SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Karlo Grlić

MODEL NENAMETLJIVE PROVJERE VJERODOSTOJNOSTI KORISNIKA POMOĆU FIZIČKE JEDINSTVENOSTI LICA ZA POVEĆANJE SIGURNOSTI UNUTAR PLATNOG SUSTAVA

Varaždin, travanj 2017.

Ovaj rad izrađen je u sklopu Centra za forenziku, biometriju i privatnost Fakulteta organizacije i informatike Varaždin pod vodstvom doc. dr. sc. Petre Grd i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2016./2017.

SAŽETAK

Naslov rada: *Model nenametljive provjere vjerodostojnosti korisnika pomoću fizičke jedinstvenosti lica za povećanje sigurnosti unutar platnog sustava*

Autor: *Karlo Grlić*

Tekst sažetka

Pretpostavci, da platni sustav nije siguran u prilog idu izvješća institucija povezanih s globalnim sustavom plaćanja. No, u isto vrijeme postoje tehnologije i metode koje u velikoj mjeri mogu pospješiti sigurnost. Postavlja se pitanje; zašto se u platni sustav ne uvedu dodatne sigurnosne provjere. Odgovor leži u činjenici da je platni sustav trom na promjene, što proizlazi iz nemogućnosti brze prilagodbe novim standardima i tehnologijama kako od strane korisnika, tako i od strane banaka. U radu su uzete u obzir činjenice o problemima implementacije novih sigurnosnih mjera te je napravljen model sustava unutar područja biometrije koji pruža rješenje za problem u danoj domeni. Rad pojašnjava dizajn modela primjenom metoda detekcije i verifikacije lica, kao jedne od jedinstvenih fizičkih karakteristika čovjeka, koja je ujedno i najmanje nametljiva. Osim toga, lice je odabrano i zbog široke rasprostranjenosti senzora koji mogu uzeti njegov uzorak, npr., mobiteli, prijenosna računala i sl. Također, za doprinos nenametljivosti razvijen je i model pomične kamere, koja olakšava uzimanje uzorka od korisnika na POS uređajima i bankomatima te ujedno korisniku olakšava uporabu takvog sučelja za transakcije, budući da se on sam ne mora pravilno pozicionirati. Osim toga, model predlaže i varijabilne granice sličnosti kod usporedbe lica prema visini transakcije. Model predstavlja i metodu obnavljanja baze lica svakom uspješnom transakcijom. Model je testiran s otvorenim i označenim bazama slika lica, a rezultat je sljedeći: maliciozni korisnik će biti prepoznat kao validan u manje od 1% slučajeva (razina pogrešnog prihvaćanja - FAR). Kako bi se isključila nemogućnost autentikacije validnog korisnika, rad predlaže i korištenje mobilnog tokena kao sekundarnog sredstva autentikacije. Rezultati testiranja ukazuju na to da bi se model mogao primijeniti u praksi te povećati sigurnost.

Ključne riječi: platni sustav, sigurnost, nenametljivost, detekcija, autentikacija, biometrija, lice

SUMMARY

Title: *A model of unobtrusive user credibility verification using physical face uniqueness for increasing security within the payment system*

Author: *Karlo Grlić*

Abstract

Reports of institutions connected with the global payment system go in the favor of the assumption, that the payment system is not safe. But, at the same time, there are technologies and methods which can, in great measure, improve security. That leads to the question, why are there no additional security checks? The answer lies in the fact that the payment system is slow to change, which is a result of incapability of consumers and banks to adapt to new standards and technologies fast. This work considers the facts about the problems of implementing the new security regulations and makes a system model, in the field of biometrics, which provides us with a solution to the problem in the given domain. Work explains the design of the model with adaptation of methods of detection and verification of the face, as one of the unique physical characteristics of human beings, which is also the least intrusive. Besides that, the face is chosen because of a widespread of sensors that can collect it's sample, for example, cell phones, laptops etc. As well, for the contribution to the obtrusiveness, a model of a moving self-adjustable camera has been developed, which facilitates taking samples of consumers from POS devices and ATM-s and also facilitates the usage of the interface for transactions, because the consumer does not need to position himself the right way. Besides that, the model suggests variable similarity acceptance boundaries for face recognition in relation to the height of transaction. Also, the model introduces user's face databases refreshing with every successful transaction. Model has been tested with open and marked database of face images and the result was as follows: the malicious user has been recognized as valid in less than 1% of the cases (False Acceptance Rate). In the case of incapability of the authentication of the valid user, the work advises the usage of a mobile token as a secondary authentication mean. The results indicate that the model could be applied in practice and that it will improve security.

Keywords: payment system, security, unobtrusiveness, detection, authentication, biometrics, face

PREDGOVOR

Ovaj rad je razvijan unutar Centra za forenziku, biometriju i privatnost Fakulteta organizacije i informatike Varaždin. Dok su u radu zastupljeni već vrlo dobro znani sigurnosni obrasci, poput dvofaktorske autentikacije i autentikacije biometrijom, autor smatra da rad najviše doprinosi, što se znanstvenog istraživanja tiče, u pogledu posebne brige o rasterećenju krajnjeg korisnika biometrijskog sustava nenametljivim pristupom. Pa je tako, između ostalog, u radu razrađen i prototipiran pokretni biometrijski senzor lica koji u praksi predstavlja novinu.

Kako autor nije imao pristupa internim bankovnim sigurnosnim sustavima, morat ćemo se zadovoljiti informacijama iz relevantne literature koja je navedena u tekstu, a tiče se upravo platnog sustava.

Rad u nekim dijelovima detaljnije opisuje pojedine koncepte, dok u drugima s nešto manje detalja. Razlog tome je to što je autor neke dijelove smatrao ponešto kompleksnijima pa ih je razložio na manje logičke cjeline (*Divide et impera!*), kako bi mu osobno, ali i svom čitateljstvu, bili puno jasniji. Također, pojedine metode i algoritmi opisani su formalno, dok su drugi opisani na razini implementacije. Ovo je zbog toga što su neki vrlo vezani za samu implementaciju pa ih je teško, ili besmisleno, formalno opisivati, dok one dijelove koji su formalno opisani, nije potrebno opisivati na implementacijskoj razini, jer je vrlo nezahvalno pojašnjavati određeni koncept u određenoj tehnologiji.

Posebna zahvala ide mentorici, doc. dr. sc. Petri Grd, koja je prilikom razvoja rada uvijek bila voljna pomoći savjetom, podrškom u okviru potrebnih resursa te poticajem na rad. Također, autor se zahvaljuje i prof. dr. sc. Miroslavu Baći, voditelju Centra za forenziku, biometriju i privatnost, na poticaju, podršci te pružanju prostora i materijala za rad, ali i na dugogodišnjem radu sa studentima na raznim kolegijima tijekom dodiplomskog i diplomskog studija.

KARLO GRLIĆ

Fakultet organizacije i informatike Varaždin
travanj, 2017.

Sadržaj

1 Uvod

Razvitkom računala i računalno potpomognutih oblika komunikacije pojavila se i mogućnost, a samim time i potreba prijenosa financijskih dobara, kao jedne od temeljnih poslovnih aktivnosti. Od početka uporabe novca, ili bilo kojeg drugog oblika univerzalno prihvaćene valute kao oblika plaćanja, postojala je opasnost od gubitka, krađe te uništenja takvog dobra.

Usavršavanjem i inovacijom metoda prijenosa sredstava, a pogotovo pomoću računalnih tehnologija, uspjelo se reducirati mogućnost gubitka i uništenja, no u pogledu krađe nije došlo do očekivane razine smanjenja. Razlog tome je, osim što je korisnička strana platnog sustava najranjivija, i kompleksnost implementacije sigurnosnog sustava koji ne bi dodatno opterećivao te zadirao u privatnost korisnika. Ovaj radu bavit će se upravo dizajnom sigurnosnog modela koji ne bi imao veliki utjecaj na kompleksnost, niti bi opterećivao korisnika, nego upravo suprotno; pružio bi korisniku osjećaj sigurnosti i kontrole.

1.1 Predmet rada

Moderna znanost o jedinstvenim karakteristikama čovjeka relativno je nova, a veliki uspon doživjela je unatrag zadnjih nekoliko desetljeća, no njezini počeci sežu, naravno, i iz ranijih razdoblja, ali i drugih znanstvenih disciplina poput medicine, biologije, fizičke i bio-antropologije, arheologije i dr. Iako u tim vremenima nije postojala formalna znanost koja bi se ticala isključivo jedinstvenosti karakteristika čovjeka, ipak, vremenom se i razvojem okolnosti moglo nazrijeti da će doći do formaliziranja iste, što se je spomenuto, i dogodilo.

Danas je biometrija vrlo razvijena znanost te je neizostavni dio moderne forenzike, sudske medicine, naprednih sigurnosnih sustava i sl. No, kao i ostale moderne znanosti, biometrija ima svoje granice, pogotovo u pogledu:

- onoga što se s njome može postići,
- okolnosti u kojima je uporabljiva i prihvatljiva i
- pouzdanosti koju pruža.

Stoga, prilikom uvođenja biometrije u bilo kakav sustav, potrebno je prethodno napraviti analizu stanja i artefakata sustava, vrijednost imovine, ljudskog faktora i rizika te isplativost investicije.

S druge strane, kako je u uvodu rečeno imamo platni sustav, tj. sustav novčanih transakcija, s kojim smo, direktno ili indirektno, gotovo u stalnoj interakciji. Prema tome, institucijama, ali i njihovim korisnicima, od velikog je interesa da platni sustav bude što je moguće sigurniji. U platni sustav je do danas implementirana nekolicina ključnih sigurnosnih značajki od kojih su najznačajnije:

- identifikacija korisnika pomoću kreditne kartice (ili drugog sredstva),
- autentikacija (verifikacija identiteta) pomoću PIN-a (lozinke, tokena, biometrijske značajke i sl.) i
- potvrda transakcije pomoću mobilnog tokena (ili sličnog uređaja, tzv. *3-D Secure*).

Predmet ovog rada upravo je dizajn modela i kreiranje funkcionalnog prototipa koji bi dodatno osigurali platni sustav, a to će u ovome radu biti ostvareno provedbom relevantnih analiza i procjena, proučavanjem literature te ispitivanjem mogućnosti implementacije biometrije lica u platni sustav.

1.2 Hipoteze i pretpostavke

Razmatranjem svega izrečenoga u predmetu rada, tj. samog merituma, postavljaju se dolje navedene pretpostavke i hipoteze oko čijeg će potvrđivanja, odnosno odbacivanja, rad biti usredotočen.

Na pretpostavci da *u platnom sustavu postoje sigurnosni propusti* temelji se cijeli rad. Ako bi platni sustav bio siguran, tj. dovoljno siguran, tada ne bi bilo smisla uvoditi nove tehnologije jer su postojeće sasvim dovoljne. Kako bi se ova pretpostavka potkrijepila u radu će se pozivati na relevantna izvješća i literaturu povezanu s platnim sustavom. Također, u radu će se platni sustav i analizirati te će se pokušati identificirati najkritičnije točke.

Hipoteza 1 (H1) - *Uvođenjem biometrijske provjere lica u platni sustav, kao dodatne mjere verifikacije, maliciozni korisnici bit će prepoznati u više od 90% slučajeva.*

H1 pretpostavlja da biometrija lica pruža kvalitete koje čine neku biometrijsku značajku sigurnom za korištenje u sustavima poput ovog. Drugim riječima, provjerom lica, transakcije malicioznih korisnika bit će zaustavljene u više od 90% slučajeva. Hipotezu H1 pokušati će se dokazati razlaganjem relevantne teorije, implementacijom prototipskog modela i algoritama te testiranjem uspješnosti rada prototipa. Kako se potvrda H1 oslanja i na uspješnu implementaciju prototipa, u radu će se s posebnom pažnjom pristupiti izradi i implementaciji istog.

Hipoteza 2 (H2) - *Konstruirani pomični senzor pronalazi položaj osobe izvan vidljivog polja kamere, unutar kuta od 120° i udaljenosti 1 metra te prepoznaje i prati pomake lica do udaljenosti od 1 metra.*

H2 pretpostavlja da je odabrana biometrijska značajka lica među najmanje nametljivima prema korisniku te se može učiniti još manje nametljivom, do razine gdje korisnik nema bojazni za uporabu, niti treba imati ikakva tehnička znanja o uporabi. U ostvarivanju ovoga, konstruirat će se pomični senzor, tj. kamera, koja će pronalaziti i pratiti kretnje lica te naposljetku uzeti potreban uzorak. U ovome se, između ostalog, najviše ogleda znanstveni doprinos ovog rada.

Kako bi se hipoteza H2 provjerila, koristit će se fizičke fotografije lica stvarne veličine, koje će biti prezentirane samom senzoru uz varijabilnost udaljenosti i pozicije unutar prostora. Prema navedenom će se mjeriti uspješnost rada senzora, tj. mjera uspješnosti uzet će se kao mjerodavna za prihvaćanje ili odbacivanje hipoteze H2.

1.3 Opći i specifični ciljevi

Ciljevi ovoga rada usko su povezani s početnim hipotezama pa je tako opći cilj:

- *unaprijediti sigurnost platnog sustava u okviru dodavanja dodatne provjere identiteta korisnika pomoću jedinstvenosti fizičke osobine lica, a da se pri tome ne naruši jednostavnost korištenja*.

Nadalje, izvedeno iz općeg, specifični ciljevi jesu:

a) *izučiti i analizirati postojeći platni sustav te uočiti njegove sigurnosne propuste, što će nam predstavljati daljnji orijentir u istraživanju*,

b) *dizajnirati model putem kojega će se ostvariti veća sigurnosti i koji će se oslanjati na biometriju lica,*

c) *implementirati vjerni prototip prema dizajniranom modelu, koji će poslužiti i za testiranje performansi modela,*

d) *konstruirati uređaj kao sastavni dio prototipa, koji će omogućiti olakšano uzimanje uzoraka lica i smanjiti opterećenje korisnika kod korištenja ovoga modela, i*

e) *testirati rad modela i potvrditi iskoristivost u praksi.*

1.4 Metodologija

Valja definirati i opće načine na koji će se pristupiti problemu i predmetu rada, dokazivanju hipotezi i ostvarivanju zadanih ciljeva. Pristup mora omogućiti provedbu namijenjenoga te svrsishodno testiranje i provjeru ostvarenja ciljeva, a u konačnici potvrdu, odnosno odbacivanje hipoteza.

Ovaj rad za postizanje navedenog koristi kako kvantitativne, tako i kvalitativne metode. Ovo proizlazi iz razloga što rad obrađuje probleme čija rješenja nije moguće uvijek kvantitativno predstaviti, poput npr. korisničkog iskustva, jednostavnosti korištenja, itd., dok se s druge strane rad u velikoj mjeri oslanja na matematičke i statističke metode kao što su mjere sličnosti, udaljenosti u prostoru, srednje vrijednosti i sl. U nastavku slijedi pregled metoda za svaku od cjelina rada prema hipotezama i zadanim ciljevima.

Prvi korak je pregled literature, tj. pregled radova koji su tematski slični ovome radu ili se bave istom tematikom. Ovime će se steći bolja slika o tome koji su vanjski doprinosi ovoj temi, a ujedno će se moći i bolje procijeniti značaj i doprinose ovoga rada. U okviru iste cjeline bit će napravljen pregled sličnih sigurnosnih modela koji se već koriste u praksi. Ovaj korak dat će dobar temelj za gradnju modela, jer će se u usporedbi s ostalim radovima, moći zaključiti kakve su kvalitete potrebne da bi se model pokazao uspješnim, a po mogućnosti i superiornijim nad ostalima.

Nakon toga slijedi pregled i rasprava o platnom sustavu. U ovom dijelu će se također izvršiti pregled relevantne literature i statističkih izvješća koja mogu dati što jasniju sliku o stanju sigurnosti platnog sustava i o tome koji su njegovi trenutni nedostaci.

U sljedećem koraku razložiti će se osnove biometrijske znanosti, a posebno će se obratiti pozornost na biometriju lica. Kao i u prethodnim koracima, koristit će se shodna literatura. Osim toga, u ovoj cjelini obradit će se sastavnice sustava biometrijske autentikacije licem - detekciju i verifikaciju. S tim u vezi, obradit će se recentni algoritmi koji će biti predloženi za implementaciju u modelu, a i korišteni u samome prototipu. U ovom poglavlju primijenit će se analiza algoritama i obrada povezane matematičke teorije.

Nastavno na sve prethodne korake, slijedi i sam dizajn, tj. projektiranje, modela i implementacija prototipa. U ovome će se djelu u velikoj mjeri koristiti metode softverskog i elektroničkog inženjerstva - *UML modeliranje, modeliranje podataka, razvoj algoritama, programskih proizvoda i elektronike*. Cilj je polučiti što sveobuhvatniji i sigurniji model, ali i što vjerniji prototip, kako bi se u sljedećoj fazi mogle izmjeriti performanse.

Konačno, model će se putem prototipa i testirati. U ovome koraku bitno je da se testovi izvedu što je moguće objektivnije i da se pokušaju simulirati stvarni uvjeti. U te svrhe model će se testirati u kontroliranim uvjetima putem dostupne baze fotografija lica i metodama pojašnjenim u poglavlju testiranje. Osim toga, važna stavka je i valjana interpretacija dobivenih rezultata. U tome će poslužiti statistička analiza i obrada

podataka u okviru: *određivanja srednjih vrijednosti skupova podataka, klasifikacije prema znanim obilježjima i testiranje hipoteza o pripadnosti uzorka*. Ovo će omogućiti donošenje zaključaka temeljenih na valjanim pretpostavkama čineći ovaj rad vjerodostojnim za korištenje u praksi ili daljnjim istraživanjima.

Naposljetku, putem dobivenih rezultata donosimo zaključak te kratku raspravu o doprinosima, nedostacima i isplativosti modela.

2 Pregled literature

U ovome poglavlju izvršit će se pregled i rasprava sličnih modela zaštite platnog sustava biometrijom lica koji se već koriste u praksi, ali isto tako i pregled radova koji se bave ovom tematikom. Cilj ovoga je imati uvid u već postojeće modele i koncepte zaštite biometrijom kako bi se mogao procijeniti značaj rada, ali i obratiti pozornost na nedostatke istih te ih u ovome modelu ispraviti.

2.1 Pregled sličnih modela u praksi

Ideja da se biometrija koristi u svrhe autenticiranja korisnika kod novčanih transakcija postoji već dugi period vremena. No, do danas, na globalnoj razini, ne postoji općeprihvaćeni sustav, iako je postojeća tehnologija i informacijska infrastruktura dostatna za njegovu implementaciju. Također, biometrijski sustavi kod transakcija uglavnom koriste biometrijsku provjeru otiska prsta, šarenice, vena ili glasa, dok se verifikacija licem u te svrhe počela spominjati tek prije nekoliko godina.

Koliko je poznato, na tržištu postoji samo nekolicina sustava koji koriste lice kao način provjere identiteta korisnika. Uporaba biometrije lica na bankomatima započela je u Kini, gdje su 2015. u pogon stavljeni prvi certificirani bankomati koji omogućuju autentikaciju provjerom lica umjesto provjerom PIN-a (Middlehurst, 2015).

Najrašireniju uslugu plaćanja provjerom lica do sada, ponudila je kartična kuća MasterCard, koja svoju tehnologiju, "*Selfie Pay*" odnedavno nudi u 16 država, nakon što je tehnologiju uspješno testirana na tržištima Nizozemske, Kanade i Sjedinjenih Država (MasterCard, Inc, 2016). Osim MasterCarda, vrlo sličan koncept plaćanja putem biometrije lica razvijaju Amazon, koja razvija mobilnu aplikaciju za plaćanja u svojim web trgovinama, (US Patent & Trademark Office, 2016) i Samsung, koji uskoro planira ponuditi uslugu "*Samsung Pay*" koja bi se provodila pomoću S8 pametnog telefona (Business Insider, Inc, 2017). Koncept MasterCarda i Amazona temelje se isključivo na korištenju mobilnog uređaja.

Nešto drugačiju uslugu nudi tvrtka Uniqul, koja posjeduje centralizirani sustav identifikacije i autentikacije korisnika na prodajnom mjestu putem vlastitih POS uređaja. Od korisnika ne traži dodatna autentikacija, već se transakcije autoriziraju prepoznavanjem lica (UNIQUL, 2013).

Navedeni modeli nisu jedini, no u trenutku pisanja rada imali su najrašireniju uporabu. Primijetimo, spomenuti modeli isključuju korištenje lozinke ili PIN-a te se oslanjaju samo na biometrijsku provjeru, što je fundamentalno različito od predmeta istraživanja ovog rada.

2.2 Pregled objavljenih radova

Iako je autentikacija licem tema mnogih radova, u ovom poglavlju izvršit će se pregled radova koji se bave užom tematikom - autentikacijom licem kod vršenja novčanih transakcija, tj. radnji unutar platnog sustava. Razlog je taj što se za primjena ovakve biometrijske metode zahtijeva uzimanje u obzir nekoliko važnih čimbenika:

- visoka sigurnost,
- jednostavnost uporabe,
- prilagodljivost uvjetima, i
- namijenjenost globalnoj uporabi.

Hemery et al. (2008) ističu kako je lice pogodno za uporabu na uređajima za plaćanje i bankomatima jer omogućuje beskontaktnu biometrijsku provjeru što uklanja brigu o higijeni na javnim mjestima. Također, važne stavke su i niska cijena CCD senzora, tj. digitalne kamere i jednostavnost uporabe. Autori predstavljaju metodu prepoznavanja lica koja dozvoljava parcijalne okluzije lica, što je bitno stavka jer korisniku omogućuje nošenje odjeće, naočala, pokrivala za glavu, itd., koji bi kod ostalih metoda smetali u prepoznavanju. Metoda za prepoznavanje koristi set karakterističnih točaka lica čije kompletno podudaranje nije potrebno kako bi se zaključilo radi li se u valjanom korisniku.

