UDC: 004:007.5 Info M str. 16-22

# UTICAJ AMBIJENTALNIH PROMENA NA KVALITET BIOMETRIJSKIH PODATAKA
# THE INFLUENCE OF AMBIENT CHANGES ON THE QUALITY OF BIOMETRIC DATA

Marija Bogićević Sretenović, Fakultet Organizacionih Nauka, marija.bogicevic@fon.bg.ac.rs
Dejan Simić, Fakultet Organizacionih Nauka, dejan.simic@fon.bg.ac.rs
Bojan Jovanović, Fakultet Organizacionih Nauka, bojan.jovanovic@fon.bg.ac.rs

REZIME: Biometrija je oblast od izuzetnog značaja kod bezbednosti informacionih sistema. Biometrijska identifikacija korisnika postaje neophodan uslov za logovanje korisnika u razne aplikacije i sisteme. Savremeno društvo dovelo je do toga da je autentifikacija odnosno verifikacija identiteta individue, postala svakodnevna potreba. Sa porastom korisničkih naloga na raznim sistemima i aplikacijama, porastao je i broj lozinki koje je potrebno zapamtiti. Taj problem biometrija pokušava da reši na globalnom nivou. Jedan od problema koji utiče na uspešnost biometrijskog sistema je loš kvalitet slike biometrijskog uzorka koji zavisi od akvizicije kao početne faze u procesu autentifikacije. S obzirom da kvalitet slike zavisi od kontrolisanih uslova okruženja samim tim to će uticati na performanse biometrijskog sistema. U ovom radu su predstavljeni mogući problemi akvizicije podataka biometrijskih modaliteta koji se najviše koriste.

KLJUČNE REČI: Biometrijski sistemi, Biometrijski modaliteti, Akvizicija podataka, Kvalitet slike

ABSTRACT: Biometry is area of special interest of information systems.Biometric authentication of users becomes essential requirement for logging into a service, an app and so on. In a modern society authentication of users i.e. verification of identity becomes everyday need. With increase of users accounts of different systems and apps, the number of passwords that one user needs to remember increases as well. This issue biometry is trying to resolve on global level. Bad photo quality of biometric sample is one of the issues that could jeopardize success of biometric systems. Quality of biometric sample depends of acquisition which is the first phase of authentication proccess. Since the image quality depends on controlled environment condition it will also have effect on biometric system performance.This paper presents possible problems od data acquisition issues of biometric modals that are mostly used.

KEY WORDS: Biometric system, Biometric modalities, Data acquisition, Image quality

## 1. UVOD

Turbulentno i savremeno društvo dovelo je do velikih promena u ljudskoj svakodnevnici. Digitalna transformacija podrazumeva izmeštanje velikog dela ljudskih aktivnosti u digitalnu sferu gde se kao poseban problem javlja uspostavljanje validnog digitalnog identiteta. Razvoj Interneta, pre svega društvenih mreža doveo je do toga da pojedinci moraju pamtiti veliki broj korisničkih naloga i lozinki. Poslednjih nekoliko godina svedoci smo značajnog razvoja informacionih tehnologija u oblasti autentifikacije i autorizacije. Sam pojam identiteta se može posmatrati i tumačiti sa raznih aspekata. Sa filozofskog aspekta pojam identiteta se poistovećuje sa jedinstvenom slikom pojedinca i određuju ga raznolikosti između osoba. Identitet nas čini jedinstvenim u odnosu na druge ljude. Sa informacionog aspekta identitet označava skup podataka koji se pridružuje određenom pojedincu u nekom sistemu za upravljanje identitetom [1]. Na osnovu utvrđenog identiteta pojedincu se odobrava pristup određenim resursima.

Tehnike menadžmenta identiteta danas su prisutne u velikom broju različitih aplikacija i od kritičnog značaja su za njihovo efektivno funkcionisanje. Menadžment identiteta rešava probleme jedinstvene prijave korisnika (*single sign-on*), upravljanja korisničkim nalozima (*user provisioning*), kao i problem kontrole pristupa (*access control*). Upravo u menadžmentu identiteta biometrija pronalazi svoju veliku primenu. Pravilno implementirana kontrola pristupa je od ključne važnosti za bilo koji sistem gde je neophodno utvrđivanje identiteta osobe. Biometrija već sada zauzima značajan deo tržišta, a prognoze su da će do kraja 2022. godine biometrijski trgovci imati 32,73 biliona dolara [1]. Istraživanje su pokazala da najveći broj, čak oko 45% populacije koja koristi korisničke naloge, po pet godina ne menja svoje lozinke što povećava stopu zloupotrebe. Čak preko 70% korisnika iste lozinke koristi za više sistema odnosno aplikacija. Upravo je uvođenje biometrije rešenje za ovakve slučajeve, jer metodom autentifikacije gde korisnik nešto jeste, odnosno upotrebom neke njegove fizičke karakteristike se potvrđuje identitet da bi mogao da pristupi željenim resursima.

Biometrija ima veliku primenu u raznim sferama ljudske svakodnevnice. Jedna od njih je elektronska trgovina, koja se u današnjem društvu više ne posmatra kao fenomen [2]. Priliv novih tehnologija doveo je do većeg broja korisnika. Danas,većina ljudi koristi elektronsku trgovinu delom zbog ekonomskih razloga, a delom i zbog ugodnosti, jer nema potrebe ići negde van. To je nešto što postoji više od dvadeset godina, jer je veliki razvoj kompjuterskih tehnologija uticao na to. Međutim, zloupotreba kartica je ozbiljan problem i najviše problema je upravo u utvrđivanju autentičnosti identiteta korisnika. Neophodno je pronaći rešenje za problem koji postoji u svim elektronskim platnim sistemima. Jedan od pravaca potencijalnog rešenja utvrđivanja identiteta podrazumeva primenu biometrijskih tehnologija. Biometrijski sistemi nalaze primenu kod raznih sistema plaćanja [3].

