Baza podataka uključuje vozače različitog spola, one koji nose naočale, koji imaju brade i dr. Uključeni su i česti izrazi lica kao posljedica smijanja i pričanja.

Slika 21- Uzorci slika dobiveni iz različitih sesija [9]

Neke dobivene slike iz različitih sesija pokazani su na slici iznad. Moramo uzeti u obzir da je kvaliteta slika generalno niska, te da svjetlosni i zvučni efekti zadaju vrlo težak zadatak za klasifikaciju.

Poznato je u zajednici prepoznavanja obrazaca da je ključan korak u eksperimentalnoj fazi vezan uz identifikaciju tri različita skupa podataka. Dobra nasumična distribucija uzoraka u tim skupovima podataka osigurava točno mjerenje performansi sustava, nadoknađujući moguće greške.

Korištene su samoorganizirajuće mape SOM (engl. *Self Organizing Map*) za nasumično uzorkovanje tijekom prve sesije. SOM grupira sve uzorke u homogene skupine od kojih se potom uzima manji dio slika i sastavljaju skupovi za obuku i provjeru. Sve slike iz druge sesije tvore testni ili slijepi skup koji se potom koristi samo za mjerenje performansa sustava.

U skladištima gdje se zahtjeva visok stupanj sigurnosti i tajnosti također nalazimo elemente biometrije. Ulazi u same zgrade uprave ili laboratorije koriste neku vrstu identifikacije osobe koja ulazi u tu prostoriju. Dopuštenje u te prostore imaju osobe koje su se dokazale u tom poslu te se na njih može osloniti.

Za veću sigurnost samog objekte postoje i kombinirano korištenje biometrijskih metoda, npr. otisak prsta i zahtjev za pinom. Najčešće se koristi neka vrsta identifikacije iskaznicom koja sadrži osobne podatke o osobi te razinu propusta, tj dopuštenja ulaska. Ulazak se može odrediti da vrijedi samo za neke prostorije tj. odjele nasumično, a nakon toga su vrata koja su pod lozinkom te se ne mogu proći ukoliko se ne utipka odgovarajuća lozinka.

Primjena biometrije je postala svakodnevna potreba koja se više ne gleda kao neka vrste zabrane, nego se uistinu gleda kao jedan od načina sigurnosti i čuvanja integriteta same ustanove.

5. ZAKLJUČAK

Jedan od temeljnih problema suvremenog svijeta je svakako promet i njegov porast iz dana u dan. Samim time nastaje i potražnja za razvojem sve većih površina za prometnice, a sukladno tome i nove tehnologije koje bi mogle kontrolirati i voditi toliku masu.

Zato se ITS pokazao kao idealno rješenje za kontrolu prometa. Time se ne nastoji otkazati svrha klasičnim načinima kontrole, odnosno policijskoj službi, već se nastoji njima pomoći. Brzina i ažurnosti prenošenja podataka Inteligentnim transportnim sustavima jednostavno je nužna stvar u svakom većem i razvijenijem prometnom središtu.

ITS iskazuje novi pristup i primjenu naprednih upravljačkih i tehnoloških rješenja, kojima se nastoji postići veća sigurnost, učinkovitost i pouzdanost prijevoza, a istodobno smanjenje utjecaja na okoliš i društvo.

Učinkovitost primjene ovoga sustava očituje se najviše u brzini reagiranja kod incidentnih situacija. Naime, u zemljama koje već dugi niz godina primjenjuju ovaj sustav, pokazalo se da se smanjio broj prometnih nezgoda i stradalih na prometnicama. ITS detaljno prenosi lokacijske oznake područja gdje se desila nezgoda te kako da najbliža jedinica za pomoć stigne do iste lokacije. Naročito je to učinkovito na autocestama i cestama s velikom količinom dnevnog prometa, prometnicama koje se teško dostupne i slično.

U radu je prikazan prijedlog uvođenja novih metoda, baziranih na binarnoj klasifikaciji i postizanju visoke razine preciznosti i performansi u stvarnom vremenu, posebno prilagođenih automobilskoj aplikaciji. U radu se objašnjava kako usvajanje kompleksnih znakova te specifičnih izraza lica može biti efikasno zamijenjeno uvođenjem generaliziranog modela nepažljive vožnje. Na ovom području može se uočiti nekoliko velikih poboljšanja a to su upotpunjavanje baze podataka za mogućnost višestrukih sesija i višestrukih korisnika te postojanje pravih sekvenci koje omogućuju temeljitu provjeru pristupa. Ta metoda omogućuje jednostavnu generalizaciju dodatnih stanja nepažnje kao što su zijevanje ili umorne geste koje se lako mogu uvesti dodavanjem ograničenog broja novih testnih uzoraka u rječnik.