Malviya (2014), uz provjeru identiteta PIN-om, uvodi provjeru lica iz 3 različita kuta - frontalno, s desne strane i s lijeve strane. Ovime se postiže vrlo visoka razina sigurnosti biometrijske provjere. Autor predviđa da se metoda koristi samo na bankomatima koji imaju mogućnost uzimanja uzorka lica iz različitih kuteva. Unatoč tome, rad ne predviđa dodatne mjere autentikacije ako se korisnik nije u mogućnosti autenticirati licem.

Parmar i Mehta (2013) se slažu da se već postojeća nadzorna infrastruktura na mjestima od visoke sigurnosti pa tako i u bankama i na bankomatima, može iskoristiti za bolju zaštitu pomoću prepoznavanja lica. Također autori ističu kako je prepoznavanje lica kod bankovnih sustava u službi verifikacije identiteta, što je različito od namjene sustava za nadzor, istragu i općenitu sigurnost, gdje se prepoznavanje koristi za identifikaciju pojedinaca.

Kumar i Vijayaragavan (2014) predlažu model bankomata bez korištenja kreditne kartice i pina, gdje se korisnik identificira i autenticira s nekim od 3 stupnja biometrijske provjere. Prvi stupanj provjere jest provjera otiska prsta. Ako je sličnost uzorka otiska prsta do 98%, tada se uz provjeru otiska provjerava i uzorak lica. Ako je sličnost otiska prsta manja od 98%, tada se koristi provjera uzorka šarenice.

Kao i u slučaju modela koji se već koriste u praksi, samo nekolicina sličnih objavljenih radova koristi kombinaciju kartice, PIN-a i biometrije lica, što sa ovim radom nije slučaj. Također, metode koje se preporučaju, izuzev rada Hemery et al. (2008), previše su invazivne, dok ovaj rad pokušava smanjiti utjecaj na krajnjeg korisnika sustava.

3 Rasprava o sigurnosti platnog sustava

U ovom poglavlju raspravljeni su sigurnosni problemi platnog sustava. Poglavlje, a i ostatak rada, isključivo se bavi sigurnošću korisničkog, tj. klijentskog dijela sustava, kao dijela koji nosi najveći sigurnosni rizik. Pod klijentskim dijelom sustava misli se na interakciju, ali i točke interakcije klijenta i sustava transakcije financijskih sredstava.

3.1 Platni sustav

Da bi se moglo identificirati ključnu problematiku vezanu uz sustav platni, tj. sustav novčanih transakcija, potrebno je definirati njegov opći model rada. Kossler (2013), Gulati i Srivastava (2007) i Hrvatska narodna banka (2014) slažu se da je platni sustav zapravo višeslojni heterogeni sustav s nekoliko komponenata ili subjekata, ovisno o transakcijama koje se u njemu obavljaju. Dakle, može se ustvrditi da u sustavu postoje minimalno dva ključna subjekta; korisnik koji inicira prijenos sredstava te financijska ustanova koja raspolaže korisnikovim sredstvima. Ako postoji i treća strana, koja prima sredstva s korisnikovog računa, onda se radi o sustavu s tri, odnosno četiri sudionika, računajući i banku onoga tko prima sredstva na svoj račun. Čest slučaj je sustav s pet ili više sudionika, pogotovo prisutan kod online plaćanja, gdje su ostali sudionici pružatelji nekog od dijelova složenog platnog sustava, koji u datom trenutku raspolaže korisnikovim financijskim podacima. Sastavnice takvog sustava su: sučelje putem kojeg korisnik vrši interakciju, tj. unosi svoje financijske podatke, platni servis koji autenticira korisnika, mreža obrade transakcije i platni sustavi banaka. Apstrakcija funkcioniranja sustava dana je na slici 3.1.

Način rada sustava ovisi o mjestu, svrsi i načinu na koji se odvija transakcija. Ovisno o prethodnim faktorima, sučelje za transakciju, ali i poveznica s financijskom ustanovom bit će drugačija. Ono što je svakako zajedničko svakom obliku transakcija je korištenje nekog oblika identifikacije i autentikacije pri odabranom platnom sučelju, bilo da se radi o kreditnim, debitnim i ostalim bankovnim karticama ili brojevima bankovnih računa, računa online sustava plaćanja, itd. Ako se pretpostavi da je kanal između financijskih institucija, banaka i dr. siguran, kao najkritičniji dio sustava može se identificirati sigurnost komunikacije između korisnika i sučelja i sučelja i financijske ustanove.

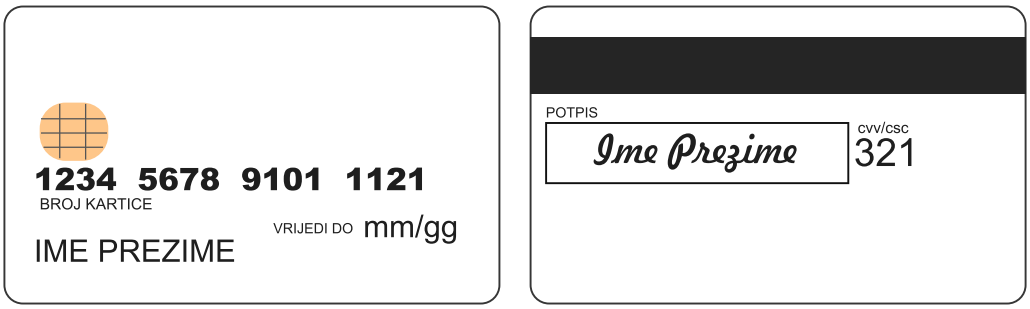
Slika 3.1: Apstrakcija funkcioniranja platnog sustava

3.2 Analiza propusta u platnom sustavu

Da sigurnosni propusti u postojećem sustavu uistinu postoje, potvrđuje i izvješće Europske centralne banke o kartičnim prijevarama (European Central Bank, 2015) (engl. *credit card fraud*), u kojemu se navodi kako je 2013. godine ukupna količina kartičnih prijevara iznosila 1.44 milijarde eura, što je 0.039% svih transakcija u Europskoj uniji, a ujedno je ta brojka i 8% veća nego 2012. godine, što ukazuje i na blagi trend povećanja. Prema izvješću organizacije Payments Cards and Mobile (Payments Cards & Mobile, 2015), koja prati kartične i mobilne transakcije na globalnoj razini, stoji kako je u SAD-u ta stopa iznosila čak 0.1%, tj. 4.15 milijardi eura, dok je u Kanadi ona 0.08% ili 361.5 milijuna eura. U navedenim izvještajima postoji nekoliko klasifikacija kartičnih prevara, no u ovom radu zadržat će se samo na jednoj - onoj koja ujedno objedinjuje i ostale. Ta klasifikacija prepoznaje prevare uz posjedovanje kartice (engl. *card-present*), gdje je

kartica ukradena, krivotvorena i sl. te prevare gdje kartica nije fizički prisutna (engl. *card-not-present*[1]).

Postavlja se pitanje, koji sigurnosni propusti dozvoljavaju da se financijski podaci i platna sredstva otuđe od korisnika, a koji da se isti ponovno upotrijebe za neovlaštene radnje. Kao što je već rečeno, najkritičniji je dio platnoga sustava interakcija korisnika sa sučeljem za transakciju. Pri interakciji sa sučeljem korisnik razmjenjuje identifikacijske i autentikacijske podatke strogo znane samo korisniku i bankovnoj ustanovi te ih tim činom izlaže mogućoj krađi i zloupotrebi. U globalu su takvi podaci zapravo informacije zapisane na kreditnim karticama (slika 3.2), kao primarnim sredstvima identifikacije te povezani PIN[2] brojevi, koji su u službi autentikacije korisnika. U skupinu ovakvih podataka također spadaju i autentikacijski podaci platnih servisa poput npr. PayPala, online i mobilnog bankarstva, itd., no kako su takvi servisi gotovo uvijek vezani uz neki bankovni račun, tj. karticu, iste se za sad može svrstati u istu kategoriju, iako će se kod dizajna i implementacije sustava svakako obratiti pozornost na primjenjivost kod takvih tehnologija.



Slika 3.2: Podaci prisutni na kreditnoj kartici

Na slici 3.2 može se primijetiti da su vidljivi podaci na kreditnoj kartici sljedeći: ime i prezime vlasnika kartice, šesnaesteroznamenkasti broj kreditne kartice (PAN[3]), valjanost kreditne kartice u obliku mjesec/godina, troznamenkasti ili četveroznamenkasti kontrolni broj CVV, CVV2, CVC, CSC, itd. (PCI Security Standards Council LLC, 2010).

Podaci vidljivi na pozadini i poleđini kartice dovoljni su da se putem njih napravi online transakcija koja ne zahtijeva fizičko posjedovanje kartice (CNP), što je jedan od propusta trenutnog sustava. Ovome se problemu u novije vrijeme pokušalo doskočiti korištenjem tzv. tokena, točnije, tehnologije poznatije pod imenom 3-D Secure, kojom korisnik, unošenjem generirane lozinke na svojemu telefonu ili unaprijed znane lozinke, potvrđuje da upravo on koristi karticu (MasterCard Payment Gateway Services Ltd, 2016). Problem

[1] Engl. Card-not-Present, ili kraće CNP, opći je naziv za sve transakcije koje ne zahtijevaju fizičko posjedovanje kartice. Uglavnom se radi o transakcijama online.

[2] Engl. *Personal Identification Number* - broj znan jedino korisniku kartice, a pomoću kojeg korisnik potvrđuje da upravo on pomoću kartice vrši transakciju.

[3] Kratica od engl. *Primary Account Number* - identifikator kreditne kartice.

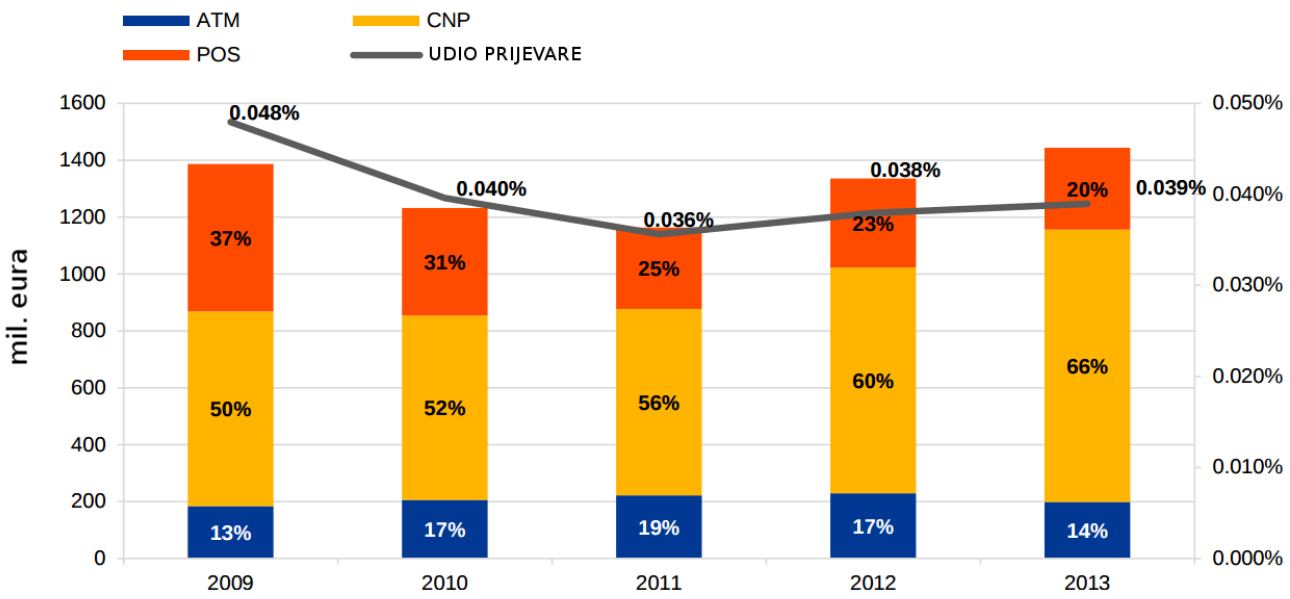
u korištenju tokena leži u tome da isti, zbog velike neprihvaćenosti kako od trgovina, tako i od korisnika, često nije obligatoran te u većini online trgovina i nije implementiran.

Osim vidljivih informacija, na kreditnim karticama može se uočiti i magnetna vrpca te elektronički EMV[4] čip koji je uveden nešto kasnije. Magnetna vrpca može se sastojati od nekoliko redundantnih traka koje, osim određenih tehničkih podataka, sadržavaju uglavnom podatke koji su vidljivi na samoj kartici (Authorize.Net LLC, 2015). Magnetna vrpca vrlo je zastarjela i ranjiva tehnologija te je glavni razlog zbog kojeg je i uveden EMV čip. U Hrvatskoj, a i u većini drugih zemalja, magnetna vrpca više se ne koristi, iako je zbog kompatibilnosti zadržana na kreditnim karticama. Treba spomenuti da je do 2012.-te godine magnetna vrpca bila i jedini oblik identifikacije na karticama korisnika u SAD-u (American Express Company, 2012), a tek se početkom 2015.-te EMV čip počeo i aktivno koristiti te upravo zbog toga u SAD-u ima i najviše kartičnih prevara (EMVCo LLC, 2016b; Payments Cards & Mobile, 2015). Ranjivost kartica s magnetnom vrpcom, tj. ranjivost sustava koji prihvaća samo magnetnu vrpcu, krije se u činjenici da se podaci zapisani na magnetnoj vrpci mogu vrlo lako očitati i zapisati na drugu karticu pomoću koje se tada može neovlašteno provoditi transakcije. Ako uzmemo u obzir da je napadač uspio doći i do PIN-a kartice, što nije rijetkost, tada napadač može pristupiti svim dostupnim sredstvima korisnika.

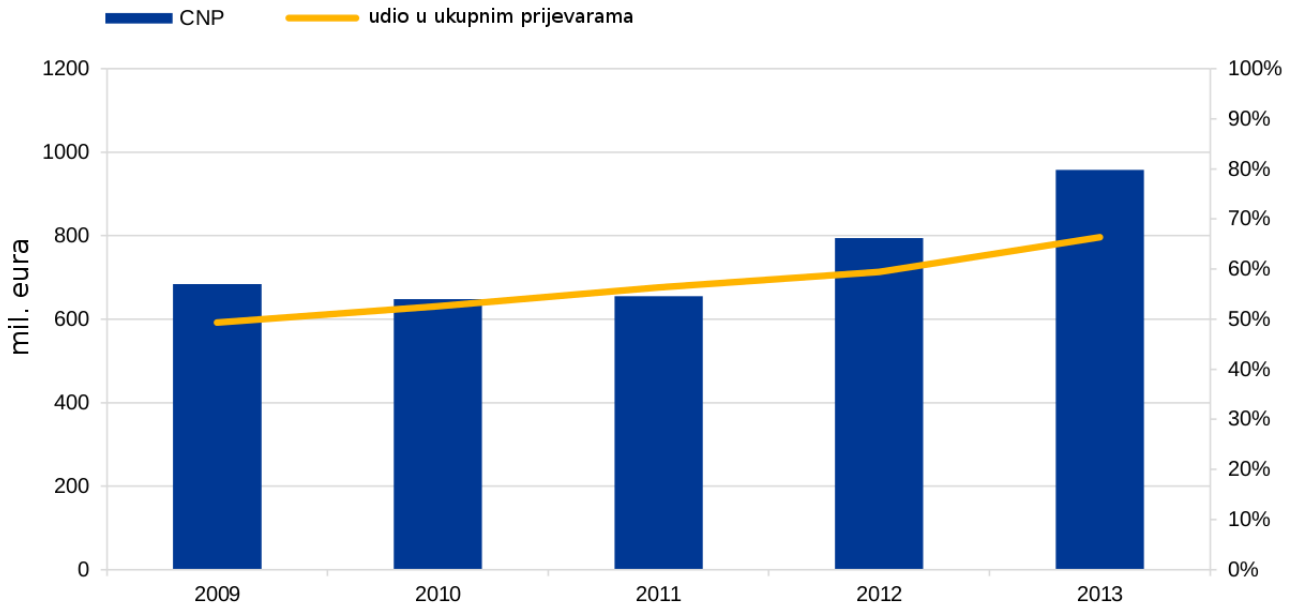
Navedeni propust rezultirao je uvođenjem već spomenutog EMV čipa, tj. sustava. Najbitnija razlika između čipa i magnetne vrpce je da se prilikom transakcije putem čipa vrši i autentičnost kartice, što je postignuto digitalnim potpisom, tj. zapisivanjem jedinstvenog broja svake transakcije (engl. *nonce*) na samu karticu, pojašnjavaju Murdoch et al. (2010). Kako je sadržaj kartice sada pri svakoj transakciji uvijek drugačiji, ne može se dogoditi da u isto vrijeme u opticaju budu originalna kartica i njene kopije. Iako se EMV sustav u svojem početku činio vrlo sigurnim, tijekom vremena otkrilo se da zapravo skriva vrlo ozbiljne sigurnosne propuste, ističu Murdoch et al. (2010).

Unatoč propustima u EMV tehnologiji, autori Murdoch et al. (2010) ističu kako je uvođenje EMV čipa ipak znatno smanjilo prevare u kojima je potrebno fizičko posjedovanje kartice (CP), odnosno njene kopije. Ono što ne iznenađuje je da se pojavio istovremeni porast broja prevara u kojima nije potrebno fizičko posjedovanje kartice (CNP). S ovime se također slažu i izvještaji Europske centralne banke i Payments Cards & Mobile-a (EMVCo LLC, 2016b; Payments Cards & Mobile, 2015). Udjeli su dani i prikazima 3.3 i 3.4.

[4] EMV je kratica za Europay - MasterCard - Visa, standard zaštite platnih kartica elektroničkim čipom (EMVCo LLC, 2016a).



Slika 3.3: Udjeli tipova kartičnih prevara od 2009. do 2013. godine. Preuzeto iz: European Central Bank (2015). Pojašnjenje: CNP - kartica nije prisutna, POS - POS uređaj, ATM - bankomat.



Slika 3.4: Rast prijevara u kojima kartica nije prisutna (CNP) kroz 2009. do 2013. godinu. Preuzeto iz: European Central Bank (2015).

Uzevši u obzir sve izneseno, može se zaključiti kako su trenutni problemi platnog sustava izazvani sigurnosnim propustima sljedeći: nedovoljna zaštita financijskih podataka korisnika, nepostojanje dovoljno pouzdane tehnike autentikacije korisnika, odnosno onemogućavanje krađe identiteta te tromost u implementaciji novih sigurnosnih tehnologija.

3.3 Iskorištavanje propusta u platnom sustavu

Prethodno su istaknuti glavne sigurnosne propuste trenutnog platnog sustava. Kako bi se imalo bolje razumijevanje posljedica sigurnosnih propusta, ali i onoga što se događa iza njih, a samim se time znalo i bolje zaštiti, u ovom poglavlju istražiti će se načini na koje napadači otuđuju financijska sredstva, kako ih koriste te kako općenito funkcionira cyber-kriminal[5] u pogledu novčanih transakcija i platnih sredstava.

Krađe financijskih podataka izvode se na veliki broj načina, no svakako znamo da se najviše krađa odvija na mjestima gdje se financijski podaci koriste. Stoga, može se zaključiti da su žarišta takvih aktivnosti: blagajne uslužnih centara, bankomati, POS uređaji, web stranice online trgovina i platnih servisa te poslužitelji na kojima se čuvaju informacije o kreditnim karticama korisnika. Vezano uz navedena žarišta, prepoznajemo sljedeće metode kojima se služe napadači: fizička krađa, skimming i nelegalne modifikacije uređaja, socijalni inženjering, phishing te maliciozni programi.

Fizička krađa - najprimitivniji je oblik krađe financijskih podataka, no nikako nije i bezazlen. Napadač krađom dolazi u vlasništvo kreditne kartice ili drugog dobra, a PIN često saznaje prevarom ili kreditnu karticu koristi online.

Skimming i modifikacija uređaja uključuje nelegalne izmjene ili dorade na bankomatima i POS uređajima koje napadačima omogućuju da preuzmu podatke s kreditnih kartica te, također, dođu i do povezanih PIN-ova. Jedan od načina realizacije ove metode je da se na utor za karticu uređaja postavi elektronička naprava koja je običnom korisniku neupadljiva i koja se doima kao dio samog uređaja. Unutar takve naprave nalazi se čitač magnetske trake ili EMV čipa. Osim toga, sastavni dio skimmera je i lažna tipkovnica za unos PIN-a ili minijaturna kamera koja služi za krađu PIN-a. Primjer skimmera dan je na slici 3.5.

Slika 3.5: Skimmer - lažni čitač kartica i tipkovnica za unos PIN-a

[5] Cyber-kriminal označava pojam vršenja kriminalnih radnji u virtualnom internetskom okružju. Iako se ovaj tip kriminala vrši u virtualnom prostoru, njegove posljedice nisu nimalo bezazlenije od ostalih oblika.

Slika 3.5 preuzeta s http://www.bankrate.com/financing/wp-content/uploads/2014/07/banking-blog-atm-skimmer-at-a-cash-machine-in-germany.jpg

Hardverske modifikacije uređaja - uglavnom se odnose na POS uređaje, a njima se nelegalno zamjenjuje originalni uređaju pa takvi uređaji onda podatke šalju i napadaču. Jedan od najvećih napada pomoću skimmer uređaja dogodio se 2013.-te godine u američkom trgovačkom lancu Target, gdje je pomoću malicioznog koda u POS uređajima ugroženo oko 40 milijuna kreditnih kartica (Krebs, 2016). Pojavom beskontaktnih kartica za plaćanje pojavili su se skimmeri koji učitavaju podatke s ugrađenog RFID čitača.