Biometrijske tehnologije nalaze najveću primenu kod utvrđivanja identiteta ličnosti u aplikacijama za kontrolu pristupa. Pri samoj akviziciji biometrijskih uzoraka od velike je važnosti način na koji se koristi senzor, odnosno sama interakcija

korisnika i senzora mora biti intuitivna. Vrlo često se dešava da je korisnik bez iskustva i da ne ostavi kvalitetan uzorak. Uspešan razvoj biometrijskog sistema zahteva i razmatranje interakcije ispitanika i uređaja. Na akviziciju utiču uslovi okruženja (osvetljenje, temperatura), demografski uticaji (godine starosti, pol, medicinska ili fizička oštećenja), karakteristike uređaja (npr. povratna informacija od digitalizatora kod verifikacije dinamičkog potpisa), a moguć je i uticaj oblika ili dizajna samog uređaja. Modaliteti kod kojih postoji kontakt sa senzorom (kao kod otiska prsta) ili poravnjanje sa senzorom (kao kod identifikacije irisom) pri akviziciji u velikoj meri zavise od interakcije čoveka i računara. U zavisnosti od uslova pod kojim se izvodi akvizicija, kvalitet slike ima varijacije u nivou kvaliteta. Kvalitet slike kod otiska prsta može da se meri nekim od sledećih parametara: snaga grebena, kontinuitet grebena, jasnost grebena i integritet strukture doline grebena ili performanse verifikacije. Performanse verifikacije se mere određenim parametrima.

## 2. POJAM BIOMETRIJE

Biometrijska informacija BI se može definisati kao smanjenje neizvesnosti u utvrđivanju identiteta pojedinca. Učesnicima bilo kog sistema, a posebno biometrijskog neophodno je sigurno okruženje u kome će se odvijati proces autentifikacije. Da bi zaštitili bilo koji informacioni sistem neophodno je da bude ispunjen trio CIA (*confidentiality, integrity, authenticity*).

A. K. Jain [4] je identifikovao sedam poželjnih kriterijuma koji određuju pogodnost korišćenja neke biometrijske karakteristike u biometrijskom sistemu. To su sledeći kriterijumi univerzalnost, jedinstvenost, stalnost, merljivost, performanse, prihvatljivost i mogućnost prevare.

- **Univerzalnost** - svaki korisnik koji želi da pristupi biometrijskom sistemu mora da poseduje biometrijsku karakteristiku koju taj sistem koristi, odnosno da je dostupna kod ljudi.
- **Jedinstvenost** - biometrijska karakteristika mora posedovati osobinu da se ne ponavlja u populaciji, tačnije da nije moguće pronaći par osoba koji ima identične biometrijske karakteristike.
- **Stalnost** - biometrijska karakteristika mora biti otporna i invarijantna na vreme koje prolazi. Ekstrahovane karakteristike moraju biti invarijantne, jer od izuzetne važnosti da algoritam koji se koristi ne bude osetljiv na promene koje mogu nastati vremenom, a uzrok tome je najčešće starenje osoba.
- **Merljivost** - svaka karakteristika mora biti merljiva. Uslovi akvizicije i senzori su neophodni da se izvrši akvizicija biometrijskog uzorka i da se on digitalizuje u odgovarajući format koji će koristiti algoritam za poređenje. Akvizicioni postupak mora biti takav da ne uzrokuje stres osobe koja je u postupku akvizicije. Metode akvizicije moraju poštovati ljudska prava i cilj je da budu neinvanzivne.
- **Performanse** - preciznost prepoznavanja i resursi koji su neophodni za njeno postizanje moraju biti u skladu sa mogućnostima aplikacije.
- **Prihvatljivost** - osobe koje će koristiti biometrijski sistem moraju biti spremne da svojevoljno pristupe postupku akvizicije kao i radu sa aplikacijom.
- **Mogućnost prevare** - odnosi se na lakoću kojim se određena biometrijska karakteristika može imitirati ili lažno duplicirati. Kod fizičkih karakteristika to može biti mimikrija ili imitacija kod bihejvioristiških.

Biometrija ima veliku primenu u svakodnevnom životu, a slede neke od oblasti gde je zastupljena:

- Najviše se koristi kod zaštite mobilnih uređaja, gde je Apple prvi uveo skeniranje otiska prsta kod iphone 5s.
- Kod zaštite graničnih prelaza, jer ljudi danas putuju više nego ikada.
- Kod izdavanja nacionalnih dokumenata, poput lične karte, zdravstvene knjižice, vozačke dozvole.
- U bankarskom poslovanju, pre svega kod biometrijskih sistema plaćanja
- Kod menadžmenta identiteta
- Za biometrijsku registraciju SIM kartica
- U bolnicama, da bi se pre svega sprečila zamena dokumenata o pacijentima
- Na aerodromima za kontrolu ulaska i izlaska iz zemlje
- Kod agencija za sprovođenja zakona u Americi, Japanu, Rusiji, Kini, Velikoj Britaniji, biometrijska identifikacija osoba zauzima značajno mesto
- Kod automobila cilj je da biometrija zameni ključ kojim se otključava ili pali auto
- Kod zaštite računara u smislu identifikacije korisnika otiskom prsta kao kod Macbook ili Dell, ili kod kompanije Lenovo koja je primenila FIDO standard takođe kod otiska prsta
- U crkvi, školi, teretani, tržnim centrima za povećanje bezbednosti tih sistema
- Kod povećanja bezbednosti zatvora u smislu praćenja dnevnih aktivnosti zatvorenika
- Kod doniranja krvi i formiranja banki krvi
- Kod sprovođenja izbora
- Kod registracije izbeglica
- Kod nekih sportskih aktivnosti, hotela [5].