Mnoge zemlje i dalje vrše istraživanja na ovom sustavu kako bi se mogao što više i skorije unaprijediti i poboljšati, te biti pristupačan za uvođenje na sve prometnice gdje je količina prometa velika i zahtjeva povećanu pažnju. To naravno, kako je već rečeno ne bi umanjilo i aktivnosti službi koje vrše redovite kontrole prometnica, ali bi svakako i njima pomoglo u otkrivanju lokacija nezgode i mogućnosti odlaska na teren kako bi se unesrećenima pomoglo.

Svrha je omogućiti ljudima siguran i brz protok prometnicama, sigurnije stizanje na odredište, te maksimalno izbjegavanje čekanja i stvaranja gužvi i kolapsa u prometu.

Literatura

[1] www.propisi.hr/files/file/142_903%20NACIONALNI%20PROGRAM%20ZA%20RAZVOJ%20I%20UVODENJE%20INTELIGENTNIH%20TRANSPORTNIH%20SUSTAVA___.doc its arhitektura (lipanj, 2015.)

[2] https://bib.irb.hr/datoteka/541816.Inteligentni_sustavi_upravljanja_prometom.doc3 (lipanj, 2015.)

[3] https://www.scribd.com/doc/120202152/Poboljˇsanje-sigurnosti-u-prometu-primjenom-ITS-rjeˇsenja (lipanj, 2015.)

[4] http://www.acuity-mi.com/Principals.php (lipanj, 2015.)

[5] http://os2.zemris.fer.hr/protokoli/2007_nimac/Seminar%5B2007%5DNimac_Luka.html#2.Biometrijski%20sustavi|outline (lipanj, 2015.)

[6] Prof.dr.sc. Miroslav Bača, Materijali sa e-studenta: Biometrija (lipanj, 2015.)

[7] A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security,, IEEE Trans. Inf. Forensicsd Secur. 1 (srpanj, 2015.)

[8] http://os2.zemris.fer.hr/protokoli/2007_nimac/Seminar%5B2007%5DNimac_Luka.html#2.Biometrijski%20sustavi|outline (lipanj, 2015.)

[9] www.elsevier.com/locate/trc (srpanj, 2015.)

[10] STALLINGS, W. *Data and Computer Networks*. London: John Wiley, 2006.

[11] STALLINGS, W. *Local Computer Networks*. London: John Wiley, 2006a.

[12] ATM FORUM, User-Network Interface (UNI) Specification, http://www.atmforum.com, travanj. 2010.

[13] BRADY, P.T. A statistical Analysis of On-off Patterns in 16 Conversation, *Bell System Technical Journal*, 47,1 (1998), 55-62.

[14] BRADY, N. A statistical Analysis of Use Case. *Proceedings of the 7th International Conference on Telecommunications ConTEL*, Zagreb, (2003), 45-52.

[15] LILYS, M. Final data structures. *Doktorski rad*. Sveučilište u Zagrebu, 2010.

[16] http://www.span.hr/hr/rjesenja/infrastruktura/informacijska-sigurnost/ (rujan, 2015)

[17] http://www.veleri.hr/files/datoteke/nastavni_materijali/k_sigurnost_s2/sigurnost_informacijskih_sustava.pdf (kolovoz,2015)

[18] http://hacking-class.blogspot.de/2011/02/denial-of-service-dos-attacks.html (kolovoz, 2015.)

[19] http://os2.zemris.fer.hr/ISMS/2008_kovacevic/dodatakB.html (kolovoz, 2015)

[20] http://os2.zemris.fer.hr/ISMS/2008_kovacevic/sigurnostIS.html (rujan, 2015)

[21] http://www.politikaplus.com/img/s/648x380/upload/images/T-U-V/vozac_san.jpg (lipanj, 2015)

[22] http://metro-portal.hr/img/repository/2010/08/medium/auto_brzina_ss.jpg (srpanj, 2015)

[23] http://mojzagreb.info/images/uploads/vijesti/13172/zet_bus.jpg (lipanj, 2015)

[24] http://cdn.trendhunterstatic.com/thumbs/fingerprint-lock.jpeg (srpanj, 2015)

[25] http://www.tip.ba/wp-content/uploads/2012/04/dnk.jpg (kolovoz, 2015)

[26] Liang, Y., Lee, J.D., 2014. A hybrid Bayesian Network approach to detect driver cognitive distraction. Transport. Res. Part C: Emerg. Technol. 38, 146–155

[27] http://www.zet.hr/default.aspx?id=1352 (rujan, 2015)

Popis tablica

Popis slika