Socijalni inženjering - iako nije tehnička metoda, često se koristi i vrlo je uspješna. Ovom metodom, pojašnjava Nacionalni CERT (2016b), napadač manipulacijom pokušava pridobiti korisnika da oda osjetljive podatke kojima napadač inače ne bi mogao pristupiti. Nerijetko se radi o financijskim podacima. Da bi dobio na uvjerljivosti, napadač uglavnom iskorištava neku poznatu činjenicu o korisniku, npr. ime i prezime, broj telefona, posjedovanje računala, itd. Napadači uglavnom ciljaju na veliki broj korisnik kako bi zarada bila što unosnija.

Phishing - metoda koja je vrlo bliska socijalnom inženjeringu, iako sadržava svoju tehničku komponentu. Naime, kod phishinga napadač pokušava pridobiti korisnika da posjeti određenu web stranicu ili servis koji se naoko čini legitimnim ili pak impersonirati neki drugi legitimni servis, gdje korisnik unosi svoje podatke koji tada bivaju poslani napadaču (Nacionalni CERT, 2016a).

Maliciozni programi - (engl. *malware* ili *crimeware*[6]) vrlo su proširena metoda koja se vrlo često koristi za krađu financijskih, ali i drugih podataka te općenito za iskorištavanje korisnikovih resursa. Korištenje malicioznih programa tehnički je najsloženija metoda krađe osobnih podataka. Princip rada malicioznog programa je sljedeći: jednom instaliran na zaraženo računalo maliciozni program uspostavlja komunikaciju s napadačem otkrivajući mu tako osjetljive podatke koji se nalaze na korisnikovu računalu ili snimajući korisnikove radnje. Napadač putem malicioznog programa može, također, i upravljati računalom putem tzv. komandnog i kontrolnoga centra (engl. *Command and Control*) te tako vršiti kriminalne radnje. Sood et al. (2013) pojašnjavaju rad složenog kriminalnog sustava iza samih malicioznih programa. Autori navode kako životni ciklus krađe podataka putem malicioznog programa ima tri etape:

1. kupnja potrebnog malicioznog softvera i resursa,
2. zaraza računala malicioznim softverom, i
3. izvlačenje financijskih i ostalih podataka s računala žrtava.

Kako je izloženo, krađa financijskih podataka pomoću propusta u platnom sustavu je, zapravo, vrlo jednostavna. No, logički se postavlja sljedeće pitanje; kako napadač dolazi do konkretnih novčanih sredstava putem otuđenih podataka? Kossman (2014) izlaže četiri najčešće metode korištenja ukradenih financijskih podataka, tj. kreditnih kartica:

[6] Termin crimeware služi za označavanje malicioznog programa kao vrlo štetnog po korisničku imovinu. Uglavnom se misli na osjetljive podatke - u ovom slučaju financijske podatke.

- preprodaja na crnome tržištu,
- krivotvorenje kartica,
- online trgovina, i
- plaćanje usluga kreditnim karticama.

Sood et al. (2013) navode kako se novac isplaćuje i preko treće strane, tzv. "monetna mazga" (engl. *money mule*), koja je specijalizirana za takve radnje.

Preprodaja na crnome tržištu - vjerojatno je najčešća metoda unovčavanja ukradenih financijskih podataka zato što prodavač uklanja rizik toga da pri korištenju istih bude uhvaćen. Kreditne kartice i ostali podaci prodaju se u specijaliziranim online trgovinama i forumima. Cijena financijskih podataka na crnome tržištu ovisi primarno o geografskoj lokaciji izdavanja kartice, valjanosti, tipu te količini informacija o vlasniku kartice, iznosi Kossman (2014). Cijene se mogu kretati od nekoliko dolara do nekoliko stotina dolara.

Treće strane - unajmljuju se za isplatu sredstava, smanjuje rizik, ali i zaradu. Sood et al. (2013) pojašnjavaju da se zarada uglavnom dijeli u omjeru 40:60 u korist treće strane, koja je specijalizirana za isplatu i krađu identiteta, a isplata se uglavnom vrši osobno u banci.

Krivotvorenje kartica - uglavnom je vezano uz skimming, a sastoji se od iščitavanja kartičnih podataka sa skimming uređajem te naposljetku i zapisivanjem tih podataka na nove kartice. Podaci se uglavnom iščitavaju i zapisuju na magnetsku vrpcu kartice. Kako je već ranije rečeno, uvođenjem EMV čipa korištenje ove metode se smanjilo, no kako je korištenje magnetske vrpce još uvijek prihvatljivo na nekim mjestima metoda se još uvijek nastavlja koristiti, objašnjava Kossman (2014).

Online trgovina - napadač može iskoristiti karticu za preprodaju dobara putem online trgovina. Kako bi ostao anoniman, napadač često unajmljuje posrednika za kupovinu koji umjesto samog napadača prima robu, a tu istu robu napadač tada prodaje po primamljivoj cijeni, a posrednik šalje na adresu kupca (Kossman, 2014). U slučaju legalnih problema sumnja pada na posrednika, tvrdi Kossman (2014).

Plaćanje usluga kreditnim karticama - Kossman (2014) navodi da, iako je to najrizičnija opcija, korištenje kreditnih kartica za direktnu kupovinu online ili u trgovinama je čest slučaj.

4 Biometrija lica

Biometriju se može definirati kao znanstvenu cjelinu koja se bavi prepoznavanjem i iskorištavanjem jedinstvenih karakteristika ljudskog tijela ili ljudskog ponašanja u svrhu jednoznačnoga određivanja ili potvrde identiteta. Do danas je poznato više od pedeset takvih karakteristika (Bača, 2015). Tehnike koje uspješno luče i koriste biometrijske karakteristike u shodne svrhe nazivamo biometrijskim tehnikama. Odlike su biometrijskih tehnika mogućnost mjerenja i usporedbe uzoraka neke biometrijske karakteristike te mogućnost automatizacije tog istog procesa (Bača, 2015; CARNet CERT i LS&S, 2006). Pojam biometrijske tehnike u većini slučajeva je vezan uz samu biometrijsku karakteristiku pa su ta dva pojma zapravo vrlo bliska. U ovom radu posebno će se razmotriti biometrijsku karakteristiku lica, pogotovo radi njene nenametljivosti prema korisniku.

4.1 Razlozi odabira lica kao biometrijske karakteristike

Glavna podjela biometrijskih karakteristika odnosi se na njihov izvor. Ako se radi o nekoj karakteristici ljudskog tijela, tada kažemo da se radi o fizičkoj karakteristici, a ako je pak u pitanju način ponašanja osobe, tada govorimo o ponašajnim karakteristikama (Bača, 2015). Uz karakteristike vežu se i određene atribute po kojima se može ocijeniti neku karakteristiku. Prema Bača (2015), to su:

1. *univerzalnost* - primjenjivost na sve osobe,
2. *jedinstvenost* - različitost karakteristike kod bilo kojih dviju osoba,
3. *stalnost* - promjenjivost karakteristike u vremenu,
4. *prikupljivost* - mogućnost uzimanja uzorka karakteristike i njegove evaluacije, i
5. *prihvatljivost* - privola korisnika.

U praksi, tj. sustavima sličnima ovome, često se koriste samo neke od svih dostupnih karakteristika. Tome je prvenstveno tako jer odlike svih karakteristika, prema gornjim atributima, nisu uravnotežene da bi se primjenjivale u svakodnevnoj interakciji s korisnicima. Prema tome, u ovom poglavlju razmotrit će se samo karakteristike koje po svojim odlikama mogu doći u obzir pri dizajnu ovakvog sustava. Dodatno, biometrijske karakteristike moraju ispunjavati uvjete:

- *biometrijski uzorak mora se moći uzeti prilikom vršenja transakcije,*

- *analiza usporedbe uzoraka mora biti gotova u razumnom vremenu, po mogućnosti trenutačno,*
- *uzimanje uzorka može biti beskontaktno ili kontaktno, no u slučaju kontaktnog, kontakt ne smije kod korisnika izazivati nelagodu,*
- *korištenje mora biti jednostavno za uporabu, i*
- *mogu se koristiti pri terminalima, online i mobilnim transakcijama*.

Odlike će se ocijeniti prema gornjim atributima te će se razložiti zašto je odabrana karakteristika lica za implementaciju ovoga sustava. Za svaku karakteristiku ocijeniti će se univerzalnost, jedinstvenost, stalnost, prikupljivost i prihvatljivost. Dodatno, osim atributa biometrijskih karakteristika, ocijeniti će se i izvedivost u praksi zato što je i to vrlo bitna stavka kod uvođenja ovakve tehnologije u neki sustav. Pod izvedivosti misli se na mogućnost uporabe na platnim terminalima, online i putem mobilnih uređaja. Ocjene su donesene na temelju sličnih razmatranjima u sljedećim izvorima: Bača (2015), Bača et al. (2006), Delac i Grgić (2004) i CARNet CERT i LS&S (2006). Prema tim kriterijima davat će se ocijene, počevši od najniže:

- niska (N) - karakteristika ne ispunjava zadani kriterij u potrebnoj mjeri,
- srednja (S) - karakteristika ispunjava zadani kriterij, ali ne u potpunosti, i
- visoka (V) - karakteristika u potpunosti ispunjava kriterij.

Pregled ocjena dan je u tablici 4.1.

Tablica 4.1: Ocijene kriterija za sve razmotrene karakteristike.

Kriterij	**Otisak prsta**	**Dlan**	**Vene**	**Lice**	**Šarenica**	**Potpis**
univerzalnost	S	V	S	V	V	N
jedinstvenost	V	S	S	N	V	N
stalnost	V	S	S	S	V	N
prikupljivost	S	V	S	V	S	V
pristupačnost	V	S	S	V	S	S
prihvatljivost	S	S	S	V	N	V

Razmatrajući ocijene koje su pridijeljene karakteristikama, vidi se da različite biometrijske karakteristike imaju različite prednosti i mane. U tablici se može primijetiti da lice ima visoku prihvatljivost, pristupačnost, prikupljivost i univerzalnost. Mane lica, kao biometrijske karakteristike, jesu jedinstvenost i stalnost.

Što se tiče jedinstvenosti, kako se u dizajnu modela koristimo licem isključivo za potvrdu identiteta, a ne raspoznavanjem osobe prema licu, tada velika jedinstvenost nije toliko značajna. U okviru poglavlja rezultata, detaljnije će se vidjeti koliko niska jedinstvenost utječe na performanse sustava.

U pogledu stalnosti, model nudi rješenje u visokoj ažurnosti uzoraka u bazi podataka, što je postignuto stalnim uvođenjem novih uzoraka tijekom vremena.

Razmotrimo još nekoliko kriterija:

- *jednostavnost korištenja* - za korištenje bi svakako bio jednostavniji sustav gdje korisnik ima što manju ulogu pa se ovdje kao logičan izbor nameće lice, kod kojeg se od korisnika ne potražuje nikakva dodatna interakcija, osim usmjeravanja pogleda prema senzoru,

- *upotrebljivost na svim uređajima* - iako sve više uređaja danas ima mogućnost uzimanja otiska prsta, a pogotovo se ovdje misli na računala i mobilne uređaje, ne može se u obzir ne uzeti činjenicu da gotovo svaki uređaj ima kameru,

- *odgovornost* - jedna od vrlo važnih činjenica pri incidentima s kartičnim prevarama jest odgovornost, naime, Murdoch et al. (2010) pojašnjavaju kako je uvođenjem EMV čipa u kartično poslovanje odgovornost za kartične incidente prebačena na korisnika jer banke EMV tehnologiju smatraju dovoljno sigurnom; dok bi se korištenjem lica moglo odrediti da li je osoba sama izvršila transakciju ili se uistinu radi o prijevari, i

- *mogućnost provjere živosti* - sprječava reprodukciju biometrijskog uzorka i varanja biometrijskog sustava provjerom živosti prezentirane slike lice, što je omogućeno karakterističnim kretnjama lica, poput pomicanja usana, facijalnih ekspresija, treptanja, itd.

Iz gore opisanih razloga za implementaciju je odabrana biometrijska karakteristika lica. Slika lica ujedno je karakteristika koja je ljudima najprirodniji način prepoznavanja osobe. Što se tiče računalnog prepoznavanja, stvari su nešto složenije. Kako bi lice moglo biti iskorišteno kao uzorak za prepoznavanje, potrebno je da lice bude u pravilnom položaju frontalno okrenuto prema senzoru. Također, uzorak lica osjetljiv je na osvjetljenje pa se i ono mora uzeti u obzir. Dobra strana korištenja lica kao biometrijske karakteristike je što ona nije nametljiva, tj. korisnički je prihvatljiva (Bača, 2015). U nastavku rada raspravljene su metode pomoću kojih se lice detektira i pomoću kojih se licem verificira korisnika.

4.2 Detekcija lica i živosti slike pomoću Viola-Jones algoritma

Da bi lice mogli koristiti u autentikaciji potrebno je poznavati njegove osobine, osobine njegove digitalne reprezentacije, metode koje se u tu svrhu koriste i, naposljetku, kakav rezultat se može očekivati. Intuitivno je jasno da prije nego što se neko lice može autenticirati, treba imati njegov uzorak, a da bi se dobio valjani uzorak, lice je prvo potrebno detektirati. Stoga, na slici 4.1 je dan opći tijek radnji koje treba zadovoljiti.

Slika 4.1: Proces autentikacije korisnika licem.

Objekt detekcije (engl. *detection*) [1] je ljudsko lice. Osnovni zadatak detekcije nekog objekta je odrediti postoji li taj objekt na danom uzorku pa je i pronalaženje lica istovjetno tome. Kako je u najvećem broju slučajeva dostupna samo dvodimenzionalna digitalna slika, tj. fotografija lica, na njenu će se obradu upravo i usmjeriti.

Prvi korak u prepoznavanju lica na fotografiji je njegovo pronalaženje, tj. detekcija, i normalizacija. Za ovaj zadatak razvijeni su mnoge metode, njih čak preko 150, navode Datta et al. (2016). Idealni sustav za detekciju lica bi za danu fotografiju morao moći pronaći sva prisutna lica bez obzira na veličinu, poziciju, orijentaciju, starost, ekspresiju i uvjete osvjetljenja (Li i Jain, 2011). Naravno, u praksi je takav sustav teško ostvariti. Jedan od principa na kojem se baziraju spomenute metode temelji se na izgledu lica (engl. *appearance-based methods*) te obliku lica ili glave Li i Jain (2011). Li i Jain (2011) ističu da su metode bazirane na ovom principu ujedno i metode čiji su algoritmi najuspješniji pa će se na njima u ovom radu i bazirati. Jedan od takvih algoritama je i algoritam autora Viole i Jonesa.

Viola i Jones (2001) svoj algoritam detekcije razvili su s ciljem omogućavanja detekcije objekata, a pogotovo lica, i to u stvarnom vremenu. Kako tvrde, iako se njihova metoda od ostalih razlikuje upravo po velikoj brzini detekcije, to ne umanjuje njegovu točnost naspram drugih metoda. Sam algoritam vrši detekciju putem ekstrakcije informacija sa sivotonskih (engl. *grayscale*) fotografija zato što sivotonski model sadrži manje podataka potrebnih za obradu od modela u boji, a opet čuva informacije važne za uspješnu detekciju.

Autori pojašnjavaju kako njihov algoritam u područje detekcije unosi tri novine, točnije rečeno, metoda detekcije sastoji se od tri komponente:

- izmijenjenoga *Adaboost* algoritma strojnog učenja,
- kaskadnih Haarovih klasifikatora (engl. *Haar Cascade Classifiers*), i
- metode brzog izračuna aritmetičke sredine skupine piksela zvane *integralna slika* (engl. *integral image*).

U nastavku rada izložen je princip rada Viola-Jones algoritma prema navedenim novitetima, a naposljetku je algoritam i implementiran u obliku samostalnog računalnog programa.

[1] Pojam detekcije treba razlikovati od pojma prepoznavanja (*engl. recognition*). Naime, prepoznavanje objekta je jednoznačno određivanje ekvivalencije promatranog i objekta iz nekog referentnog skupa, dok pojam detekcije označuje pripadnost objekta nekoj klasi objekata, tj. detekcija odgovara na pitanje spada li detektirani objekt u klasu objekata. Npr.,je li objekt na slici lice ili ne.

4.2.1 Integralna slika

Svaki algoritam detekcije nužno provodi operacije i analize nad materijom koja sadrži uzorak. Usporedno tome, algoritam detekcije lica na fotografiji nužno mora biti u interakciji s vrijednostima predstavljenim na fotografiji. Kako je već ranije spomenuto, najmanji gradivni element digitalne fotografije je piksel, a u vezi s pikselom vezana je i spomenuta funkcija čitanja vrijednosti piksela.

Budući da ovaj algoritam upotrebljava sivotonski model fotografije, podrazumijevat će se da bilo koji piksel slike može poprimiti vrijednost (0-255) $f(x, y) \in \langle 0, 255 \rangle, x = 0, \ldots n, y = 0, \ldots m$ gdje su n broj horizontalnih, a m vertikalnih stupaca piksela slike (Katsaggelos i Cummings, 2016).

U detekciji objekata na fotografiji učestalo se promatraju dijelovi fotografije koji predstavljaju određenu cjelinu, koja pomaže u, ili je objekt detekcije. Takve cjeline se u većini slučajeva razlikuju po boji. Kako bi detektirali razliku u boji jedne takve cjeline, naspram njene okoline, trebamo izračunati srednju vrijednost svih piksela u danoj cjelini, tj. trebamo izračunati aritmetičku sredinu. Kako se Viola-Jones algoritam detekcije u velikoj mjeri oslanja na traženje srednje vrijednosti skupine piksela, autori su morali polučiti metodu koja će u svega nekoliko operacija konstantne složenosti dati traženu vrijednost. Kao rezultat ove potrebe nastala je metoda integralne slike, tj. metoda izračuna kumulativne vrijednosti elemenata u matrici. Prednost ovoga algoritma je niska vremenska složenost $O(n)$, tj. za dani broj piksela n, operaciju čitanja i pribrajanja moramo provesti najviše n puta.

Postupak izračuna srednje vrijednosti za neko područje na slici kod metode integralne slike je sljedeći (Viola i Jones, 2001):

1. *izračunaj integralnu sliku prema izvornoj fotografiji,*
2. *provedi izračun sume željenog područja integralne slike po formuli, i*
3. *podijeli sumu brojem piksela u području.*

Metoda integralne slike zahtijeva da područje za koje izračunavamo srednju vrijednost bude u pravokutnom obliku zbog samog načina izračuna. Sada će se izračunati integralna sliku gornjeg prikaza zadanim algoritmom (Viola i Jones, 2001):

Algoritam 1: Izračun integralne slike

Podaci: digitalna fotografija u sivotonskom modelu D veličine $n \times m$ piksela

Rezultat: integralna slika I

inicijaliziraj matricu integralne slike I dimenzije $n \times m$;

za *svaki piksel D (x,y) od (0,0) do (n,m)* **čini**

- upiši u I u element $i_{x,y}$ vrijednost piksela $D(x,y)$;
- **ako** $D(x,y-1)$ *postoji* **onda**
  - uvećaj $i_{x,y}$ za $D(x,y-1)$;
- **ako** $D(x-1,y)$ *postoji* **onda**
  - uvećaj $i_{x,y}$ za $D(x-1,y)$;
- **ako** $D(x-1,y-1)$ *postoji* **onda**
  - uvećaj $i_{x,y}$ za $D(x-1,y-1)$;

Način izračuna integralne slike može se zapisati i formulom (Viola i Jones, 2001):

$$s(x,y) = i(x,y) + s(x,y-1) + s(x-1,y) - s(x-1,y-1), \tag{4.1}$$

gdje s predstavlja matricu[2] integralne slike, a i matricu piksela izvorne slike. Nakon što je pokazano kako izračunati integralnu sliku, sada će se pojasniti kako se zapravo može iskoristiti za dobivanje sume piksela željenog područja, tj. aritmetičke sredine piksela. Uzmimo za primjer sliku veličine 16 piksela i njenu integralnu inačicu (prikaz 4.2):

5	2	5	2
3	6	3	6
5	2	5	2
3	6	3	6

5	7	12	14
8	16	24	32
13	23	36	46
16	32	48	64

Slika 4.2: Slika sa danim vrijednostima piksela (lijevo) i dobivena integralna slika (desno).

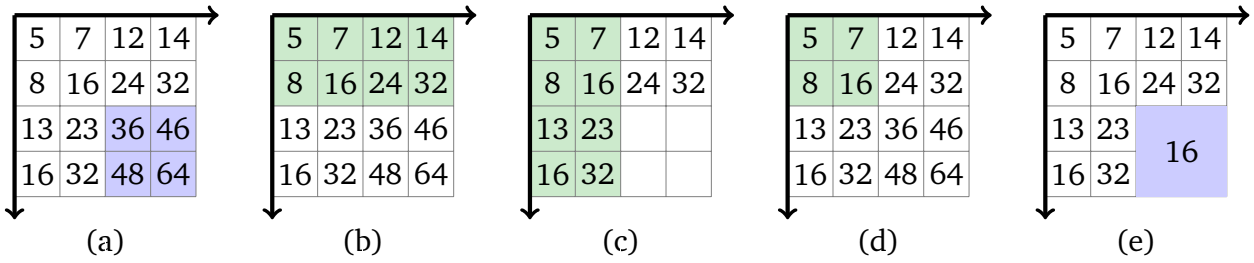
Primijetimo kako je svaka vrijednost ćelije u integralnoj slici zapravo suma svih pripadajućih piksela lijevo i iznad u izvornoj slici (uključujući i piksel za kojeg gledamo vrijednost u integralnoj tablici), tj. (Viola i

[2] Pojmom matrica zapravo korektnije nazivamo pojam integralne slike zbog toga što slika zapravo nije slika, već matrica istih dimenzija kao i matrica piksela izvorne slike.