Biometrijske karakteristike odnosno modaliteti se mogu podeliti u dve osnovne grupe i to fizičke i bihejvioristiške. Fizičke karakteristike su one biometrijske karakteristike koje su ugrađene u svakog pojedinca tj. određene su telesnim sklopom svakog pojedinca. U fizičke karakteristike spadaju:

- Otisak prsta - najčešće korišćena biometrijska karakteristika koja predstavlja obrazac grebena i udubljenja kože na jagodici prsta.
- Dužica oka (*eng. Iris*) - to je prstenasta regija oka ograničena zenicom i beonjačom sa svake strane
- Geometrija šake - sistemi su zasnovani na merenjima uzetim sa ljudske šake, uključujući njen oblik, veličinu dlana, kao i dužinu i širinu prstiju.
- Dlan - dlanovi na ljudskim rukama sadrže različite oblike udubljenja i ispupčenja, slično kao kod otiska prsta

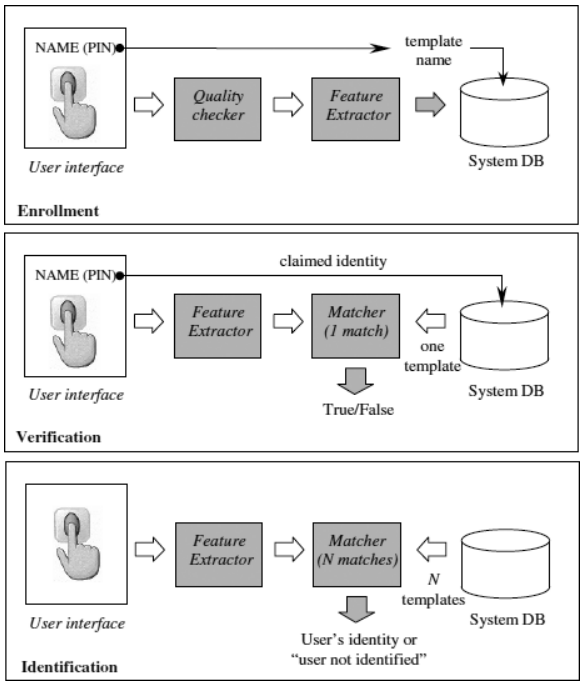
- Mrežnjača (*eng. Retina*) - struktura retine je veoma bogata i predstavlja jedinstvenu karakteristiku svake osobe
- Lice - neinvazivna metoda koja se koristi za identifikaciju u svakodnevnom životu
- Termogram lica - slika generisana usled toplote koju zrači ljudsko telo može se dobiti pomoću infracrvene kamere na neinvazivan način, slično regularnoj fotografiji
- Uho - uočljive su razlike kod ljudi prema obliku uha i strukturi ušne školjke
- Miris - svaki objekat odaje miris koji je karakteristican po svom hemijskom sastavu i koji može da se iskoristi za pravljenje razlike među različitim objektima
- DNK - to je jednodimenzioni, jedinstveni kod neke osobe, izuzev što identični blizanci imaju identične DNA oblike

Bihejviorističke karakteristike su biometrijske karakteristike koje su definisane specifičnostima ponašanja individue prema spoljnjem svetu i one se tokom životnog veka čoveka menjaju pod uticajem vremena i okruženja kroz koje pojedinac prolazi. U bihejvioralne karakteristike svrstavaju se:

- Potpis - način na koji osoba potpisuje svoje ime predstavlja karakteristiku te osobe
- Glas - glas je kombinacija fiziološke i bihejviorističke biometrije, osobine nečijeg glasa zavise od oblika i veličine vokalnog trakta, usta, nazalnih šupljina i usana, koji se koriste u sintezi govora.
- Hod - specifičan način na koji se kreće neka osoba i predstavlja kompleksnu prostorno vremensku biometriju
- Otkucaji na tastaturi - svaka osoba kuca na tastaturi na karakterističan način
- Način interakcije sa korisničkim interfejsom

### 3. BIOMETRIJSKI SISTEMI

Biometrijski sistem može da funkciniše u dva moda, registracija (*enrollment*) i autentifikacija (*authentication*) ili prepoznavanje (*recognition*) u okviru koje se razlikuju dva procesa identifikacija i verifikacija. Postoje aplikacije kod kojih se radi samo identifikacija, zatim aplikacije kod kojih se radi samo verifikacija, kao i aplikacije kod kojih se radi i identifikacija i verifikacija. Dakle kod autentifikacije biometrijski sistem funkcioniše kao patern prepoznavanja, gde se izdvajaju četiri ključna modula senzorski modul, modul za ekstrakciju, baza podataka i modul uklapanja. Senzorski modul služi za akviziciju biometrijskih uzoraka od korisnika. U modulu za ekstrakciju se vrši ekstrahovanje odnosno izdvajanje ključnih karakteristika iz biometrijskog uzorka. Svi biometrijski uzorci zajedno sa ključnim podacima o svakom korisniku poput imena, prezimena, JMBG, smeštaju se u bazu podataka. Modul za uklapanje koristi se za upoređivanje uzorka u bazi sa onim koji je uzet u procesu akvizicije. U skladu sa ovim modulima razlikuju se i procesi u biometrijskim sistemima. Na Slici 1. su prikazani procesi registracije, verifikacije i identifikacije.




**Slika 1.** *Proces registracije, verifikacije i identifikacije[6]*

Biometrijski sistemi su u velikoj meri zavisni od vrste senzora, segmentacije i izvlačenja ključnih karakteristika da bi se na valjan način upravljalo podacima koji su prikupljeni iz ekstrahovanih uzoraka i da bi se došlo do ispravnog odgovora. Posmatrajući kako ispitanici koriste senzore, nekoliko dizajnerskih nedoumica može biti rešeno ukoliko se integrišu znanja i iskustva industrijskog i interaktivnog dizajna, ergonomičnosti i korisnosti [7].