Jones, 2001)

$$s(x,y) = \sum_{x' \leq x, y' \leq y} i(x', y'). \tag{4.2}$$

Upravo ta činjenica omogućava izračun sume nekog područja bez da se ponovno dohvaća vrijednosti piksela, npr. želi se izračunati područje obojeno u plavo (prikaz 4.3 (a)):



Slika 4.3: Ilustracija izračuna sume područja piksela integralnom slikom.

kako je suma svih piksela na slici jednaka 64 (što je vidljivo iz zadnje ćelije integralne slike), intuitivno je jasno da trebamo oduzeti okolna područja od sume cijele slike kako bi dobili sumu željenog područja. Prvo oduzimamo sumu područja iznad (4.3 (b)) pa potom područje lijevo (4.3 (c)). Treba primijetiti kako je dvaput oduzeto područje s vrijednošću 16 (4.3 (d)), a razlog je što ga oba navedena područja sadrže (4.3 (b) i (c)), iz tog će se razloga u izračunu pribrojiti vrijednost tog područja (4.3 (d)) pa se na kraju dobiva ukupna suma piksela zadanog područja (4.3 (e)):

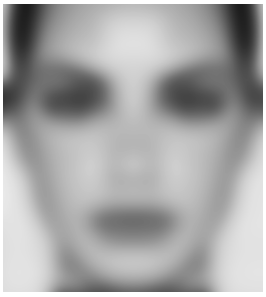
$$\sum(piksela) = (a) - (b) - (c) + (d) = 64 - 32 - 32 + 16 = 16$$

Posljednji je korak izračun aritmetičke sredine tako što će se podijeliti suma s brojem piksela unutar zadanog područja (u ovom slučaju sredina iznosi 4). Metoda integralne slike primjenjiva je na bilo koju sliku i na bilo koje područje te će ista u samo četiri operacije dohvaćanja (nakon što je izračunata integralnu sliku) dati traženi rezultat.

4.2.2 Kaskadni klasifikatori

U prethodnom poglavlju napomenuto je kako se kod detekcije objekata na slici u većini slučajeva promatraju skupine piksela (cjeline), radije nego pojedinačni pikseli. Ovo je primarno iz dva razloga; prvi je da takav algoritam radi puno brže, a drugi je da cjeline imaju veći značaj te ih se lakše stavlja u korelaciju, nego pojedinačni pikseli. Cjeline se, kako je već istaknuto, mogu diferencirati bojom, odnosno rubovima, a budući da algoritam detekcije radi primarno s fotografijama u sivotonskom modelu, može se reći da se radi o diferenciranju tamnijih ili svjetlijih područja na slici.

Ovdje dolazimo do pitanja na koja se područja na slici trebamo usredotočiti te na koji ih način evaluirati naspram područja okoline. Odgovor je da se kod različitih objekata traže različite cjeline (od sada će se za cjeline koristiti stručniji izraz - značajke, engl. *features*). Kako je objekt detekcije lice, usredotočit će se na značajke koje su njemu karakteristične. Uzme li se na čas primjer modifikacija slike lica 4.4, koja je pretvorena u sivotonski model sa zamućenjem, stvari postaju mnogo jasnije, naime na slici se mogu uočiti



Slika 4.4: Slika u sivotonskom modelu u filteru Gaussovo zamućenje

svjetlinom diferencirana područja te je već intuitivno jasno što se na slici treba uočiti kako bi se detektiralo lice. Ako se malo promisli o načinu na koji algoritam Viola-Jones detektira lica, može se već sada uočiti da će algoritam imati problema u detekciji objekata koji nisu tipičnog izgleda, npr. brada na licu, itd.

Preostalo je još proučiti kako zapravo algoritam pronalazi takva tipična područja i kako razlučuje pozitivne od negativnih detekcija. Termin koji se koristi za automatsko odlučivanje u području strojnog učenja[3] i računalnog vida[4] je klasifikator (engl. *classifier*).

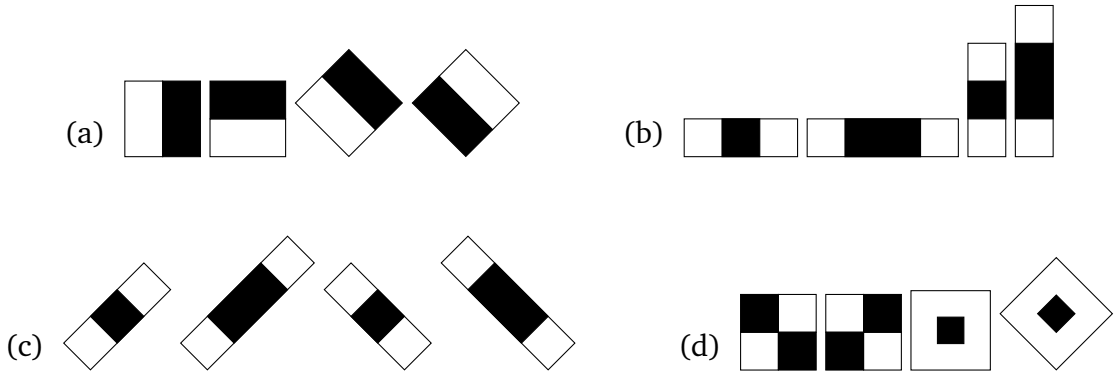
Algoritam Viola-Jonesa u tom smislu je zapravo jaki binarni klasifikator, gdje se atribut jaki odnosi na postotak točnosti klasifikacije, a atribut binarni odnosi na vrstu klasifikatora - binarni klasifikator je onaj koji odlučuje je li objekt detektiran ili nije. Kako bi dobili jaki klasifikator, autori su sekvencijalno spojili više slabih klasifikatora tj. klasifikatora čija je točnost nešto veća od nasumičnog odabira. Sekvenca takvih klasifikator zove se kaskada (engl. *cascade*). Pogledajmo sada kako se zapravo radi klasifikacija na temelju slabih klasifikatora. Svaki slabi klasifikator vezan je uz prepoznavanje određene značajke objekta. Kako je objekt lice, ono sadrži svoju specifičnu kaskadu (sekvencu) značajki[5]. Unaprijeđeni Viola-Jones algoritam za prepoznavanje lica u kaskadi poznaje sljedeće značajke i njihove kategorije (4.5):

Tamni dio svake značaje označuje tamnije područje na objektu detekcije, analogno tome, svjetliji dijelovi su u kontrastu s tamnim, npr. predio očiju svakako je tamniji od predjela čela itd. Ono što je

[3] Strojno je učenje grana računalne znanosti koje proučava i razvija algoritme po kojima računalo može automatski donijeti odluku - tzv. umjetna inteligencija

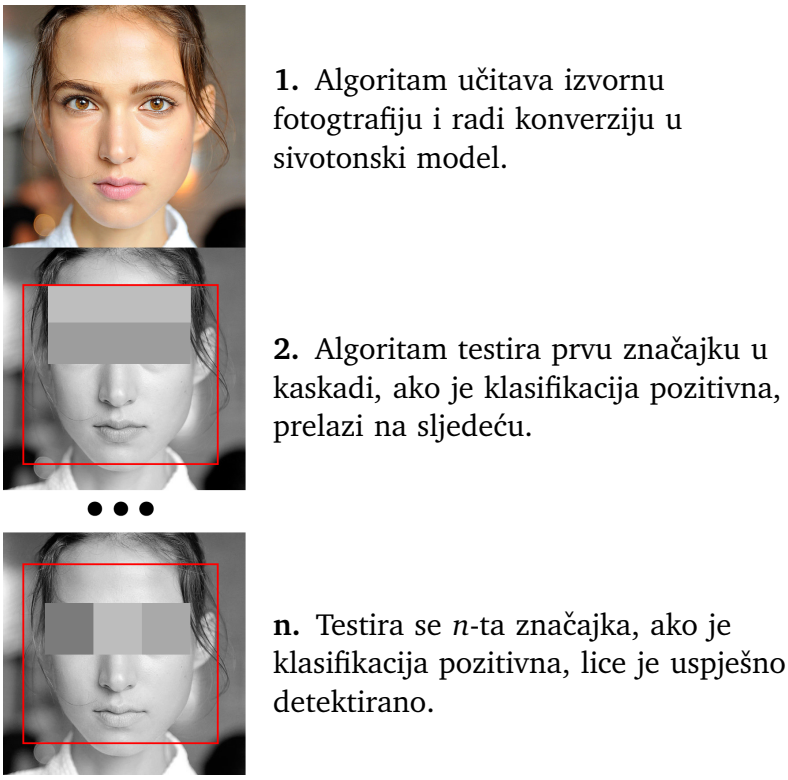
[4] Računalni je vid pojam koji se odnosi na računalnu obradu objekata u stvarnom svijetu, a koji su u digitalnom obliku reprezentirani kao slike, video sekvence itd.

[5] Odabir značajki radi se algoritmom strojnog učenja AdaBoost, o kojem će više riječi biti u sljedećem poglavlju.



Slika 4.5: Prošireni set Haarovih značajki: (a) rubne značajke, (b i c) linijske značajke i (d) dijagonalne i centrične značajke (Viola i Jones, 2001).

potrebno napomenuti je da značajke navedene u prikazu nisu vezane uz točno određeni dio lica, već ih algoritam učenja, opisan u sljedećem poglavlju, odabire i reda u kaskadu. Klasifikatori su u kaskadi poredani točno određenim redoslijedom kako bi se na lažnoj detekciji izgubilo što manje vremena, tj. da bi se već u najranijem dijelu analize područja taj dio slike odbacio kao negativan. Prve značajke u kaskadi stoga imaju postotak pogreške od 10-30%, dok one kasnije imaju 40-50%, navode Viola i Jones (2001).



Slika 4.6: Pojednostavljeni prikaz detekcije

Kao što se može uočiti na slici 4.6, sve značajke u kaskadi moraju biti uspješno detektirane kako bi konačan ishod detekcije bio pozitivan. Način na koji se značajka detektira je sljedeći. U početku, algoritam

inicijalizira potprozor (engl. *subwindow*) detekcije veličine 24x24 px (potprozor je ilustriran crvenim okvirom na slici 4.6) na poziciji (0,0). U potprozoru započinje testiranje (detekcija) kaskadom značajki tako što algoritam postavlja prvu značajku pod točno određenim parametrima: veličina značajke, rotacija značajke i pozicija značajke (ovo je zbog toga što algoritam ide od pretpostavke da se u navedenom potprozoru nalazi lice, a ako uistinu i je tako, značajka će biti detektirana). Na dijelu značajke koji je označen kao tamniji računa se suma piksela izvorne slike u sivotonskom modelu (suma piksela se naravno računa putem integralne slike). Na dijelu značajke koji je označen kao svjetliji, također se računa suma piksela kao i u koraku prije, a dobivene sume se oduzima. Bude li rezultat unutar zadanog raspona (engl. *threshold*) značajka je detektirana. Bivanje unutar zadanog raspona označuje da je "ispod" tamnijeg dijela značajke uistinu tamniji dio slike, a isto vrijedi i za svjetliji dio. Spomenuti dozvoljeni raspon također je određen algoritmom učenja.

Ako je prethodna značajka detektirana, algoritam učitava novu značajku u kaskadi te se ponavljaju prethodni koraci. Isto je za sve pozitivno detektirane značajke, a bude li i zadnja značajka detektirana, lokacija i područje potprozora se bilježi kao detektirano lice. Ako značajka nije detektirana potprozor detekcije pomiče desno (ili dolje) tj. na novu lokaciju tako prolazivši cijelu fotografiju.

Nakon što je detektor prošao cijelu fotografiju veličinom potprozora detekcije 24x24px, veličina tog prozora uvećava se za 1.25 puta (a time se uvećavaju i značajke) te se ponovno radi detekcija na cijeloj slici. Veličina se prozora uvećava sve dok ona ne dosegne veličinu fotografije. Formalnije pojašnjenje rada dano je u opisu algoritma 2.

Algoritam 2: Algoritam detektiranja značajki (Viola i Jones, 2001)

Podaci: digitalna fotografija D veličine $n \times m$ piksela, kaskada značajki Z

Rezultat: kvadrati koji omeđuju detektirane značajke K

inicijaliziraj potprozor detekcije P veličine 24×24 px na lokaciji $D(0,0)$;

i, j := 0;

dok $P <= n \times m$ **čini**

  ponavljaj

    za *svaku značajku z iz kaskade Z* **čini**

      postavi značajku unutar potprozora detekcije;

      SS := suma piksela pod svijetlim dijelom značajke z;

      ST := suma piksela pod tamnim dijelom značajke z;

      ako *je* $ST - SS$ *u dozvoljenom intervalu* **onda**

        $K(ij) := P$;

      inače

        odbaci potprozor kao nedektiran;

    pomakni prozor detekcije na sljedeću lokaciju;

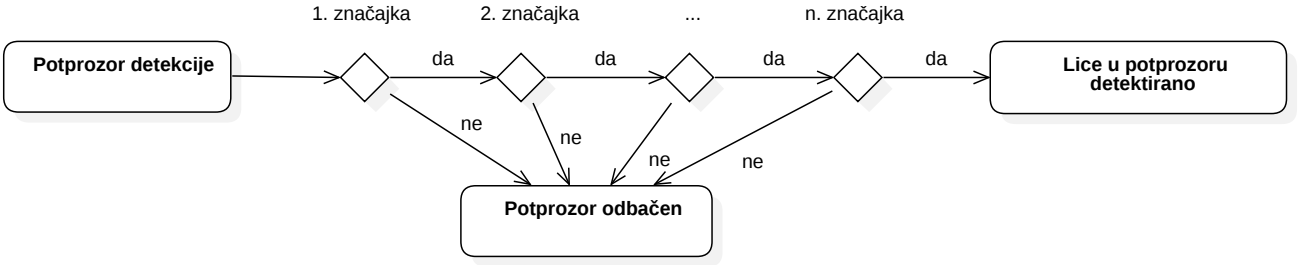
    j++;

  dok ne bude P *je na poziciji* (n, m);

  $P := P \times 1.25$;

  i++;

Najveći doprinos ove metode je brzina detekcije, naime, evaluacija jedne značajke oduzima oko 60 mikroprocesorskih instrukcija. Metodu se može prikazati i degeneriranim binarnim stablom odluke 4.7:



Slika 4.7: Kaskada binarnih klasifikatora

4.2.3 AdaBoost

U prethodnom poglavlju je objašnjena srž rada algoritma detekcije, no još je preostalo za pojasniti način na koji se odabiru pojedine značajke i kako se one slažu u kaskadu. Krečući od činjenice da se u jednom inicijalnom prozoru dimenzija 24x24 px može definirati preko 160,000 kombinacija različitih značajki različitih veličina i pozicija, što je za detektor vrlo velik i nepotreban broj, prvenstveno zbog brzine rada, a i zbog činjenice da toliki broj značajki ne bi imao previše doprinosa na postotak detekcije. Pogledajmo sliku 4.8, na slici je jasno vidljivo da je uistinu moguće uočiti veliki broj značajki na kompleksnom objektu

Slika 4.8: Prikaz nekolicine mogućih značajki.

detekcije kao što je lice. Kako bi odabrali koje značajke su uistinu najpotrebnije za uspješan postotak detekcije, autori su iskoristili već postojeći algoritam strojnog učenja po imenu AdaBoost, što je složenica od izraza "*adaptive boosting*". Izraz boosting se odnosi metodu kreiranja klasifikatora. Naime, kako je već spomenuto, klasifikator detekcije lica sastavljen je od slabih klasifikatora koji sami po sebi ne mogu sa sigurnošću ustvrditi radi li se o licu ili ne pa upravo zato takve slabe klasifikatore[6] kombinira se i spaja u jedan jaki klasifikator - navedena metoda strojnog učenja naziva se "*boosting*". Pojednostavljeni princip odabira značajki koje tvore klasifikator je sljedeći; algoritmu učenja AdaBoost, dan je skup slika na kojima postoji željeni oblik detekcije, te skup slika na kojima ne postoji objekat (lice) [7]. AdaBoost zatim prolazi kroz sve navedene slike i isprobava sve moguće značajke. One značajke koje se pokažu kao najbolji klasifikatori te u kombinaciji s drugim klasifikatorima daju najtočniju detekciju, ulaze u konačnu kaskadu. Također, oni klasifikatori koji se pokažu najmanje uspješnima, također mogu ući u kaskadu, no vrijednost njihove odluke je invertirana. Formalno, prema Viola i Jones (2001), algoritam opisujemo:

[6] Matematički korektna definicija slabog klasifikatora u kontekstu Viola-Jones algoritma je sljedeća:

$$h_j(x) = \begin{cases} 1, & \text{ako je } p_j f_j < p_j \theta_j \\ 0, & \text{inače} \end{cases} \tag{4.3}$$

gdje je x potprozor detekcije, f značajka, p polaritet koji određuje oduzima li se suma piksela tamnijeg dijela od svjetlijeg ili obrnuto, i θ - raspon dozvoljenih vrijednosti (engl. *threshold*).

[7] Oblik učenja u kojem su algoritmu već poznati negativni i pozitivni uzorci naziva se nadzirano učenje (engl. *supervised*)

1. uzmimo da su fotografije za treniranje klasifikatora pomoću AdaBoost algoritma označene s $(x_1, y_1), \ldots, (x_n, y_n)$, gdje je $y_i = \{0, 1\}$, već prema tome je li na fotografiji objekt detekcije ili nije,

2. inicijaliziramo težinske koeficijente $w_{1,i} = \frac{1}{2m}, \frac{1}{2l}$ za $y_i = \{0, 1\}$ respektivno, gdje su m i l broj negativnih, odnosno pozitivnih fotografija,

3. za $t = 1, \ldots, T$:

   (a) normaliziraj težinske vrijednosti $w_{t,i} := \frac{w_{t,i}}{\sum_{j=1}^{n} w_{t,j}}$ tako da w_t čini distribuciju vjerojatnosti,

   (b) za svaku značajku j treniraj klasifikator h_j koji je ograničen na samo tu značajku, dok stopu pogrešnosti računaj prema formuli $w_t, \epsilon_j = \sum_i w_i |h_j(x_i) - y_i|$,

   (c) odaberi klasifikator h_t, koji ima najnižu stopu pogrešnosti ϵ_t,

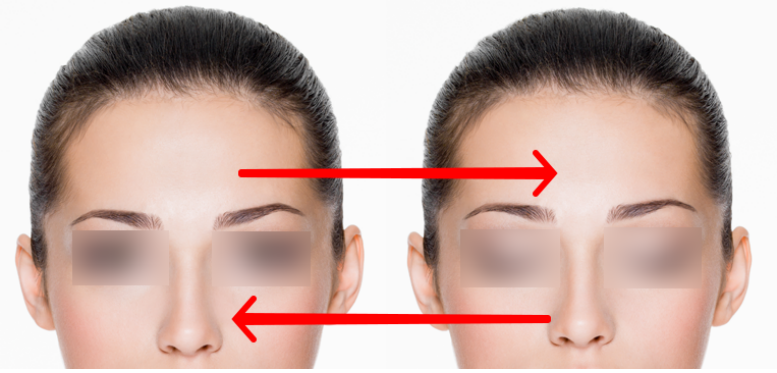
   (d) ažuriraj težinske koeficijente tako da je $w_{t+1,i} = w_{t,i} \beta_t^{1-e_i}$, gdje je $e_i = 0$, ako je x_i točno klasificiran, odnosno $e_i = 1$ ako to nije slučaj, također, $\beta_t = \frac{\epsilon_t}{1-\epsilon_t}$.

4. Konačno, jaki klasifikator dobiva se u obliku $h(x) = \begin{cases} 1, & \sum_{t=1}^{T} \alpha_t h_t(x) \geq \frac{1}{2} \sum_{t=1}^{T} \alpha_t \\ 0, & \text{inače} \end{cases}$,

   gdje je $\alpha_t = log \frac{1}{\beta_t}$

4.2.4 Detekcija živosti prema treptaju očiju

Na isti način na koji se detektiralo lice na fotografiji, može se detektirati i područje očiju pa će se stoga ovaj algoritam iskoristiti i za provjeru živosti slike. Provjera će se sastojati od toga da se u vremenskom intervalu s video sekvence uzimaju uzorci očiju korisnika sve dok se ne dogodi treptaj. Ako se treptaj ne dogodi u uobičajenom vremenu, sustav može pretpostaviti da mu je prezentirana statička slika te da ga se pokušava prevariti. Ako osoba ima veći interval treptanja nego li je to uobičajeno, sustav može intervenirati i naložiti korisniku da namjerno trepne kako bi potvrdio da se ne radi o lažnom uzorku.



Slika 4.9: Ilustracija treptaja i razlike u srednjoj vrijednosti svjetline kod otvorenih (lijevo) i zatvorenih (desno) očiju.

Kako se treptaj spontano događa svakih 3-6 sekundi (Fitzakerley, 2015), sustav bi trebao u razumnom vremenu, tj. za vrijeme vršenje transakcije, moći pretpostaviti da li se radi o stvarnoj osobi.

4.3 Verifikacija lica histogramima lokalnih binarnih uzoraka

Nakon što je pokazano na koji će se način detektirati i pribaviti uzorak lica, u sljedećem koraku mora se razmotriti kako će se putem tog uzorka korisnika verificirati, tj. autenticirati. Kao i metoda za detekciju, i ovih metoda postoji u velikom broju, a također ih se može, prema prijedlogu Datta et al. (2016), podijeliti u sljedeće skupine:

- metode bazirane na izgledu lica,
- metode potprostora (engl. *subspace-based*),
- metode bazirane na neuronskim mrežama,
- metode bazirane na 3D modelu lica,
- ostale metode zasnovane na korelaciji.

Kako je ranije spomenuto, metode koje se baziraju na izgledu lica imaju široku primjenu, kako u detekciji, tako i u prepoznavanju. Srž metode je, prema Datta et al. (2016) geometrijski opis karakteristika lica i njihov suodnosi koji su potom zapisani u vektor značajki, koji se pak koristi u određivanju udaljenosti dvaju uzoraka.