### 4. AKVIZICIJA I UTICAJ NA OSETLJIVOST PERFORMANSI BIOMETRIJSKIH SISTEMA

Akvizicija biometrijskih uzoraka je prva faza u procesu identifikacije individue kod biometrijskih sistema, tako da je jako bitno da proces počne na pravilan i adekvatan način koji će obezbediti dobre performanse sistema. Svaki biometrijski modalitet ima neke karakteristike zbog kojih se akvizicija i uslovi u kojima se izvodi moraju prilagoditi njemu. Sa druge strane stoji pojedinac koji može da ima trajna oštećenja prsta, izrazito suvu ili vlažnu kožu, sklonost ka promuklošću, čestu promenu načina potpisivanja, starenje kao jedan od faktora što sve može da utiče na kvalitet biometrijskih uzoraka. Na akviziciju biometrijskih uzoraka utiču i uslovi okruženja, interakcija čoveka i računara. Od izuzetne važnosti je da istraživanja budu rasprostranjena na polje izučavanja i kako se biometrijski uzorci ponašaju tokom vremena, kako se krajnji rezultati odražavaju na performanse sistema.

Ključni modul u ovoj fazi je senzorski modul koji prikuplja sirove biometrijske podatke korisnika. U zavisnosti od biometrijskog modaliteta razlikuju se forme prikupljenih podataka, pa tako mogu biti dvodimenzionalne slike kao što je kod otiska prsta, lica, irisa i drugih. Izuzetak je akvizicija glasa kod koga

su podaci predstavljeni jednodimenzionalnom amplitudom. Takođe i potpis koji se uzima u online režimu gde se prati pritisak olovke, pozicija i brzina, ili kod prepoznavanja na osnovu mirisa ili DNA koji su hemijski bazirani. Za sve uzorke koji su zasnovani na slici od izuzetnog značaja je rezolucija, broj slika kao i osetljivost kamere. Prate se demografski podaci poput pola, godina starosti i nekih kulturnih pitanja i vrednosti ključnih za dizajn senzorskog modula. Dizajn senzorskog modula zavisi i od cene, veličine i izdržljivosti.

### 4.1 *Performanse*

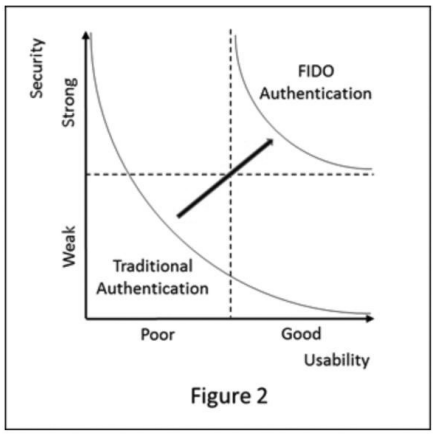
Evaluacija performansi za biometrijske tehnologije zahteva uopštenost, ekspertizu, pravičnost i pouzdanost. Pod uopštenošću se podrazumeva da metode moraju biti primenljive za sve tehnologije raznih biometrijskih modaliteta. Za ekspertizu je od izuzetne važnosti da metode budu kreirane i dizajnirane od strane kompetentnih stručnjaka. Što se tiče pravičnosti bitno je da su sve metode i evaluacioni indeksi postavljeni korektno. Rezultati evaluacije neophodno je da budu pouzdani.

### 4.2 *Metrike*

Prilikom evaluacije biometrijskog sistema, potrebno je na kvantitativan način izmeriti njegove karakteristike. Metrike koje se koriste u ovu svrhu zapravo se odnose na željene karakteristike biometrijskog modaliteta. Veza između metrika i željenih karakteristika biometrijskog modalita može biti direktna ili indirektna. Preciznost biometrijskog sistema može se meriti na sličan način kao prilikom evaluacije hipoteza u statistici - moguće su dve greške, FMR(False Match Rate) ili FAR (False Acceptance Rate) i False Non-Match Rate(FNMR) ili FRR (False Rejection Rate). FNMR i FMR se nalaze u međusobnoj zavisnosti, a obe mere su zapravo funkcije praga osetljivosti sistema (*threshold*) odnosno praga odlučivanja, kog inače određuje sam korisnik sistema. Odnosi ove dve mere se u najvećem broju slučaja prikazuju na ROC(Reciever Operating Characteristics) krivama koje prikazuju performanse biometrijskog sistema. Mogu se prikazati i DET (Detection Error Tradeoff) krivama koje prikazuju normalno odstupanje i interpolaciju između tačaka kod FRR i FMR. Prilikom akvizicije podataka, odnosno registrovanja korisnika biometrijskog sistema, može doći do problema kod nekih od korisnika. Mere koje se odnose na ovaj problem jesu FTA(Failure to Acquire), FTE(Failure to Enroll) i TTE(Time to Enroll). Takođe u upotrebi su GAR(Genuine Acceptance Rate), EER(Equal Error Rate) i HTER(Half Total Error Rate). Genuine acceptance rate se dobija kao razlika 100 - FNMR.

### 4.3 *FIDO standard*

FIDO – *Fast Identity Online* alijansa je formirana 2013. godine sa ciljem da reši problem jake autentifikacije za pristup online servisima. Ideja je bila da se formiraju otvoreni standardi za jaku i sigurnu autentikaciju koja se relativno lako koristi. To je specifikacija koja se konstantno razvija i prati savremene informacione tehnologije, pri čemu je osnovna ideja da se autentifikacija obavlja korišćenjem biometrijskih modaliteta umesto korišćenja lozinke [8]. Jedan od osnovnih FIDO principa je da se zadovolji zahtev korisnika za jednostavnošću a obezbeđujući jaku bezbednost i privatnost podataka. Korisnici ne moraju da pamte lozinke. Jedan od načina realizacije jednostavnosti je da se korisnik jednom autentifikuje prilikom inicijalne registracije sa mogućnosću korišćenja više servisa kasnije. Ovaj standard najveću primenu pronalazi u bankarskim aplikacijama na mobilnim uređajima. Neka od istraživanja koja su obavljena iz 2014. godine ukazuju na to da je prosečna cena koštanja nekog sistema za autentifikaciju velike kompanije iznosila oko 189000$. Pri čemu kompanije gube oko 420$ po zaposlenom u borbi sa lozinkama, gde FIDO značajno smanjuje troškove. Na sledećoj slici je grafik koji pokazuje razliku tradicionalne autentifikacije lozinkama i Fido autentifikacije. Neke od kompanija koje su usvojile FIDO autentifikaciju za neke svoje servise i uređaje su i Google, Samsung, Alibaba, Paypal, Bank of America i mnoge druge.




**Slika 7.** *Autentifikacija lozinkom i FIDO autentifikacija [9]*

### 4.4 *Problemi akvizicije podataka kod biometrijskih modaliteta*

U narednom delu teksta sledi opis problema akvizicije sa kojim se sreću razni biometrijski sistemi koji koriste razne modalitete koji se u praksi najviše koriste, a to su lice, šaka, potpis, iris i otisak prsta.

#### 4.4.1 *LICE*

Prepoznavanje osoba na osnovu karakteristika lica i irisa su najzastupljenije beskontaktne metode akvizicije [10]. Lice kao biometrijski modalitet je najviše izučavan u idealnim uslovima, gde su svetlo, rezolucija i ugao gledanja kontrolisani. Johnson [10] je izveo eksperiment gde je testirao 25 osoba, kojima je uzeo biometrijski uzorak sa razdaljine 5 i 25 koraka u raznim uslovima okruženja. Pratio je osvetljenje, zamućenje, ugao gledanja, okluziju odnosno apsorbovanje, rezoluciju slike, pokrete u skladu sa kontrolisanim uslovima akvizicije. Kada su imali osobu koja nosi naočare za vid, tada su uzimali dve slike, sa i bez naočara. Analiza je urađena koristeći softverski alat MATLAB. Neki od zaključaka do kojih su doš-

li je da su vrednosti kontrasta za slabo osvetljenje više nego kod drugih stanja. Zaključili su da srednje osvetljenje kada je akvizicija sprovedena na 5 koraka razdaljine dovodi do većih vrednosti kontrasta od očekivanih [10].

Prepoznavanje na osnovu lica kod biometrijskih sistema puno zavisi od osvetljenja, kao i mesta gde je postavljena kamera kojom se obavlja akvizicija [11]. Jedan od ekperimenata koji je obavljen iz ove oblasti je i da je testirano deset proizvođača senzora gde su se svi složili da spoljašnje svetlo puno utiče na kvalitet slike koja se obrađuje u biometrijskom sistemu. Poredili su uzorke koji su prikupljeni istog dana u spoljašnjim uslovima pod lošim svetlom sa onim u zatvorenom prostoru. Zaključak je da su performanse sistema drastično lošije kod akvizicije u spoljašnjim uslovima, sa 95% smanjile su se na 54%. U stvarnom životu mala je verovatnoća da u istom danu se identifikuje osoba u zatvorenom i otvorenom prostoru, ali svakako je ostavljeno puno prostora za dalja istraživanja i ispitivanja u raznovrsnim scenarijima okruženja.

#### 4.4.2 *ŠAKA*

Geometrija šake se koristi kao biometrijski modalitet za prepoznavanje osoba od 1980. godine u aplikacijama za kontrolu pristupa, evidenciju prisustva i mnogim drugim. Postoji više faktora koji utiču na kvalitet slike uzetog uzorka u ovom slučaju. Jedan od pokazatelja koji se posmatra je univerzalnost šake-gde šaka pojedinca može biti značajno različita od svih ostalih očekivanih prosečnih šaka. Kao npr. pojedincu može nedostajati prst što nije u skladu sa očekivanim rezultatom i to dovodi do problema akvizicije poznatog kao FTA-*Failure to Acquire* odnosno neuspeh za akviziciju. Biometrijski sistem za prepoznavanje na osnovu šake akviziciju obavlja tako što ispitanik spušta ruku na ploču gde vrhovi prstiju moraju da dotaknu određene pinove [12]. Ukoliko do toga ne dodje ili ispitanik nema neki prst, tada se mora preći na drugi scenario gde se ruka rotira izazivajući bilo ulnarnu ili radijalnu devijaciju ručnog zgloba.

#### 4.4.3 *POTPIS*

Verifikacija dinamičkim potpisom se dugo koristila za autentifikaciju pojedinaca na osnovu njihovih karakteristika potpisa. Aplikacije za autentičnost dokumenata, finansijske transakcije, sve transakcije bazirane na papiru moraju imati potpis kao garant da je određeni dokument poslat odnosno da je transakcija obavljena. Potpis je inicijalno posmatrano bihejvioristička karakteristika i zbog toga ne zavisi od nekih parametara kao neki drugi modaliteti, već isključivo od samog potpisnika. Potpis je naučena tehnika, sadrži mere koje mogu biti zamenjene u zavisnosti od senzora, može biti promenjen od strane vlasnika, može da ima nekoliko verzija, sve zavisi od transakcija ili namere samog vlasnika potpisa [13]. Sve su ovo izazovi sa kojima se susreću projektanti biometrijskog sistema zasnovanog na identifikaciji na osnovu potpisa. Tekuća dinamička verifikacija potpisom se koristi na isti način i u iste svrhe i umesto stvarnog potpisa. Potpis ima ograničen broj ekstrahovanih karakteristika, uključujući kooordinate x,y, zatim vreme, zavisi i od digitalizacije, pritiska. Te ulazne varijable se koriste za globalne i lokalne karakteristike opisanih u [14]. Drugačiji način karakterisanja potpisa je kroz analizu udarca same olovke pri potpisu. Sve ove dinamičke osobine sakupljene tokom samog čina potpisivanja čine da se oni koji lažiraju tuđi potpis lakše razotkriju.