Neke od poznatijih metoda potprostora jesu PCA (engl. *Principal Component Analysis*), LDA (engl. Linear Discriminant Analysis), *Fisherfaces*, itd. Navedene metode baziraju se na smanjenju dimenzionalnosti

originalnog uzorka, čime se ističu samo jake karakteristike, i stvaranju opisa cjelokupnog lica putem više takvih uzoraka (Datta et al., 2016).

Neuronske mreže pojam su koji se veže uz umjetnu inteligenciju, naime, neuronska mreža simulira proces donošenja odluka kod živčanog sustava čovjeka, tj. početno se prima nekakav podražaj te se nizom odluka i grananja, koje su općenito nepoznate vanjskom opažaču, dolazi do finalne odluke, tj. akcije. Na sličan način funkcioniraju i metode za prepoznavanje temeljene na neuronskim mrežama. Naime, prije nego što se tehnika neuronske mreže može koristiti u prepoznavanju uzorka, potrebno je pripremiti set podataka za treniranje. Ovdje se govori o tzv. nadziranom treniranju, gdje se algoritmu daje neki ulazni podatak i podatak o rezultatu koji se očekuje, a sam algoritam stvara logiku o tome kako će doći do tog rezultata. Tako se u ovom slučaju algoritmu daju uzorci lica i podatak kome taj uzorak pripada (Datta et al., 2016).

Slično kao i kod metoda baziranih na izgledu lica, metode korelacije zasnivaju se na jedinstvenom odnosu značajki lica, poput očiju, usta, nosa , obrvi, itd. Stoga, da bi se ova metoda mogla koristiti potrebno je naći što veći broj karakterističnih točaka koje se mogu staviti u korelaciju (Datta et al., 2016).

Za implementaciju sustava autentikacije odabrana je tehnika prepoznavanja putem usporedbe histograma lokalnih binarnih uzoraka (engl. *Local Binary Patterns Histograms*), u daljnjem tekstu *LBPH*. Glavna razlika između spomenutih metoda i LBPH je u pristupu opisa lica. Dok nabrojane tehnike lice gledaju holističkim pristupom, tj. gledaju lice kao cjelinu, LBPH segmentira lice u interesna područja, već prema tome koji dio lica je pogodniji za prepoznavanje, pojašnjavaju Ahonen et al. (2006). Prednosti ove metode nad ostalima su parcijalna invarijantnost na osvjetljenje, rotaciju i okluziju te brzina prepoznavanja uzorka (Ahonen et al., 2006). U nastavku će se izložiti rad LBPH tehnike i njene primjene u prepoznavanju lica kroz tri faze:

1. ekstrakcija lokalnih binarnih uzoraka,
2. kreiranje histograma i evaluacija uzoraka, i
3. usporedba uzoraka histogramima.

4.3.1 Ekstrakcija lokalnih binarnih uzoraka

Metodu su za raspoznavanje lica prvi puta upotrijebili Ahonen et al. u radu objavljenom 2004. godine. Kao i ostale metode, LBP se bazira na smanjenju šuma i dimenzionalnosti digitalne fotografije, kako bi se dobile jasno izražene karakteristične značajke neke teksture, u ovom slučaju lica. Li i Jain (2011) objašnjavaju kako se radi o operatoru, odnosno deskriptoru teksture lokalnog dometa. U svom osnovnom obliku, LBP

operator redoslijedno uzima područje fotografije od 3×3 piksela te računa vrijednost centralnog piksela prema njegovom odnosu sa susjednim pikselima. Izračun se radi prema algoritmu 3.

Algoritam 3: Algoritam izračuna lokalnih binarnih uzoraka Ahonen et al. (2006)

Podaci: digitalna fotografija D veličine $n \times m$ piksela

Rezultat: matrica M lokalnih binarnih uzoraka

inicijaliziraj matricu M dimenzije $n \times m$;

za *svaki piksel* $D(x, y)$ *od* $(0, 0)$ *do* (n, m) **čini**

  ako *je* $D(x, y)$ *rubni piksel* **onda**

    u element $m_{x,y}$ matrice M upiši 0;

  inače

    inicijaliziraj polje P veličine 8 bitova;

    za *svaki susjedni piksel* $D('x,'y)$ *piksela* $D(x, y)$ **čini**

      ako *je vrijednost* $D(x, y) > D('x,'y)$ **onda**

        u polje P dodaj 0;

      inače

        u polje P dodaj 1;

    u element $m_{x,y}$ matrice M upiši vrijednost P u dekadskom obliku;

Formalno, prema Lopez (2010), algoritam se opisuje kao:

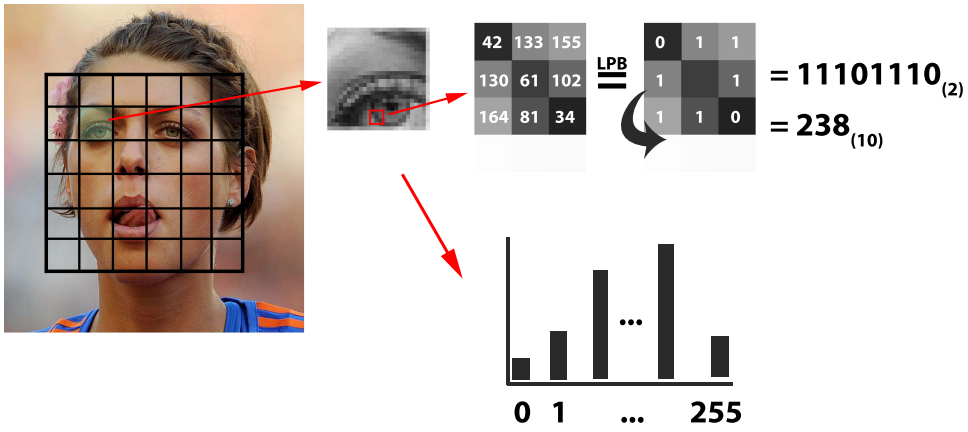
$$LBP(x_c, y_c) = \sum_{n=0}^{7} s(l_n - l_c)2^n, \tag{4.4}$$

gdje je l_c vrijednost centralnog piksela, a l_n vrijednost susjednog piksela. Funkciju $s(k)$ definira se kao:

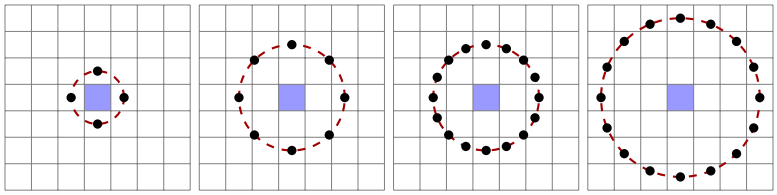
$$s(k) = \begin{cases} 1, & ako\ je \quad k \geq 0 \\ 0, & ako\ je \quad k < 0 \end{cases} \tag{4.5}$$

Opisani postupak ilustriran je na slici 4.10.

Osim osnovnog oblika LBP-a (3×3), Ahonen et al. (2006) navode da se u metodi koriste i kružni LBP koji definira broj piksela koji se koriste u susjedstvu te različite udaljenosti centralnog piksela od njegovog susjedstva (P, R) - gdje P predstavlja broj piksela susjedstva, a R udaljenost od centralnog piksela u pikselima. Ovo proširenje osnovnog LBP-a omogućuje da se analiziraju teksture čiji se uzorci mogu jasnije razaznati ako se koristi veći radijus, odnosno broj okolnih piksela.



Slika 4.10: Ekstrakcija LBP i kreiranje LBPH.



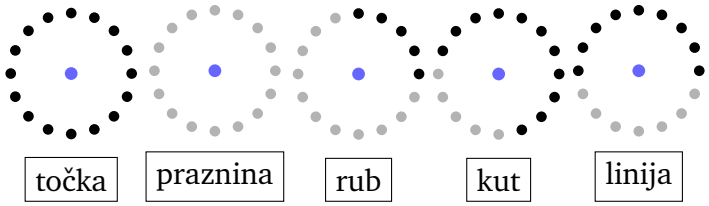
Slika 4.11: Različiti LBP operatori, već prema $(P,R) = (1,4),(2,8),(2,16),(3,16)$, respektivno. Napravljeno prema prikazu iz (Ahonen et al., 2006). Na 2. i 3. grafu vidi se da se točke poklapaju s granicom između 4 susjedna piksela. U tom slučaju se za vrijednost točke uzima vrijednost bilinearne interpolacije susjednih piksela(Li i Jain, 2011).

Osim proširenja kružnim LBP, Ahonen et al. (2006) spominju i pojam ujednačenog LBP-a (engl. *uniform LBP*). Naime, radi se smanjenju dimenzije konačnog deskriptora slike bez gubitka za raspoznavanje važnih informacija. Dimenzija deskriptora smanjuje se smještanjem neujednačenih LBP uzoraka u jednu kategoriju, a sve ostale u svoje zasebne kategorije. Kako se LBP uzorak prevodi u 8-bitnu riječ, mogućih vrijednosti ima $2^8 = 256$, tj. od $0000\,0000_{(2)}$ do $1111\,1111_{(2)}$, ili u dekadskom zapisu 0 - 255.

Ujednačeni uzorak je onaj kod kojeg postoje maksimalno dvije tranzicije bitova: iz 1 u 0 i obrnuto. Na primjer, $1110\,0000_{(2)}$ ima jednu tranziciju - iz 1 u 0, slično, $1110\,0011_{(2)}$ ima dvije tranzicije - iz 1 u 0 te opet iz 0 u 1. Navedeni LBP uzorci su ujednačeni uzorci. Primjeri neujednačenih uzoraka su: $1110\,0101_{(2)}$, $1001\,1001_{(2)}$, itd. Logički se naravno postavlja pitanje zašto bi reducirali broj mogućih uzoraka na skupinu od 58[8] ujednačenih? Naime, ujednačeni uzorci daju puno jasniji opis teksture za razliku od neujednačenih, koji uglavnom unose smetnje (Valstar, 2015). Pogledajmo na slici 4.12 neke od ujednačenih uzoraka i njihovo značenje.

Stoga, ujednačenim LBP uzorcima zapravo se želi bolje istaknuti rubne značajke i konture - što je zapravo i potrebno za uspješno prepoznavanje. Kako se vidi na slici 4.13, (prvi red),

[8] Broj mogućih ujednačenih LBP-a iznosi 58 jer je upravo toliko kombinacija ujednačenih uzoraka unutar svih 256 kombinacija.



Slika 4.12: Nekolicina ujednačenih LBP uzoraka i opis onoga što oni predstavljaju. Napravljeno prema prikazu iz (Li i Jain, 2011).

uklanjanje neujednačenih uzoraka (desno) eliminira dosta šuma prisutnog u deskriptoru s ujednačenim i neujednačenim LBP uzorcima. Također, može se primjetiti kako iluminacija (ako je ujednačena) ne ugrožava stvaranje valjanog deskriptora (drugi red). U trećem redu može se vidjeti deskriptore koji su nastali korištenjem kružnog LBP operatora radijusa $R = 5$ i 8 točaka $(5, 8)$.

Slika 4.13: LBP slike dobivene ekstrakcijom LBP uzoraka. Originalna slika (lijevo), LBP deskriptor (sredina), LBP deskriptor ujednačenih uzoraka(desno). Prvi red - normalni LBP deskriptor, drugi red - smanjena iluminacija, treći red - LBP deskriptor s povećanim radijusom.

4.3.2 Kreiranje histograma i evaluacija uzoraka

Sada kada se zna kako se fotografija može izraziti kao LBP deskriptor, postavlja se pitanje kako takav format prikazati na numerički, tj. za usporedbu povoljan, način. Ahonen et al. (2006) u svojem radu pojašnjavaju da za usporedbu uzoraka potrebno kreirati histogram, tj. vektor, koji će u sebi imati spremljene vrijednosti

LBP uzoraka, njihovu lokaciju na slici te važnost uzorka za prepoznavanje lica[9]. Kako usporedba uzoraka na razini piksela općenito nije dobar način usporedbe, autori predlažu da se deskriptor podijeli na m dijelova, po mogućnosti $m = 7 \times 7 = 49$, i da se za svaki dio izračuna histogram, tj. vektor koji će pohraniti vrijednost uzorka i njegove učestalosti u tom dijelu.

Formalno, prema Li i Jain (2011), histogram svakog dijela definira se kao:

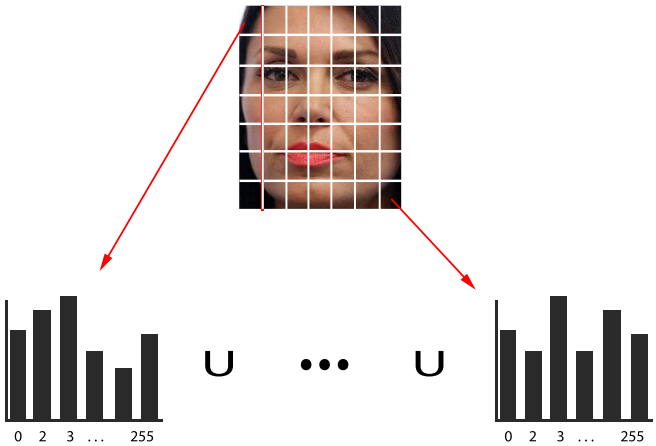
$$H_i = \sum_{x,y} I\{f_l(x,y) = i\}, \quad i = 0, \ldots, n-1, \tag{4.6}$$

gdje je n broj tipova uzoraka, $f_l(x,y)$ LBP deskriptor slike te:

$$I\{A\} = \begin{cases} 1, & ako\ je \quad A = 1 \\ 0, & ako\ je \quad A = 0. \end{cases} \tag{4.7}$$

Nakon što je izračunat histogram za svaki od m dijelova, isti se konkateniraju[10] te tvore histogram, ili vektor, koji konačno numerički opisuje sliku lica, kako je prikazano na slici 4.14. Formalno, prema Lopez (2010), konkatenaciju se opisuje sa:

$$H_{i,j} = \sum_{x,y} I\{f_l(x,y) = i\} I\{(x,y) \in R_j\}, \quad i = 0, \ldots, n-1, \quad j = 0, \ldots, m-1 \tag{4.8}$$



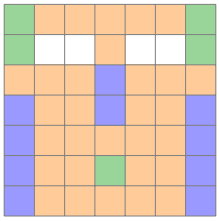
Slika 4.14: Izračun i konkatenacija histograma po dijelovima.

Dimenzija konačnog vektora, za predložene vrijednosti, iznosi $7 \times 7 \times 59 = 2891$ (Valstar, 2015). Primijetimo, svaki od histograma nosi informaciju o lokaciji, već prema tome na kojoj je poziciji u konačnom

[9] Kako je ranije spomenuto, svi dijelovi lica nemaju jednaku mogućnost determiniranja osobe. Npr. oči i usta bolje opisuju lice nego što to čini čelo ili obrazi, itd.

[10] Pojmom konkateniranje označava se spajanje, što je u ovom primjeru suprotno od zbrajanja.

histogramu, tj. vektoru (Ahonen et al., 2006). Također, lokacija sa sobom nosi i informaciju o tome kolika je njezina važnost u prepoznavanju uzorka (prikaz 4.15).



Slika 4.15: (Ahonen et al., 2006) predlažu sljedeću raspodjelu važnosti područja za prepoznavanje: područje očiju i obrva (bijela) je najvažnije (4.0), nakon njega slijedi područje usta i krajevi čela (zelena) (2.0), onda ostatak lica (narančasta) (1.0), i na kraju nos i krajevi čeljusti (plava) (0.0).

4.3.3 Usporedba uzoraka histogramima

Konačno, nakon što se dobilo vektore uzoraka te se znaju težinske vrijednosti dijelova deskriptora, može se krenuti u usporedbu istih te donijeti konačnu odluku o tome da li se uzorci poklapaju ili ne. Za usporedbu histograma uzoraka Ahonen et al. (2006) predlažu Hi-kvadrat test[11] (χ^2 test) dan formulom:

$$\chi_w^2(U,V) = \sum_{j,i} w_j \frac{(U_{i,j} - V_{i,j})^2}{U_{i,j} - V_{i,j}}, \tag{4.9}$$

gdje su U i V dva uzorka dana u obliku konačnog histograma, i - i-ta komponenta histograma u j-toj lokaciji te w_j - težinski koeficijent područja j (prema 4.15). Konačni rezultat - $\chi_w^2(U,V)$, kazuje nam koliko su dva uzorka slična, točnije udaljena. Ovisno o dobivenom rezultatu sustav će odlučiti da li je sličnost dovoljna da bi se korisnik autenticirao.

[11] Hi-kvadrat test (engl. *Chi square*) ukazuje na postojanje ili nepostojanje obilježja koje bi odbacilo nultu hipotezu (Tekstilno-tehnološki fakultet, 2008). Nulta hipoteza je u ovom slučaju ta da oba uzorka pripadaju istoj osobi.

5 Model nenametljive provjere korisnika

U prethodnom poglavlju ukazani su problemi sigurnosti koji se pojavljuju prilikom vršenja transakcija. Sigurnosni rizik[a] koji slijedi iz takvih propusta je krađa i neovlašteni pristup platnim sredstvima i informacijama o platnim sredstvima te u konačnici njihova uporaba u svrhu nelegalnoga stjecanja financijske dobiti, ili direktno putem nekog od sučelja, ili daljnjom preprodajom na ilegalnim tržnicama.

U ovom poglavlju bit će raspravljen koncept modela koji smanjuje sigurnosni rizik korištenja platnih sredstava uvođenjem dodatne provjere biometrijskih značajki lica korisnika, a da pritom ne zadire u privatnost korisnika, niti nameće kakve dodatne zahtjeve prema korisniku, tj. naglasak kod koncepta i implementacije ovakvog sustava bit će na neintruzivnosti. Osim neintruzivnosti, posebna pažnja bit će usmjerena i na mogućnost korištenja na mobilnim uređajima i računalima. Naime, u prethodnom poglavlju spomenuto je kako je uvođenjem EMV čipa pala stopa kartičnih prevara na POS uređajima i bankomatima kao rezultat verifikacije kreditne kartice, a u isto vrijeme je porasla stopa prevara online. Cilj ovoga sustava je spriječiti i pojavu alternativnih metoda kartičnih prevara uvođenjem i provjere identiteta korisnika, koja do sada nije bila implementirana u zadovoljavajućoj mjeri.

[a] Sigurnosni rizik može se definirati kao mogućnost realizacije neželjenog događaja (CARNet CERT i LS&S, 2003).

5.1 Opis modela

Korisnika se u sustav uvodi registracijom kod ustanove koja izdaje platno sredstvo (kreditne kartice, bankovni računi, online servisi, itd.). Prilikom registracije korisnik daje svoje osobne podatke kao i valjani biometrijski uzorak[1]. Uzorak se potom, kao i ostali podaci, uvodi u bazu podataka te se korisniku izdaju identifikacijski podaci u obliku korisničkog imena, broja računa, kreditne kartice, PIN-a, itd. ili ih korisnik sam odabire ovisno o usluzi koja mu se daje. Na koncu, izdavanjem korisničkih podataka usluga postaje aktivna.

Nakon registracije korisniku treba aktivirati uslugu mobilnog tokena[2] koja služi u svrhu autorizacije transakcije u slučaju da biometrijski sustav odbije transakciju valjanoga korisnika ili da korisnika obavijesti

[1] Valjanim biometrijskim uzorkom smatra se uzorak koji omogućuje detekciju karakterističnih značajki koje moraju biti istaknute kako bi se mogla vršiti usporedba s drugim uzorcima i verifikacija s ponovljenim uzorkom pri autentikaciji.

[2] Mobilni token je aplikacija davatelja usluge bankarstva ili sl., kojom se mobilnim uređajima omogućuje autorizacije i potvrda transakcije.

o pokušaju neovlaštenog korištenja platnog sredstva.

Korisnik potom stupa u interakciju sa sustavom unoseći svoje identifikacijske i autentifikacijske podatke. Paralelno s korisničkim unosom podataka podsustav za detekciju uzorka traži, detektira te potom uzima jedan ili više uzoraka koji se po korisničkom unosu podataka šalju zajedno s istima podsustavu za autentikaciju korisnika. Ako su korisnički podaci koje je unio korisnik valjani, a biometrijski uzorak odgovara uzorku kojeg je korisnik dao prilikom registracije, sustav dopušta transakciju te se korisnika putem sučelja obavještava da je transakcija uspješno obavljena. Ilustracija sustava u uporabi dana je na slici 5.1.

Slika 5.1: Ilustracija korištenja biometrijskog sustava.

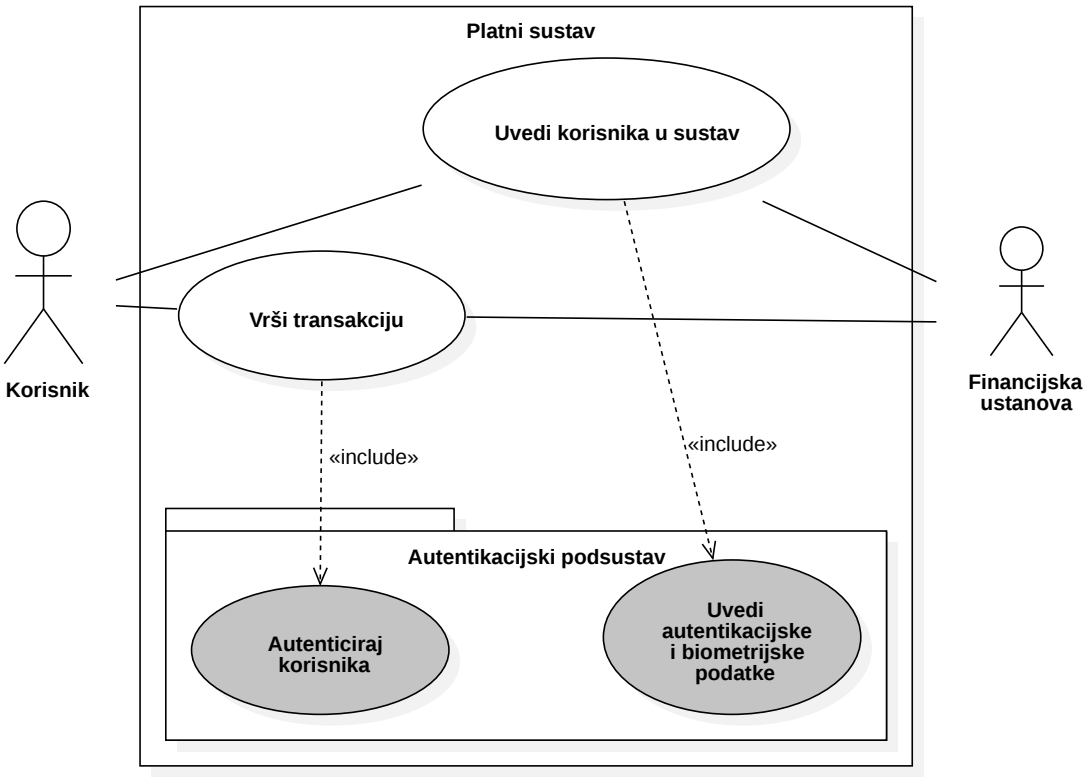
U slučaju da je korisnik unio valjane podatke, no biometrijski uzorak nije uspješno uspoređen, sustav, ovisno o razini politike sigurnosti, visini iznosa transakcije i postotku podudarnosti uzoraka, može trenutno dopustiti transakciju i putem mobilne mreže obavijestiti korisnika kako je njegov račun korišten, ili od korisnika, također, putem mobilnog uređaja u službi sigurnosnog tokena, tražiti verifikaciju transakcije. U slučaju korištenja mobilnog uređaja za verifikaciju korisnik može odobriti ili zabraniti transakciju te tako spriječiti moguću zloupotrebu platnog sredstva.

Mobilni uređaj može imati funkciju uzimanja uzorka ako se transakcija vrši putem mobilnog bankarstva, interneta ili ako platni terminal nije osposobljen za uzimanje uzoraka.

5.2 Općenita arhitektura modela

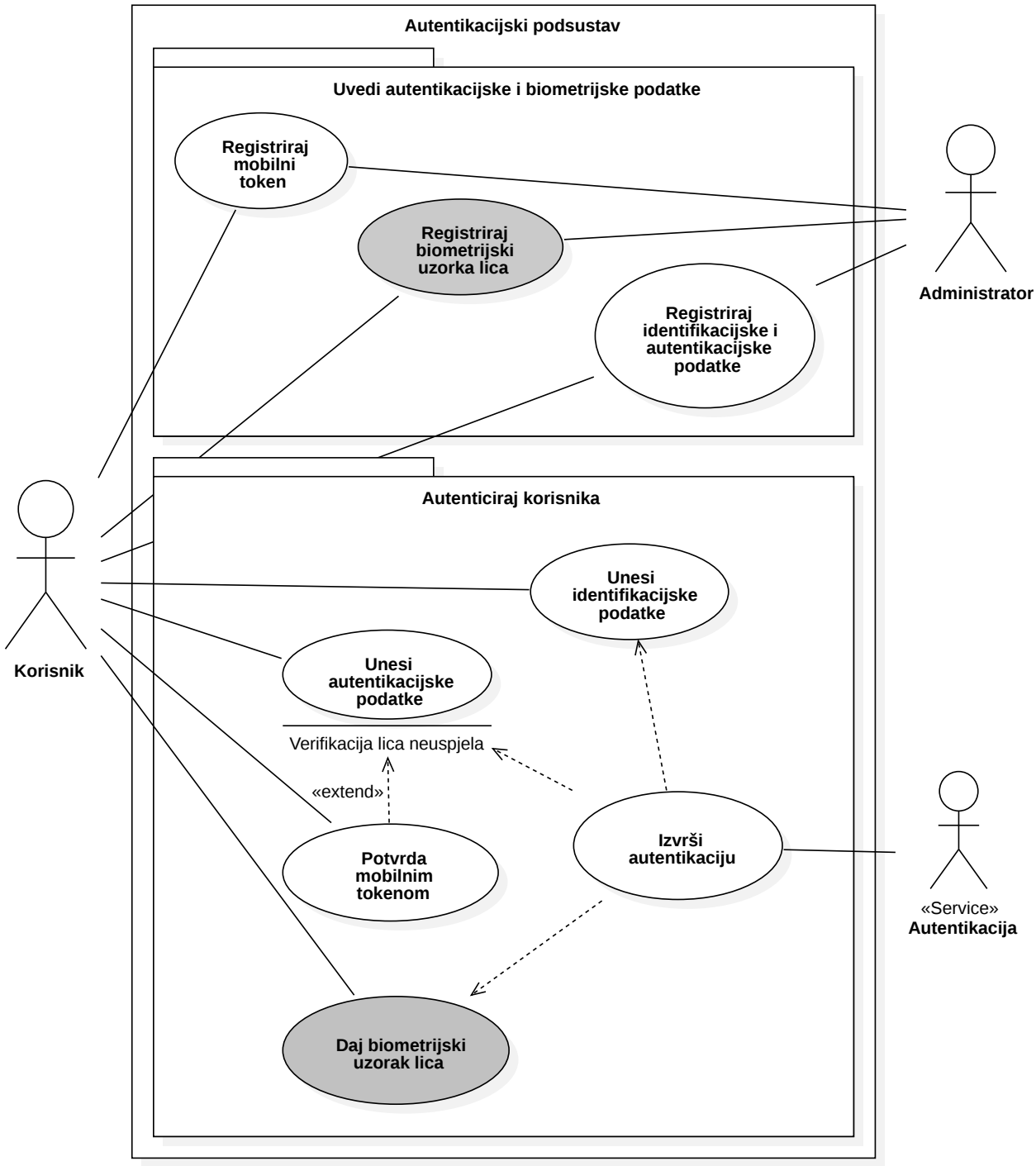
U ovom potpoglavlju izložit će se dizajn sustava autentikacije putem biometrijskih karakteristika lica gledajući s visoke razine. Pritom, izloženi dizajn ni u kojem slučaju detaljno ne prikazuje sve sastavnice sustava, niti prikazuje cjelokupni platni sustav, već samo one dijelove koji su vezani uz autentikaciju. Neki dijelovi prikazani su na vrlo visokoj razini, dok su drugi prikazani na detaljnijoj. Razlog tome je činjenica da su pojedini dijelovi sustava ovise o načinu implementacije.

U poglavlju platnom sustavu dan je osvrt na opći model slijeda događaja kod vršenja transakcija, a sada će se dati općenitiji model s naglaskom na autentikaciju - prikazan dijagramom slučaja korištenja 5.2.



Slika 5.2: Dijagram slučaja korištenja platnog sustava.

Iz gornje apstrakcije sustava posebno je avžan slučaj korištenja autentikacije, ali i uvođenje korisnika u sustav, koji je povezan sa samom autentikacijom jer se prema opisu koncepta upravo u toj fazi uzimaju uzorci biometrijske karakteristike lica za daljnju usporedbu. Na slici 5.3 vidi se opći model autentikacijskog podsustava iz perspektive vanjskih korisnika.



Slika 5.3: Dijagram slučaja korištenja autentikacijskog sustava.

Vanjski korisnici su oni koji su u interakciji sa sustavom, odnosno dio sustava. U autentikacijskom sustavu prisutna su tri korisnika.

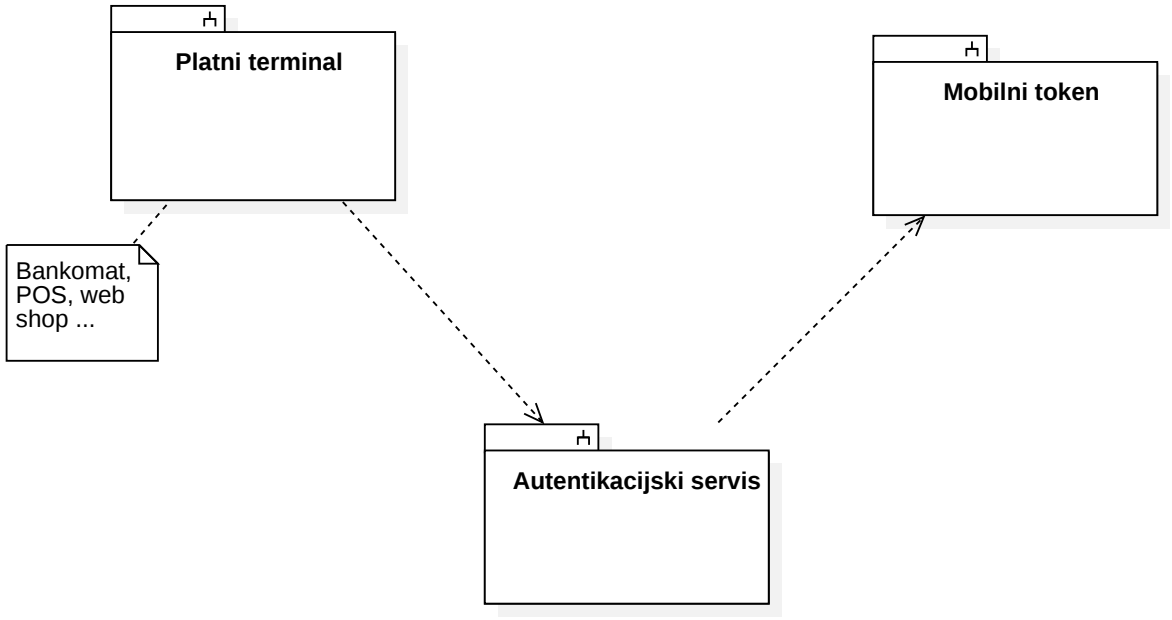
- Korisnik - fizički korisnik sustava, tj. klijent financijske ustanove koja pruža uslugu biometrijske autentikacije

  - sudjeluje u registraciji računa, tj. daje biometrijski uzorak i aktivira mobilni token na svom uređaju,
  - unosi identifikacijske podatke poput detalja kreditne kartice, korisničkih imena, email računa itd.,
  - unosi autentikacijske podatke poput PIN-ova i lozinki,
  - pasivno daje biometrijski uzorak prilikom vršenja transakcije, i
  - potvrđuje identitet mobilnim tokenom ako ga sustav ne može autenticirati putem uzorka, ili uzorak ne može biti uzet.

- Administrator - fizička osoba/e, službenik financijske ustanove osposobljen i ovlašten za registraciju novih korisnika i uzimanje biometrijskog uzorka
  - sudjeluje u registraciji računa, tj. uzima biometrijski uzorak i aktivira mobilni token na uređaju klijenta,
  - izdaje identifikacijske i autentikacijske podatke klijentu, tj. korisniku (kreditne kartice, brojeve računa, PIN, itd.).

- Autentikacija - servis koji vrši autentikaciju korisnika
  - autenticira korisnika na temelju unesenih identifikacijskih i autentikacijskih podataka, a po neprihvaćanju biometrijskog uzorka, ili nedostatka istog, šalje zahtjev za potvrdu mobilnim tokenom.

Na dijagramu 5.4 prikazana je osnovna generička biometrijska arhitektura sustava za autentikaciju.



Slika 5.4: Arhitektura sustava za transakcije na visokoj razini apstrakcije.

Arhitektura autentikacijskog podsustava sastoji se od tri komponente:

- platnog terminala,
  - bilo da se radilo o fizičkom uređaju ili web servisu, platni terminal, posredno ili neposredno, komunicira s autentikacijskim servisom radi provjere autentikacijskih podataka
- autentikacijskog servisa, i
  - koji vrši autentikaciju na temelju unesenih podataka i biometrijske identifikacije te zatražuje potvrdu mobilnim tokenom, ako je to potrebno
- mobilnog tokena
  - koji potvrđuje identitet osobe ako biometrijski uzorak nije prepoznat ili ga nije moguće prikupiti

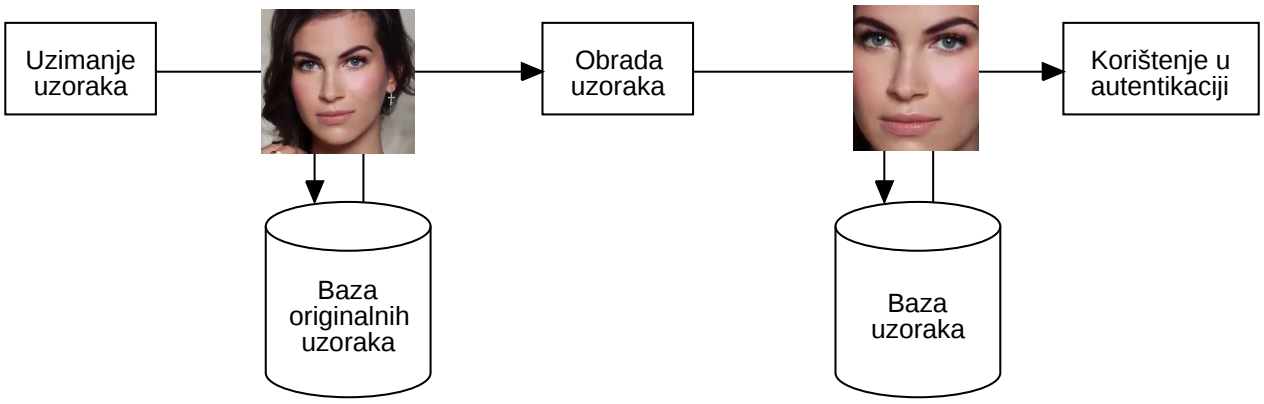
Kako je iz dijagrama vidljivo, autentikacijski servis centralni je objekt sustava te povezuje platni terminal i mobilni token, koji su u službi iniciranja transakcije i autentikacije.

5.3 Uvođenje autentikacijskih i biometrijskih podataka u sustav

Prije no što korisnik može koristiti transakcijski sustav, potrebno je ga je uvesti u sustav te izdati korisničke podatke. Prvo se uvode klasični korisnički podaci poput korisničkog imena i lozinke ili broja kreditne kartice

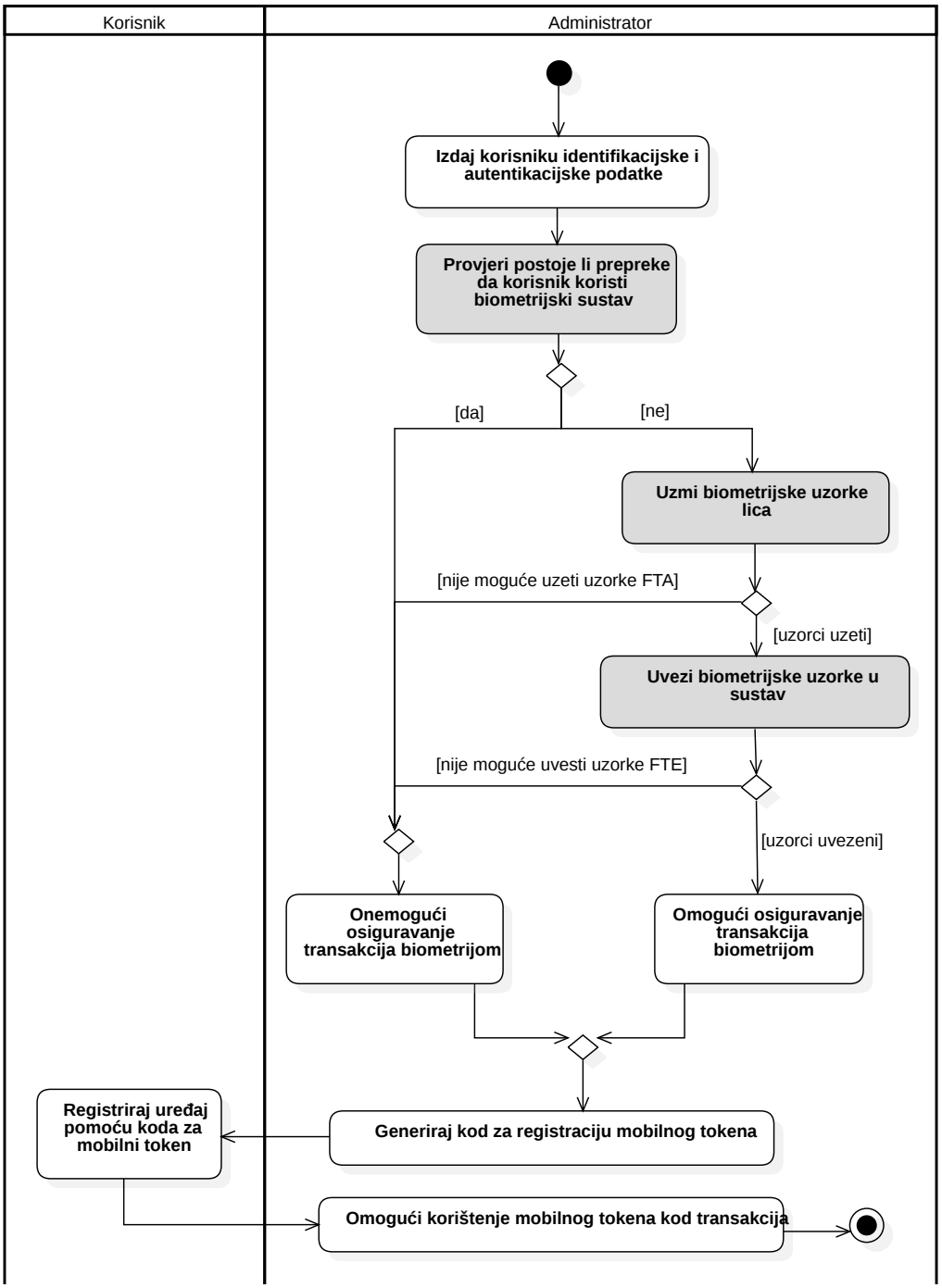
i PIN-a, itd. Potom je potrebno provjeriti da li je moguće koristiti biometrijski sustav. Prepreke korištenju biometrijskog sustava mogu biti razne, poput npr. privole korisnika, invaliditeta, tehnološkog predznanja, itd.

Sljedeći korak je uvođenje korisničkih biometrijskih uzoraka lica u bazu uzoraka (prikaz 5.5). Broj i kakvoća uzoraka ovisni su o implementaciji konkretnog algoritma prepoznavanja. Unatoč tome, većina algoritama potražuje da su uzorci takvi da je cijelo lice ravnomjerno i dovoljno osvijetljeno, u pravilnom položaju te da su granice uzorka rubovi lica uz što manje površine koja nije lice.



Slika 5.5: Uvođenje uzoraka u bazu za korištenje u autentikaciji

Moguće je da sustav ne može uzeti uzorke zbog netipičnosti izgleda lica, deformacija i sl. U tom slučaju radi se o tome da sustav ne može prikupiti valjane uzorke (engl. *Failure to Acquire*) te takav korisnik ne može koristiti biometrijski sustav. Osim nemogućnosti uzimanja uzorka, prilikom uvođenja korisnika moguće je i da se prikupljeni uzorci zbog nedovoljne kvalitete ne mogu koristiti u biometrijskom sustavu ili ih sustav ne prepoznaje kao valjane (engl. *Failure to Enroll*). U tom slučaju korisnik ne može koristiti biometrijski sustav. Na dijagramu 5.6 formalno je prikazan postupak registracije autentikacijskih i biometrijskih podataka u sustav.

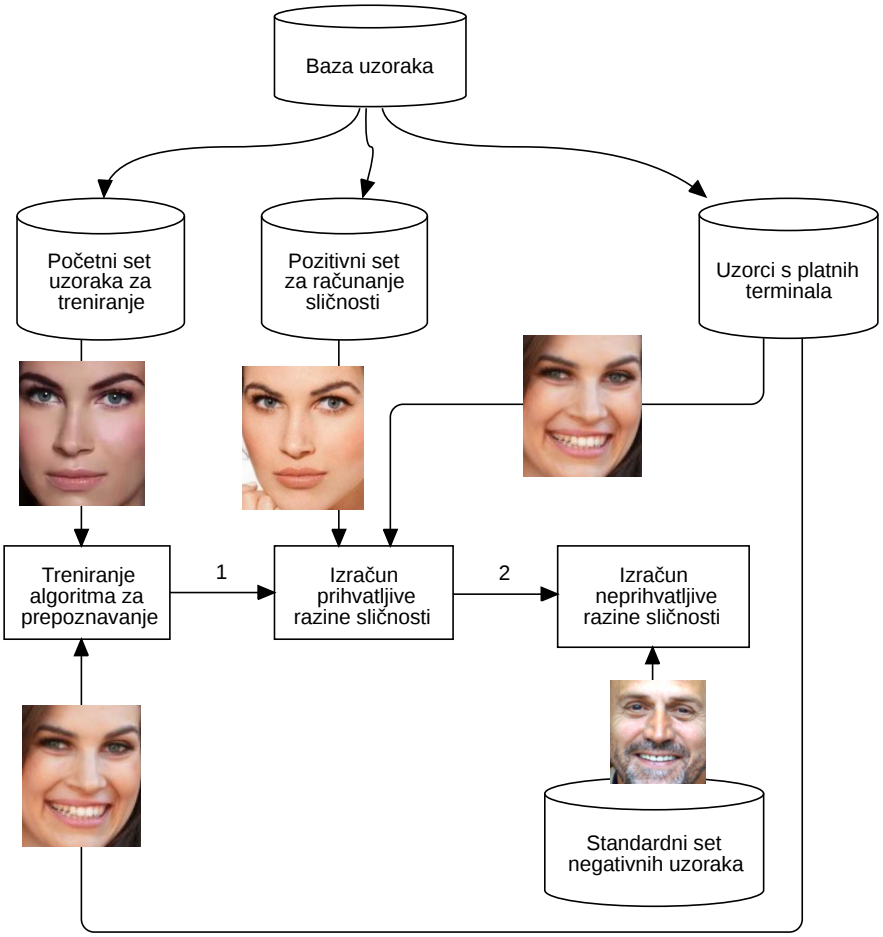


Slika 5.6: Tok aktivnosti za proces uvođenja autentikacijskih i biometrijskih podataka u podsustav

Kako sam rad u okviru modela ne nameće korištenje specifičnih algoritama, štoviše, potiče se izgradnja modularnog sustava, poželjno je da originalni uzorci budu dovoljne kvalitete kako bi se uvođenjem novih algoritama i metoda mogli ponovno iskoristiti.