Na osnovu visegodišnjeg iskustva došlo se do zaključka da postoji potreba da se testiraju biometrijske performanse kada su uzorci uzeti na više različitih senzora. Urađen je eksperiment gde je prikupljeno preko 15000 dinamičkih potpisa sa mobilnih uređaja a zatim su urađene analize da bi se prepoznale promenljive konstantne kod svih uređaja [15]. Cilj je bio da se uporedi dinamika potpisa kod testiranja na tradicionalnim uređajima kao što su digitalne table naspram mobilnih i *wi-fi* uređaja. Uradjena studija je obuhvatila ispitanike koji su bili starosti između 19 i 26 godina a bilo ih je 203. Uglavnom su ispitanici bili studenti, gde je 66% bilo muškaraca volontera, a 35% žena je bilo starije od muškaraca. Ispitanika koji se potpisuju desnom rukom je bilo 91%, a levom 9%. Zaključak istraživanja je da postoji značajna razlika u specifičnim varijablama kod raznih digitalnih uređaja poput Wacom, Palm i Interlink E-pad [15]. Kad su ovi uređaji grupisani zajedno, razlike u varijablama nastavljaju trend razlike značajnosti. Tip uređaja neophodno je da se pridruži na neki način svakom potpisu tako da istraživači mogu da uporede potpise uzete na istom tipu uređaja.

#### 4.4.4 *IRIS*

Prepoznavanje osobe na osnovu irisa je beskontaktna metoda akvizicije, kao i kod modaliteta lica. Ovo je polje istraživanja koje nudi širok spektar eksperimentalnih istraživanja u oblasti akvizicije [16]. Jedan od eksperimenta je izveo [6] sa kolegama gde su pratili rezoluciju, osvetljenje, varijacije na granice van fokusa zamućenja, ugao gledanja, zamućenje pokreta, okluzija oka na rastojanju 5 i 25 koraka. Rezultate su analizirali kroz Matlab i zaključili da razni uslovi okruženja utiču na kvalitet slike, kao što je standardna devijacija kod mera kontrasta koja je uvek visoka [17]. Kontrast slike zavisi od boje očiju ispitanika.

#### 4.4.5 *OTISAK PRSTA*

Prepoznavanje individue na osnovu otiska prsta je najzastupljenija biometrijska tehnologija sa gotovo 60% učešća u odnosu na sve druge modalitete, kao što je već rečeno u radu [18]. Prepoznavanje na osnovu otiska prsta ima veoma dugu istoriju, čak iz vremena Mesopotamije oko 3000 godina pre nove ere [19]. Za biometriju bi bilo idealno kada se uzorak ne bi menjao kroz vreme, odnosno da otisak prsta koji se jednom uzme od ispitanika ne mora opet da se ponavlja, ali to zavisi od fizičkih karakteristika ličnosti što je gotovo nedostižno [20]. Tokom vremena se neke osobine ličnosti menjaju, neko pusti bradu, neko izgubi na težini, promeni se potpis ( npr. promenom prezimena) ili promene koje se dešavaju usled nekih povreda, poput posekotine, ožiljaka na prstu. Posekotine ili ožiljke na prstu odnosno određeni stepen oštećenja može prouzrokovati i profesionalno habanje koje zavisi od zanimanja individue. Svako od ovih stanja ili alteracija može uticati na

kvalitet slike a samim tim na performanse biometrijskog sistema. Postoje reference o uticaju fizičkih promena kao što su ožiljci, bore, kontakt sa senzorom (brzina i pritisak) kao i godine starosti mogu uticati na performanse biometrijskog sistema ili algoritma za prepoznavanje.

Do značajnih podataka došli su i autori [21] u Kini, koji su upoređivali otiske prsta uzete u severnoj i južnoj Kini. U severnoj Kini su ispitanici imali između 21 i 25 godina. Izvedena je akvizicija u periodu od decembra 2013. godine do maja 2017. godine. Mesečno je ispitano oko hiljadu ljudi i uzeta su po dva otiska sa svakog prsta. U južnoj Kini ispitanici su imali takođe između 21 i 25 godina, posmatran je period od januara 2013. godine do maja 2017. godine i ovde je učestvovalo preko 1000 ljudi mesečno. Praćeni su sezonski faktori i njihov uticaj na kvalitet slike otiska prsta, kao i *ESR* i *CPR.* Neki od zaključaka do kojih su došli je da ESR i CPR imaju isti trend varijacije, da je kvalitet otiska prsta u velikoj meri različit zimi i leti, tačnije da su bolji rezultati kod otisaka uzetih u julu i avgustu.

Proces prepoznavanja može rezultirati lošim rezultatima a sve zbog lošeg kvaliteta slike otiska prsta, što je posledica nekih parametara okruženja. Može biti posledica određenog stanja kože prsta što su granični slučajevi, jer je uglavnom koža prstiju u granicama normalnog stanja. Može se desiti da na prstu bude plik, posekotina ili nabor. Što se tiče stanja kože razmatra se kako utiče hrapavost, suvoća ili vlažnost kože prsta. Uvek se razmatra i ponašanje čoveka u procesu akvizicije, da li čovek isuviše jako pritisne čitač ili slabo, a takođe i kakvo je poravnjanje prstiju na senzoru, što je takođe problem interakcije čoveka i računara. U ovu grupu problema spada i brzina kojom ispitanik ostavlja otisak prsta na senzoru [22]. Što se tiče uslova okruženja zaprljana površina senzora utiče na kvalitet slike, kao i ekstremno visoka temperatura ili osvetljenje. Neki od uslova koji su proučavani i testirani u kontrolisanim uslovima su sledeći: hladan prst, ohlađen vlažan prst, zagrejani prst, natopljen prst, prst sa slojem lepka, prljav prst [23].