5.3.1 Izračun raspona prihvatljivih razina sličnosti uzoraka

Nakon uvođenja korisnika u sustav, potrebno je izračunati raspon sličnosti u kojem će se novi uzorci prihvaćati, odnosno odbacivati. Izračun se temelji početnom pozitivnom i negativnom setu, a u toku korištenja sustava raspon sličnosti se podešava prema novim uzorcima s platnih terminala. Na slici 5.7 prikazan je postupak uvođenja i korištenja uzoraka za određivanje raspona sličnosti.



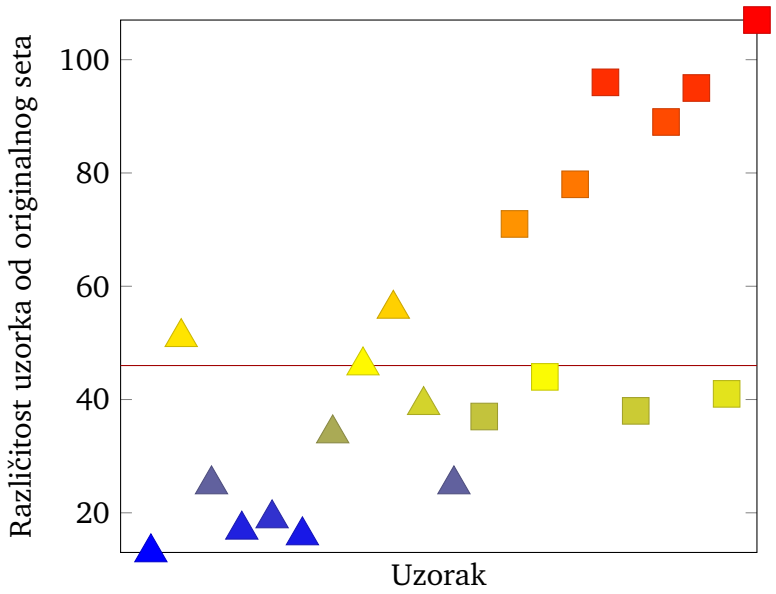
Slika 5.7: Početni izračun raspona prihvatljivih razina sličnosti uzoraka

Prvi korak je tzv. *treniranje* algoritma prepoznavanja prema početnom setu. Nakon što algoritam bude istreniran, računaju se različitosti s pozitivnim setom, odnosno setom s uzorcima istog korisnika te s negativnim setom, tj. setom čiji uzorci nisu korisnikovi. Nad dobivenim vrijednostima vrši se statističku analizu u okviru srednjih vrijednosti i mjera varijabilnosti, pomoću kojih se može odrediti raspon sličnosti unutar kojeg će se prihvaćati uzorke s platnih terminala.

Kada korisnik počne koristiti biometrijski sustav, prilikom svake prijave nastajat će novi uzorci, koji će potom biti spremani u bazu uzoraka. Novi uzorci koristit će se za ponovno treniranje algoritma kako bi

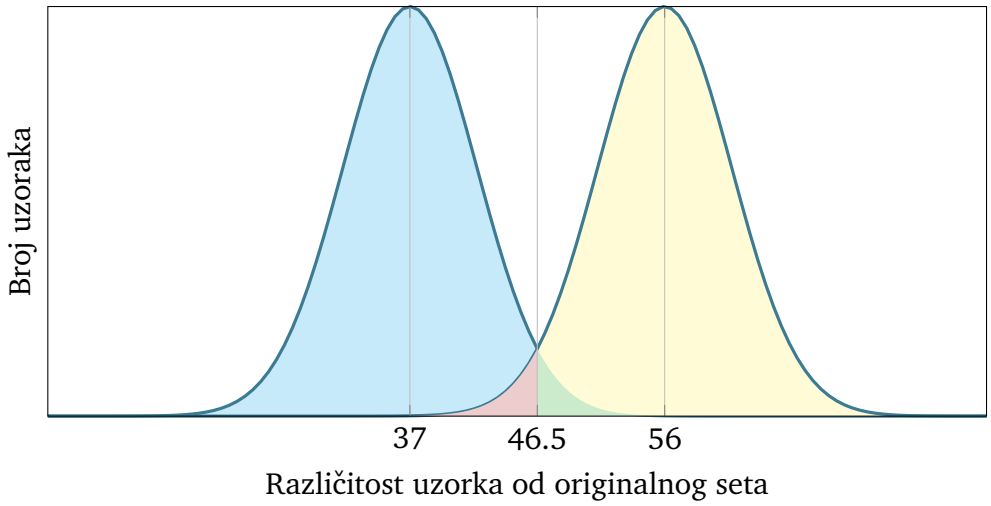
se pospješilo prepoznavanje. Obnavljanje baze uzoraka prilikom svake transakcije jedan je od doprinosa ovoga rada te je detaljnije opisano u nastavku.

Prilikom izračuna raspona sličnosti potrebno je voditi brigu o tome da se granična vrijednost postavi tako da se u što većoj mjeri eliminiraju uzorci koji ne pripadaju korisniku te da se u što manjoj mjeri odbace uzorci koji pripadaju. Kako se vidi na slici 5.8, granica sličnosti, tj. različitosti, postavljena je na ovom primjeru na 46.5, gdje se eliminira većina lažnih uzoraka (kvadrati), a prihvaća većina valjanih (trokuti).



Slika 5.8: Primjer postavljanja granice prihvatljivih razina različitosti uzoraka

Na slici 5.9 prikazana je očekivana distribucija uzoraka prema različitosti s treniranim setom uzoraka. Ako bi za granicu uzeli mjeru sličnosti od 46.5 (presjek krivulja), tada bi područje obojano zeleno ispod krivulje označavalo pogrešno odbačene uzorke (FRR), a ono obojeno crveno pogrešno prihvaćene uzorke (FAR).



Slika 5.9: Očekivana distribucija sličnosti valjanih uzoraka (plavo) i nevaljanih uzoraka (žuto).

Granica prihvaćanja postavlja se prema sigurnosnoj politici kakva se želi provoditi. Formalno, kod autenticiranja svakog novog uzorka zapravo se provodi jednosmjeran test na gornju granicu, gdje se hipoteze koje se testiraju opisuju kao (Dobša, 2017):

$$H_0 \ldots \lambda \leq \lambda_0 \tag{5.1}$$

$$H_1 \ldots \lambda > \lambda_0 \tag{5.2}$$

gdje nulta hipoteza H_0 kazuje da uzorak pripada osobi, tj. originalnom setu uzoraka, a alternativna hipoteza H_1 da ne pripada. Prema tome, λ predstavlja mjeru različitosti novog uzorka, dok λ_0 predstavlja granicu prihvatljivosti. Nadalje, prilikom postavljanja gornje granice u obzir se uzima tri parametra (Dobša, 2017):

- α - *vjerojatnost odbacivanja istinite nulte hipoteze (FRR) ili signifikantnost,*
- $beta$ - *vjerojatnost prihvaćanja lažne nulte hipoteze (FAR), i*
- $1-\beta$ - *vjerojatnost odbacivanja lažne nulte hipoteze, tj. snaga testa.*

Dakle, postavljanjem razine signifikantnosti i vjerojatnosti prihvaćanja lažne hipoteze, može se utjecati na to kolika je vjerojatnost da se valjani korisnik prijavi, odnosno da se lažni korisnik odbaci. U nastavku rada predstavljena je metoda fluktuacije granične vrijednosti sličnosti u proporciji s visinom transakcije.

5.4 Autenticiranje korisnika

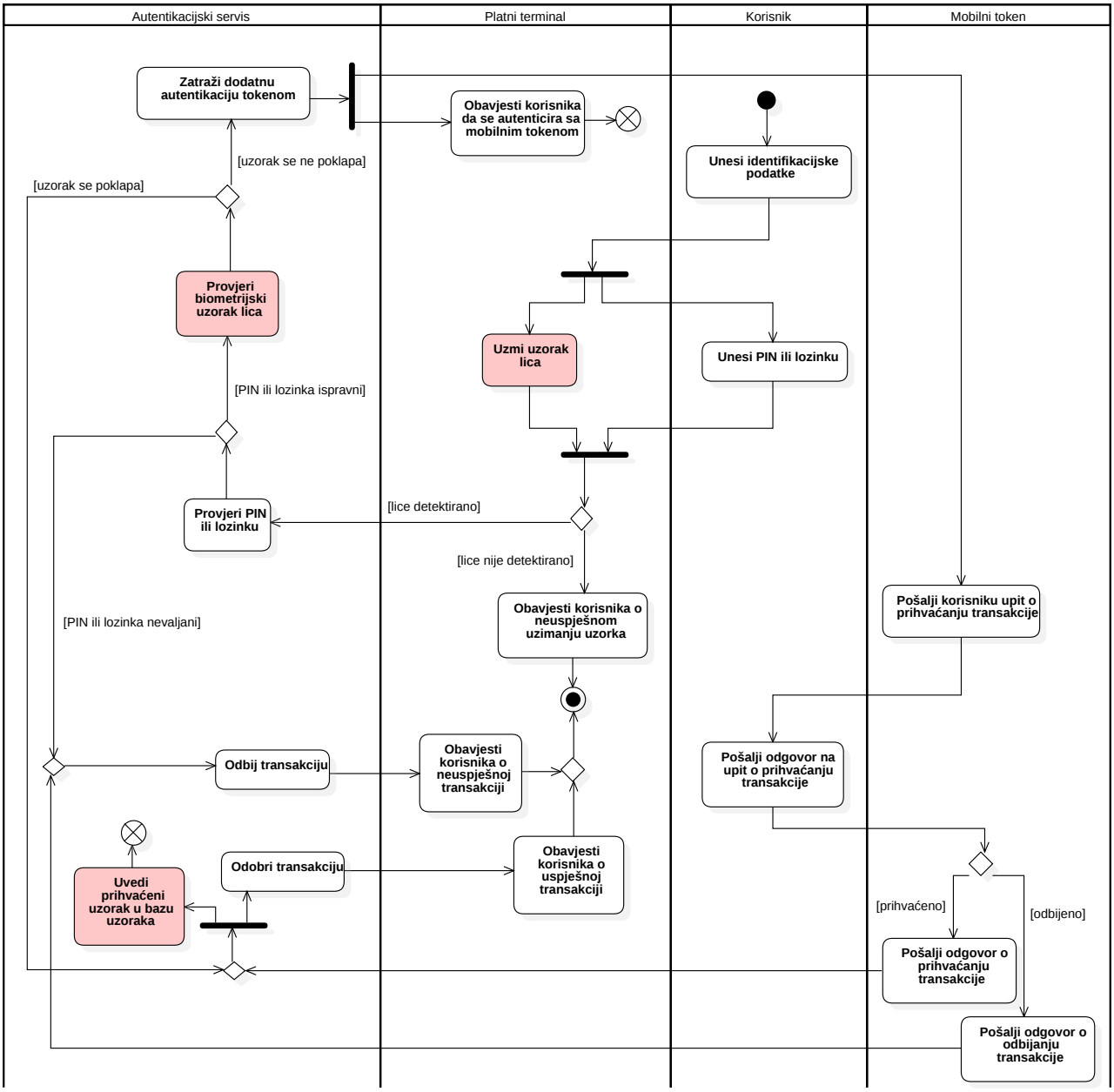
Nakon što je korisnik uspješno unesen u biometrijski sustav, transakcije se mogu početi osiguravati provjerom lica. Prvi korak je iniciranje transakcije od strane korisnika pri kojemu isti unosi identifikacijske podatke poput korisničkog imena ili broja kreditne kartice. Po unosu navedenog, platni terminal, bilo bankomat, POS uređaj ili računalo, šalje upit za unos PIN-a ili lozinke, te u isto vrijeme, tj. paralelno, inicira prikupljanje uzorka lica uz provjeru živosti slike. Paralelnost je ovdje zbog toga da bi se uštedjelo na korisnikovom vremenu te se uklonila potreba za obraćanjem pažnje na prikupljanje uzorka. Ako se uzorak automatski ne prikupi, korisnika će se obavijestiti da se pokuša prilagoditi senzoru kako bi transakcija uspješno provela. Ako se uzorak lica ne može uzeti, transakcija se ne može provesti kako se onda ne bi moglo manipulirati ostalim sredstvima autentikacije.

Po slanju autentikacijskih i biometrijskih podataka na autentikacijski servis isti se provjeravaju. Ako potvrda PIN-a ne uspije, transakcija se odbija, a ako je PIN prihvaćen, nastavlja se s provjerom uzorka lica.

Ako se uzorak lica potvrdi, isti se sprema u bazu uzoraka za daljnje usporedbe, a transakcija se odobrava. U suprotnom, od korisnika se traži autentikacija mobilnim tokenom. Uspije li se korisnik autenticirati mobilnim tokenom, transakcija se prihvaća, a uzorak ponovno ulazi u bazu uzoraka, uz provjeru odstupanja od ostalih uzoraka u bazi, kako bi se spriječilo ubacivanje lažnog uzorka u bazu.

Na dijagramu 5.10 formalno su prikazane aktivnosti koje se provode u procesu autentikacije korisnika. Ovdje se neće opisivati sve aktivnosti jer je većina općenito prisutna u svim sustavima za autentikaciju pa samim time i dovoljno jasna. Aktivnosti koje nose inovaciju modela detaljnije će se opisati u narednim poglavljima, a one su:

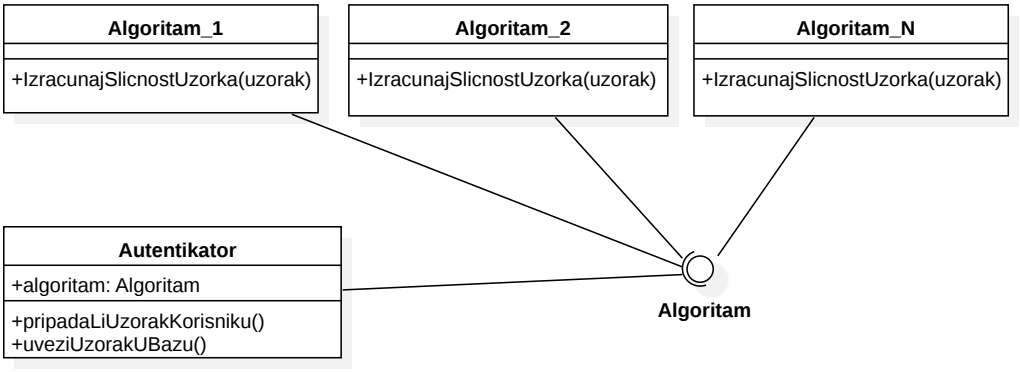
- *Uzmi uzorak lica*,
- *Provjeri biometrijski uzorak lica*, i
- *Uvedi prihvaćeni uzorak u bazu uzoraka*.



Slika 5.10: Tok aktivnosti za proces autentikacije

Kako je već napomenuto, u ovom modelu se ne nameće odabir autentikacijskih algoritama i metoda, štoviše, model predlaže izgradnju modularnog sustava koji bi dopuštao modifikacije i optimizacije algoritama u samom tijeku korištenja. Također, poradi veće sigurnosti, poželjno je koristiti više algoritama čijim bi se konsenzusom ostvario točniji klasifikator ili bi se manjkavost jednog algoritma mogla nadoknaditi drugim i sl. Za ostvarenje navedenog, model predlaže da svi implementirani algoritmi moraju imati propisanu specifikaciju ulaznih i izlaznih parametara, tj. da izračunata sličnost bude normalizirana kako bi se rezultati mogli usporediti. Isto tako, potrebno je da algoritmi imaju propisane metode, ako se radi u

okviru objektno orijentiranog dizajna. Konačno, autentikator algoritme treba koristiti sukladno specifikaciji, dok se odabir i kombiniranje algoritama prepušta unutrašnjoj logici modela. Prijedlog modularnosti ilustriran je dijagramom klasa 5.11.



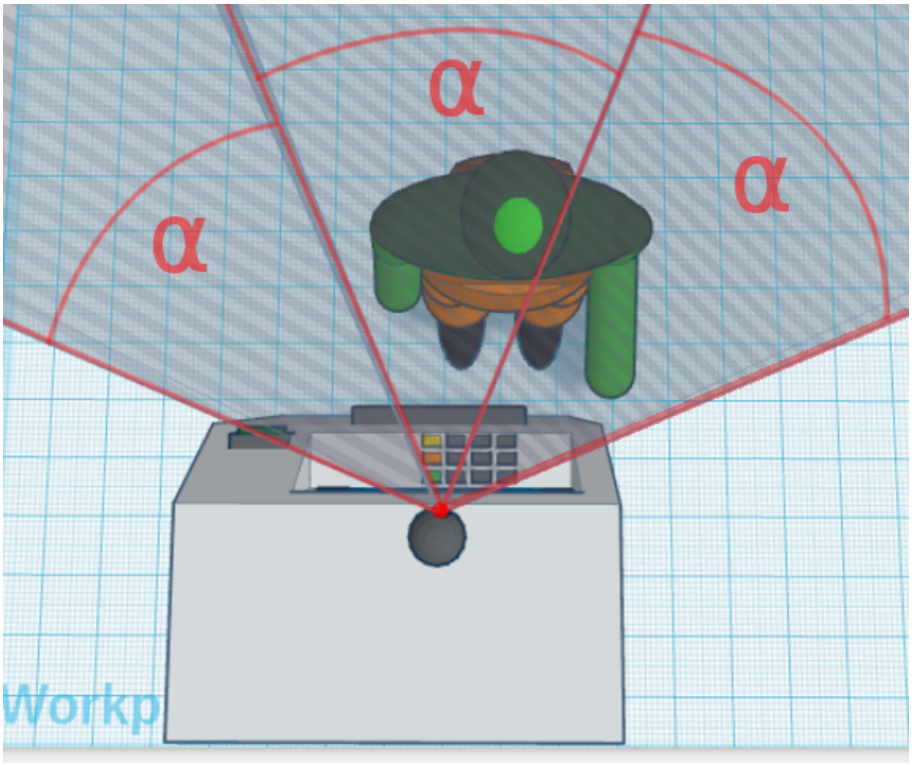
Slika 5.11: Modularnost algoritama prepoznavanja u autentikacijskom sustavu

5.4.1 Postupak prilagođenog uzimanja uzorka lica

Postupak prilagođenog uzimanja uzorka lica odnosi se samo na POS uređaje i bankomate, a sastoji se od implementacije hardverskog sklopa koji može odrediti položaj osobe i njenog lica te pratiti lice u prostoru ako postoji tendencija izlaska iz vidljivog polja kamere. Za pronalaženje osobe u prostoru pretpostavlja se sljedeće:

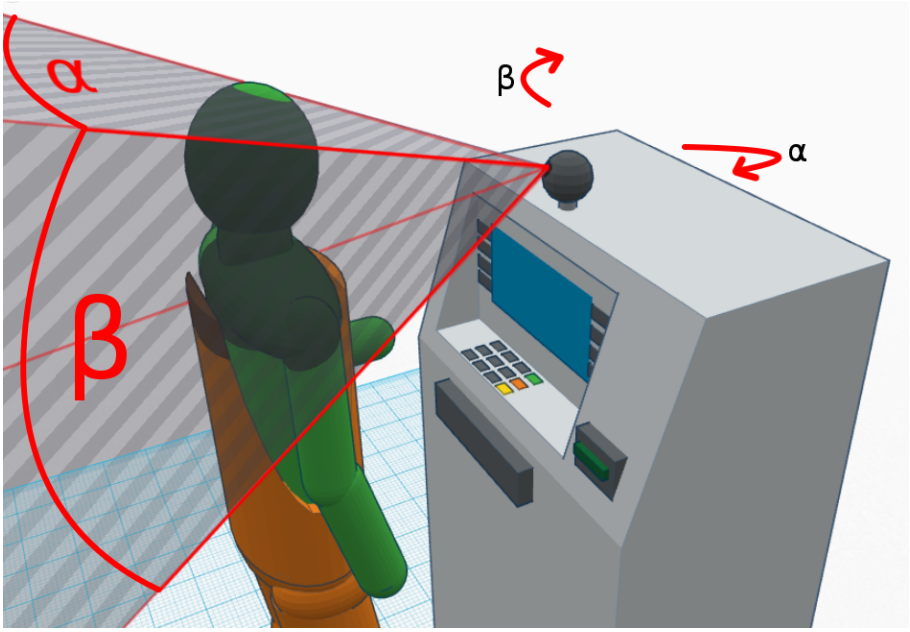
- *osoba koja vrši transakciju na najmanjoj je udaljenosti od uređaja od ostalih osoba koje mogu biti u blizini*,
- *osoba je u trenutku vršenja transakcije u interakciji s uređajem*,
- *osoba je licem usmjerena prema zaslonu uređaja*, i
- *lice osobe nije prekriveno*.

Ove pretpostavke omogućuju da se prvotno odredi horizontalna pozicija osobe u prostoru, a onda i vertikalna pozicija lica. Određivanje horizontalne pozicije moguće je ostvariti detekcijom osobe na slici te zakretanjem objektiva za vidljivi kut kamere kako bi se pokrio cijeli prostor ispred senzora. Također, moguće je koristiti i senzor aproksimacije udaljenosti objekta od senzora, gdje bi se osoba uzela kao najbliži objekt. Detekcija horizontalne pozicije dana je na slici 5.12.