Postoji značajan broj eksperimenata i zaključaka do kojih se došlo istraživanjem. Jedan od njih je i da je jako ograničeno znanje kod ispitanika koji imaju iznad 62 godine. Kvalitet slike kod ovih ispitanika se odražava na performanse sistema. Sickler i Eliot [24] su došli do zaključka da starija populacija ima slabu definiciju grebena i da niži stepen vlažnosti dovodi do toga da su slike lošijeg kvaliteta nego kod mladih ljudi koji imaju između 18 i 25 godina. Ovo je od velike važnosti za zemlje koje implementiraju prepoznavanje na osnovu otiska prsta za neke od društvenih usluga, poput izdavanja vozačke dozvole.

Kang, Lee, Kim, Shin i Kim [25], sproveli su istraživanje o evaluaciji performansi biometrijskog sistema u zavisnosti od čitača za otisak prsta. Testirali su 4 vrste senzorskih tehnologija i to optičku, poluprovodničku, termalnu i taktilnu. U zavisnosti od vrste senzora pratili su kako se menja kvalitet slike otiska prsta a pod određenim uslovima. Smatrali su da je od velike važnosti da simuliraju uslovi okruženja poput temperature vazduha i vlažnosti, kao i faktori koji se tiču samog korisnika kao što su vlažnost kože i pritisak na senzor.

Modi i Elliot [26] su izveli istraživanje gde su posmatrali dve grupe ispitanika jednu koja je starosti između 18 i 25, gde je učestvovalo 79 individua. Druga grupa su bili korisnici iznad 62 godine gde je bilo 60 ispitanika. U eksperimentu je korišćen optički senzor Digital PersonaU.are.U.2000, gde je uzet otisak sa po 4 prsta svake ruke. Ukupno je bilo 480 uzoraka starije grupe i 632 mlađe populacije. Ekstrakcija karakteristika u velikoj meri zavisi od kvaliteta slike otiska prsta. Srednji broj minucija se računa kod starije i mlađe grupe, tako da je kod mlađe grupe on iznosio 54,8, a kod starije grupe 90,3.

Elliot [11] je sa svojim istraživačima postavio eksperiment gde je pošao od pretpostavke da ne postoji razlika u efektivnosti kvaliteta slike kod dve grupe ispitanika. U jednoj su bili ljudi stariji od 62 godine, a u drugoj, mlađoj populaciji su bili oni između 18 i 25 godina. Ukupno je u istraživanju učestvovalo 54 ispitanika. Otisak prsta je uzet na dve vrste senzora, odnosno čitača optički i kapacitativni. Rezultat eksperimenta je da postoji razlika i da je statistički značajan sa 0,01 tako da je polazna hipoteza odbijena. Sve detalje eksperimenta prikazali su u skladu sa Pirsonovom korelacijom. Druga hipoteza je bila da ne postoji značajna razlika u vlažnosti kože prsta kod obe grupe ispitanika. I ova je odbijena jer je pokazana razlika od takođe 0,01 ali kod optičkog senzora, a kod kapacitativnog samo za desni prst. Ovo studija koju su oni izveli pokazala je da više pažnje treba posvetiti godinama starosti ispitanika nego stepenu vlažnosti u zavisnosti od starosti.

Sledi pregled opisanih problema akvizicije podataka kod biometrijskih modaliteta.

**Tabela 1.** *Lista problema akvizicije podataka kod biometrijskih modaliteta.*

| Redni broj | Biometrijski modalitet | Naziv problema | Opis problema | Broj reference |
|---|---|---|---|---|
| 1. | Lice | Razdaljina | Razdaljina pojedinca od senzora utiče na kvalitet slike | [10] |
| 2. | Lice | Svetlo | Kvalitet slike zavisi od količine svetla. | [11] |
| 3. | Šaka | Univerzalnost šake | FTA se dešava ako pojedincu nedostaje neki prst . | [12] |
| 4. | Potpis | Pritisak olovke | Od pritiska olovke i samog udarca olovke u papir zavisi proces identifikacije. | [14] |
| 5. | Potpis | Dinamika potpisa | Postoji značajna razlika u specifičnim varijablama kod različitih digitalnih uređaja. | [15] |
| 6. | Iris | Ugao gledanja | Ugao gledanja u značajnoj meri utiče na kvalitet slike. | [14] |
| 7. | Iris | Boja očiju | Kontrast slike zavisi od boje očiju ispitanika. | [17] |
| 8. | Prst | Vlažnost prsta | Kvalitet otiska prsta je bolji leti nego zimi zbog vlažnosti prstiju. | [21] |
| 9. | Prst | Brzina akvizicije | Ukoliko isuvise brzo se obavi akvizicija veća je verovatnoća da ne bude uspešna. | [22] |
| 10. | Prst | Zaprljan prst | Kvalitet slike je los ukoliko je prst ili senzor zaprljan. | [23] |
| 11. | Prst | Temperatura vazduha | Kvalitet slike je bolji pri nižoj temperaturi | [25] |

## ZAKLJUČAK

Ovaj rad daje pregled u oblasti problema akvizicije podataka biometrijskih modaliteta, sa posebnim osvrtom na uslove okruženja pod kojima se izvodi akvizicija. Istraženo je da različiti uslovi okruženja pod kojima se izvodi akvizicija utiču na kvalitet slike biometrijskih uzoraka. Neophodno je još istraživanja u oblasti poboljšanja kvaliteta slike. Eksperimentalni rezultati mogu doprineti kreiranju kvalitetnijih rešenja koja se primenjuju u okruženjima koja nisu standardna. Rezultati ovog istraživanja mogu doprineti razvoju nekog novog senzora za sam proces akvizicije, kao i procedure akvizicije. Jedan od daljih pravaca istraživanja je upravo izvođenje eksperimenta akvizicije biometrijskog uzorka u različitim uslovima okruženja na raznim senzorima i praćenje osetljivosti performansi jednog takvog biometrijskog sistema.

## REFERENCE


[1] A.Pando, ‘’Beyond security:Biometrics integration into everyday life’’, Forbes Cominity Council, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#5c14ce1b431f , poslednji put pristupano maj 2019.

[2] D. T. Ahmad, M.HaAriri, User Acceptance of Biometrics in E-banking to improve Security, Business Management Dynamics, vol.2, no.1, pp 01-04, jul 2012.

[3] Jovanović B., Bogićević M., Milenković I., The Architecture of integrated identity management and multimodal biometric systems, XIV International Symposium SymOrg 2014, Zlatibor, Srbija, ISBN 978-86-7680-295-1.

[4] Jain, Anil K., Ruud Bolle, and Sharath Pankanti. Biometrics: personal identification in networked society. kluwer academic publishers, 1999

[5] ‘25 Uses of Biometric in today’s society’’, https://biometrictoday.com/uses-of-biometric-technology-today-society/, poslednji put pristupano novembar 2018

[6] D. Maltoni, D. Maio, A.K Jain, S. Prabhakar, Handbook of Fingerprint Recognition,Springer, 2nd ed 2009.

[7] Kukula E.P., Elliott S.J., Duffy V.G. (2007) The Effects of Human Interaction on Biometric System Performance. In: Duffy V.G. (eds) Digital Human Modeling. ICDHM 2007. Lecture Notes in Computer Science, vol 4561. Springer, Berlin, Heidelberg

[8] K.Hu, Z.Zhang, “Security analysis of an Attractive Online Authentication Standard: FIDO UAF Protocol”, China Communications , Volume: 13 , Issue: 12 , December 2016.

[9] FIDO Alliance, ‘’ FIDO 1.0 Final Specifications Have Arrived’’, whitepaper, 2014

[10] P.A. Johnson, P.Lopez-Meyer, N.Sazonova, F.Hua, S.Schuckers, “ Quality in Face and Iris Research Ensemble (Q-FIRE), “2010 Fourth IEEE International ConfeRence on Biometrics: Theory, Applications and Systems , Washington 2010.

[11] S.J.Elliott, E.P.Kukula, N.C.Sickler, ‘’ The Challenges of the environment and the human/biometric device interaction on biometric system performance’’, 2004 http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=D0B89B37C2F7F389101F0F4DB7D3F64E?doi=10.1.1.133.910&rep=rep1&type=pdf, pristupano oktobar 2018. godine .

[12] Kumar, Ajay, et al. “Personal verification using palmprint and hand geometry biometric.” International Conference on Audio-and Video-Based Biometric Person Authentication. Springer, Berlin, Heidelberg, 2003.

[13] Brault, J.-J., Plamondon, R.: A Complexity Measure of Handwritten Curves: Modeling of Dynamic Signature Forgery, IEEE transactions on Systems, man and Cybenetics, 1993

[14] Leclerc, F., Plamondon, R.: Automatic Signature Verification: The State of the Art - 1989-1993.Word scientific publishing co, Singapore 1994

[15] A.J.Mansfield, J.L.Wayman, Best Practices in Testing and Reporting Performance of biometric devices, Biometric Working Group, NPL Report CMSC 14/02

[16] G. Medioni, J. Choi, Cheng-Hao Kuo, and D. Fidaleo, “Identifying noncooperative subjects at a distance using face images and three-dimensional face models’’, Systems, man and Cybernetics, Part:A, Systems and Humans, IEEE Transactions on, 2009

[17] J. Daugman, “How iris recognition works,” Image Processing. 2002. Proceedings. 2002 International Conference on, 2002, pp. I-33-I-36 vol.1.

[18] Berry, J., Stoney, D.: History & Development of Fingerprinting. In: Lee, H.C., Gaensslen, R.E., Advances in Fingerprint Technology, pp1-40.CRC Press, Stoney

[19] Burke, J.: AuthenTec Ships Record 10 Million Biometric Fingerprint Sensors (2006)

[20] C.Maple, P.Norrington, The Usability and Practicality of Biometric Authentication in the Workplace, Proceedings of the First International Conference on Availability, Reliability and Security (ARES’06)

[21] P.Zhang, W.Liu, D.Yin, Y.Shi, X.Xu, ‘’ Analysis of fingerprint quality fot season factor‘’, ICCIP 17 November 24-26, Japan, ISBN 978-1-4503-5365-6/17/11, doi.org/10.1145/3162957.3163027, 2017

[22] F.D.Tatar, “ Fingerprint recognition algorithm, CCSEIT, AIAP, DMDB, ICBB,CNSA-2017

[23] V.Nidlova, J.Hart, ‘’ Reliabilty of Biomeric identification using fingerprints under adverse conditions’’, Agronomy Research 13(3), 786-791, 2015.

[24] N.C.Sickler, S.J.Elliot, “An evaluation of fingerprint image quality across an elderly population vis-à-vis an 18-25 year old population”, Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology ,IEEE , Las Palmas, 2005.

[25] H.Kang, B.Lee, H.Kim, D.Shin, J.Kim, “ A study on performance evaluation of fingerprint sensors”. AVBPA 2003, LCNS 2688, pp 574-583, 2003.

[26] S.K.Modi, S.J.Elliot, “Impact of Image Quality on Performance: Comparison of Young and Elderly Fingerprints”, Proceedings of the 6th International Conference on Recent Advances inSoft Computing, 2006.



**mr Marija Bogićević Sretenović,** asistent na Katedri za informacione tehnologije, Fakultet organizacionih nauka, Univerzitet u Beogradu
**Kontakt:** marija.bogicevic@fon.bg.ac.rs
**Oblast interesovanja:** elektronski sistemi plaćanja, zaštita računarskih sistema, biometrijske tehnologije



**Dejan Simić,** Fakultet organizacionih nauka, Univerzitet u Beogradu
**Kontakt:** dejan.simic@fon.bg.ac.rs
**Oblast interesovanja:** Zaštita računarskih sistema, Biometrijski sistemi



**Bojan Jovanović,** Fakultet organizacionih nauka, Univerzitet u Beogradu
**Kontakt:** bojan.jovanovic@fon.bg.ac.rs
**Oblast interesovanja:** virtualizacija, biometrija, DevOPS, microservices