Slika 5.12: Ilustracija detekcije položaja osobe u prostoru zakretanjem senzora za kut vidljivog polja α

Nakon detekcije horizontalne pozicije, može se detektirati i položaj glave, odnosno lica u prostoru, s time da se sada objektiv pomiče vertikalno, kako je prikazano na slici 5.13.

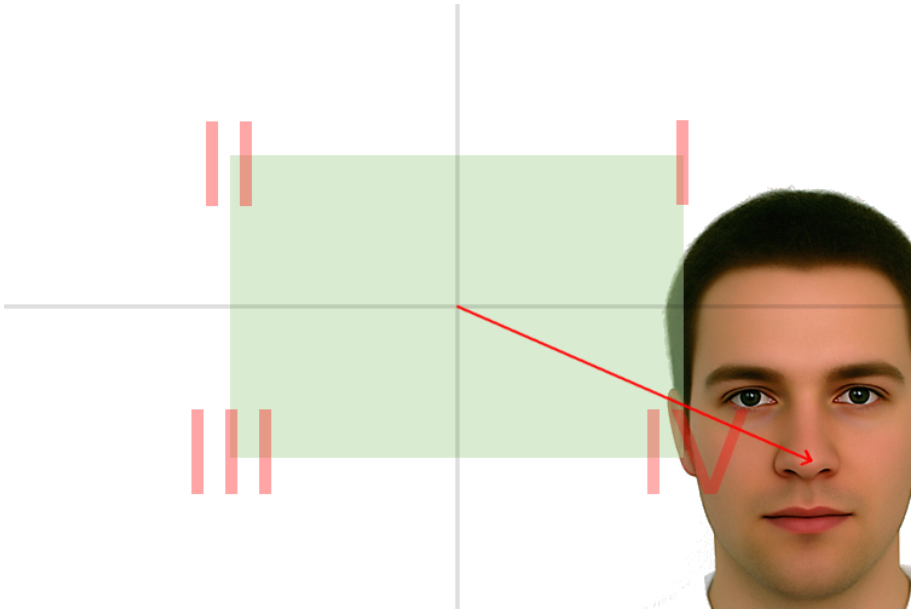


Slika 5.13: Ilustracija automatskog pronalaženja lica u prostoru zakretanjem senzora za kuteve vidljivih polja α (horizontalno) i β (vertikalno) i uzimanja uzorka

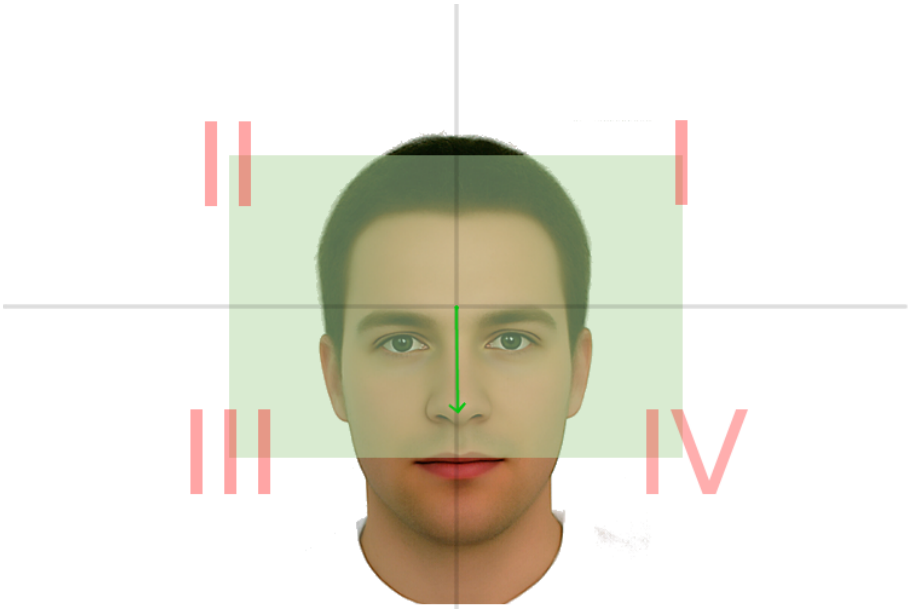
Jednom kada je lice pronađeno, uređaj pomacima prati lice ako osoba kretanjem izlazi iz područja detekcije senzora. Ovo se ostvaruje na sljedeći način. Kadar koji senzor slike obuhvaća podijeljen je na četiri kvadranta i područje sigurnog za detekciju koje obuhvaća centralnu četvrtinu (područje omeđeno zeleno na slici 5.14). Ako se lice nalazi izvan sigurnog područja detekcije, određuje se kvadrant u kojem se lice nalazi. Kada se ustanovi kvadrant, senzor se pomiče za jedinični korak prema sljedećim položajima:

- I kvadrant - *gore, desno,*
- II kvadrant - *gore, lijevo,*
- III kvadrant - *dole, lijevo, i*
- IV kvadrant - *dole, desno.*

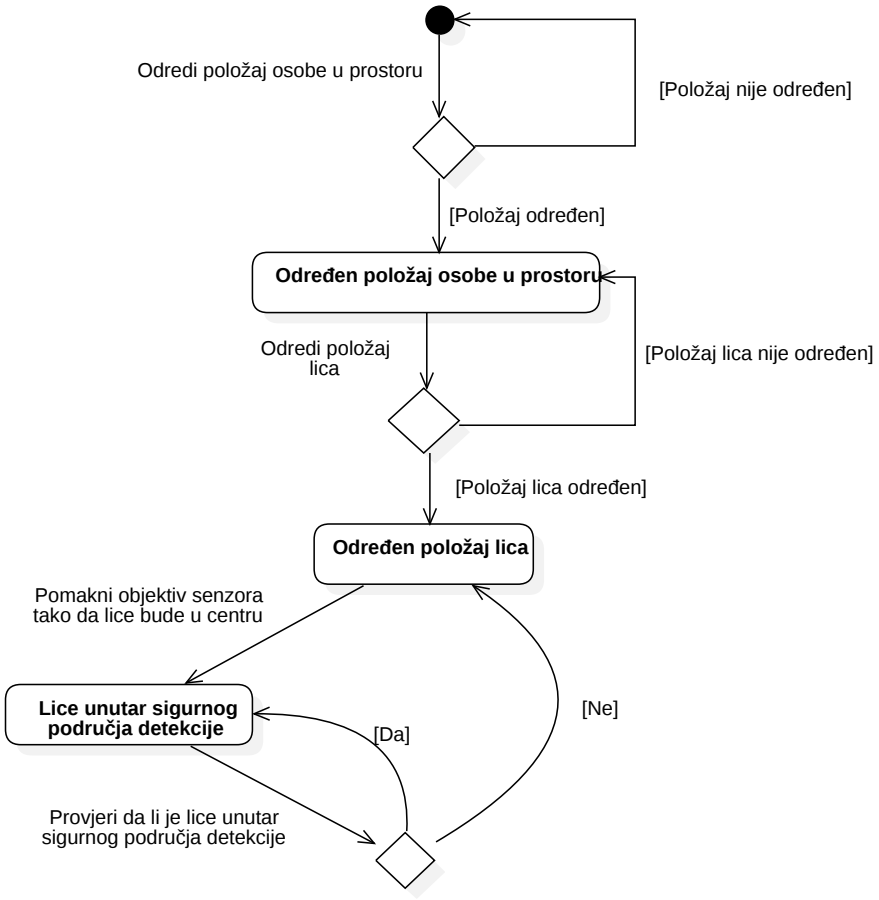
Nakon pomicanja za jedinični korak, ponovno se vrši detekcija te se ponavljaju prethodno opisane radnje. Jedinični korak najmanji je mogući korak kojeg okretni mehanizam senzora pruža. Pomicanjem za najmanji korak omogućuje se visoka ažurnost kretanja u odnosu na promjenjivi položaj lica. Konačno, prije no što je se uzorak može uzeti, potrebno je provjeriti živost lica, tj. ustanoviti da li se uistinu radi o živoj osobi, a ne fotografiji osobe. Provjera živosti slike može se izvršiti putem detekcije ponašajnih karakteristika lica ili putem ostalih obilježja poput npr. topline, reljefnosti, apsorpcije svjetla i sl. Ako se ustanovi da lice nije živo, transakcija se odbija na razini platnog terminala.



Slika 5.14: Ilustracija detektiranog lica izvan sigurnog područja detekcije.



Slika 5.15: Ilustracija detektiranog lica unutar sigurnog područja detekcije.

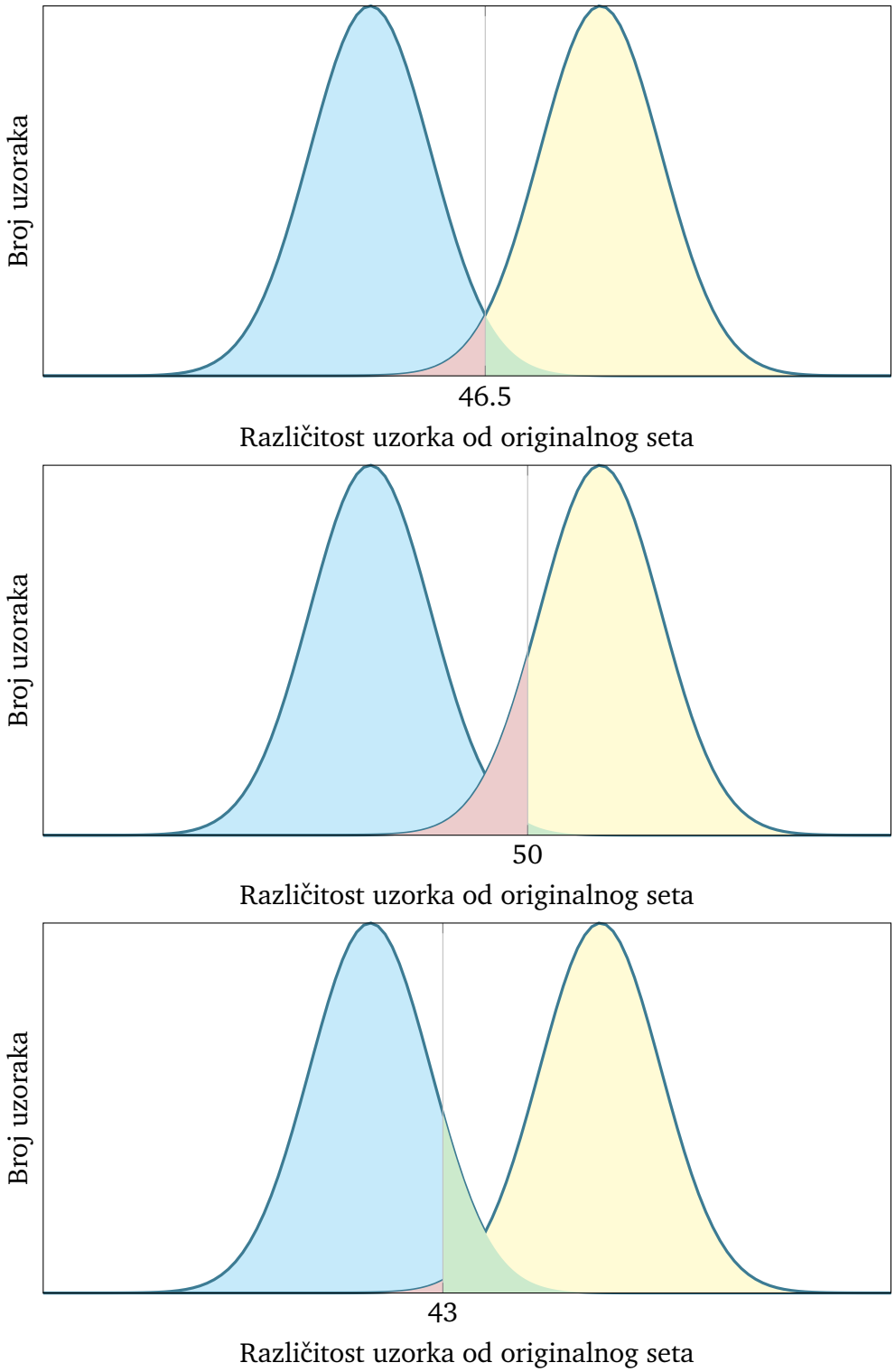


Slika 5.16: Dijagram promjena stanja koji opisuje pronalazak i očuvanje lica unutar sigurnog područja detekcije.

5.4.2 Metoda fluktuacije dozvoljenog odstupanja sličnosti prema visini transakcije

Kako sustav ne bi previše opterećivao korisnike pri svakodnevnim transakcijama manjeg iznosa, ovaj model predlaže mogućnost korištenja manje razine sličnosti pri nižim novčanim transakcijama. Kod takvih transakcija raspon sličnosti postavio bi se tako da se valjani korisnik gotovo uvijek može autenticirati, dok većina lažnih korisnika to nije u mogućnosti.

Sličan model koristi se kod beskontaktnih kartica, gdje se iste mogu koristi za transakcije do 100 kuna (do 1000 kuna dnevno) (Maroshi, 2015), a za veće iznose potrebno se autenticirati PIN-om ili potpisom. Isti model može se primijeniti i na fluktuaciju sličnosti, gdje bi se za transakcije do 100 kuna (do 1000 kuna dnevno), prihvaćala viša stopa različitosti, a za veće niža. Na slici 5.17 ilustrirano je pomicanje granice sličnosti.



Slika 5.17: Na prvom grafu koristi se statična gornja granica, dok se na druga dva grafa pokazuje pomak s visoke gorenje granice (za niske transakcije) na nisku (za visoke). Granica prihvatljivosti i visina transakcije obrnuto su proporcionalne.

5.4.3 Uvođenje prihvaćenih uzoraka u bazu

U analizi biometrijskih karakteristika napomenuto je da je stalnost lica srednja, tj. da se s vremenom mijenja (prikaz 5.18) pa je zbog toga potrebno izgled lica pratiti kroz kontinuirani tok vremena. Grd (2015) pojašnjava kako se promijene na licu manifestiraju kroz morfologiju lica i teksturu. Kako se algoritmi prepoznavanja oslanjaju na obje karakteristike, izmjenom ovih karakteristika sustav može zatajiti.

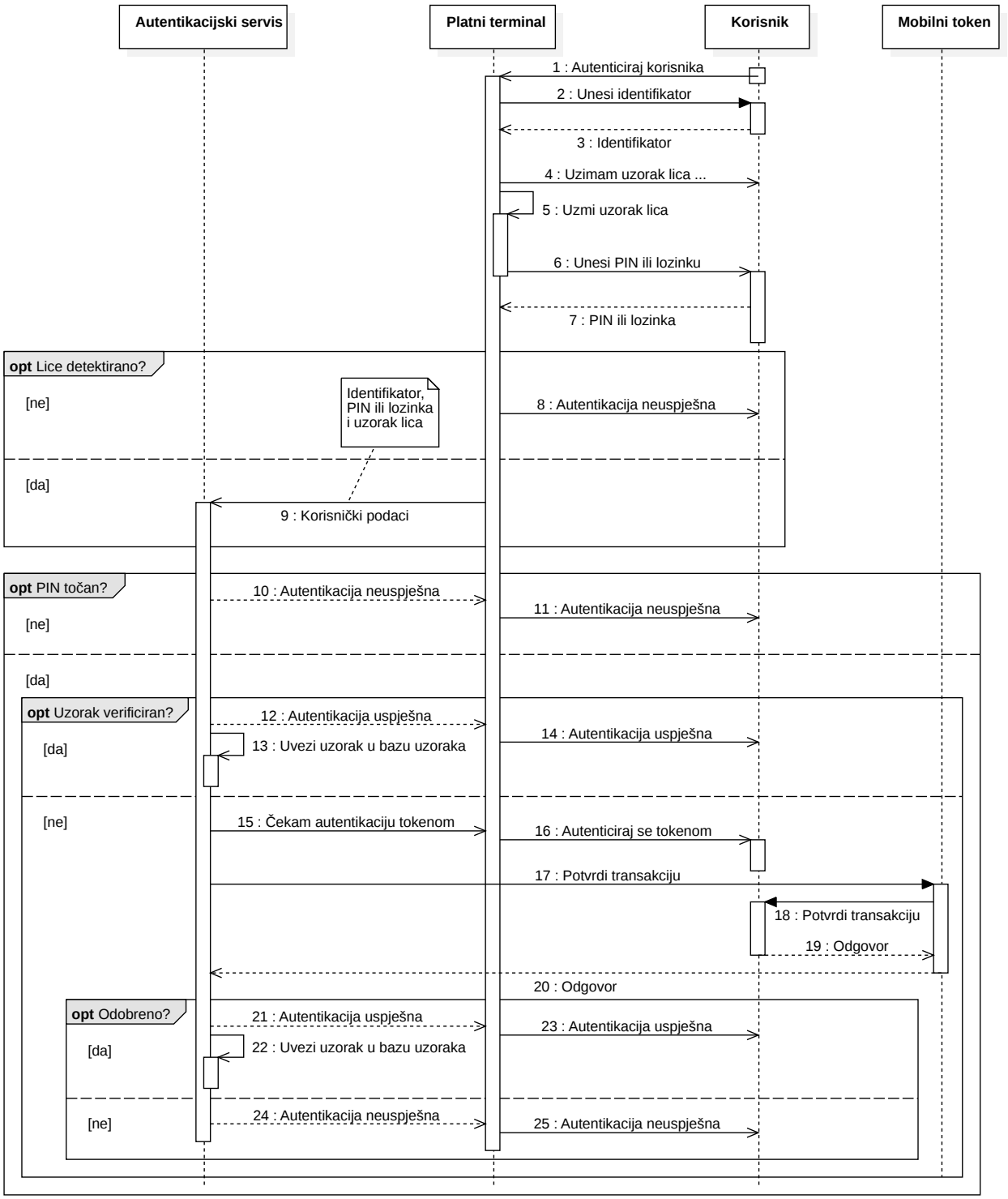
Zbog toga, svaki puta kada se korisnik uspješno autenticira, bilo licem ili tokenom, uzorak lica pohranjuje se u bazi za sljedeća uspoređivanja. Također, pohranjivanje uzoraka služi i za provjeru pri mogućim incidentima, što je vrlo važna odlika ovog sustava.

Slika 5.18: Promijena izleda lica tijekom vremena (Izvor: http://www.plasticsurgery.co.za/facial-aging/)

Prilikom uveđanja uzorka lica kod autentikacije tokenom, potrebno je provjeriti je li različitost takvog uzorka prevelika, odnosno je li različitost tog uzorka veća od najrazličitijeg pozitivnog uzorka. Ako jest, uzorak se mora provjeriti ručno od strane službene osobe u financijskoj instituciji u prisustvu korisnika. U suprotnom bi se ova funkcionalnost sustava mogla zlouporabiti tako što bi se bez znanja korisnika putem tokena u biometrijski sustav uvodile maliciozne osobe.

5.5 Specifikacija protokola

Na dijagramu sekvenci 5.19 dan je formalni redoslijed provođenja aktivnosti, tj. komunikacije između sastavnica sustava.



Slika 5.19: Dijagram sekvenci za proces autentikacije

Kako vidimo, platnom terminalu prvo dolazi zahtjev za autentikaciju. Zahtjev može doći od nekog drugog sustava, ako se radi o web trgovini ili sl., ili od istog sustava ako se radi o POS uređajima i bankomatima. Nadalje, primivši obavijest o unosu identifikatora, npr. kreditne kartice, emaila i sl., korisnik unosi istog. Nakon toga platni terminal obavještava korisnika da je započet proces uzimanja uzorka lica. Iako se ovime od samog korisnika ništa ne traži, dobro je da korisnik zna kako sustav pokušava doći do uzorka lica, ne bi li korisnik kojom svojom nehotičnom radnjom to onemogućio (prekrivanjem lica, nošenjem sunčanih naočala i sl.). U istom trenutku se od korisnika traži unos primarnoga autentikacijskog sredstva, PIN-a ili lozinke. Kako se od korisnika očekuje da, pogotovo kod fizičkih platnih terminala, lice usmjeri ka zaslonu, odnosno tipkovnici, može se predvidjeti gdje treba detektirati korisnikovo lice, kao što je prikazano na ilustraciji 5.1. Nakon što je korisnik unio PIN, odnosno terminal uzeo uzorak lica, podaci se šalju servisu za autentikaciju te se čeka uspješna autentikacija. Ako sustav prilikom skeniranja nije mogao pronaći uzorak lica, transakcija se prekida.

Kada je Autentikacijski servis dobio autentikacijske podatke, vrši autentikaciju. Prvo se provjerava valjanost PIN-a, a ako on nije valjan transakcija se prekida, u suprotnom se provjerava uzorak. Po provjeri uzorka sustav odlučuje da li je podudarnost uzorka dovoljna za autentikaciju. Ako je, tada se platni terminal obavještava o uspješnoj autentikaciji, a uzorak sprema u bazu uzoraka. Ako nije, tada se transakcija šalje mobilnom tokenu na odobrenje. Također, korisnika se putem platnog terminala obavještava da se autenticira pomoću mobilnog tokena.

Nakon što korisnik potvrdi ili odbije transakciju putem mobilnog tokena, odgovor se šalje natrag autentikacijskom servisu, a Autentikacijski servis platnom terminalu. Primijetimo kako ovdje s ciljem sigurnosti ne postoji direktni kontakt između platnog terminala i mobilnog tokena.

Što se tiče sigurnosti komunikacije, ovdje se neće iznositi opće sigurnosne principe poput korištenja kriptografije, SSL certifikata o identitetu i dr., već će se to smatrati poznatim i već implementiranim u ovaj sustav.

5.6 Dozvoljena stanja

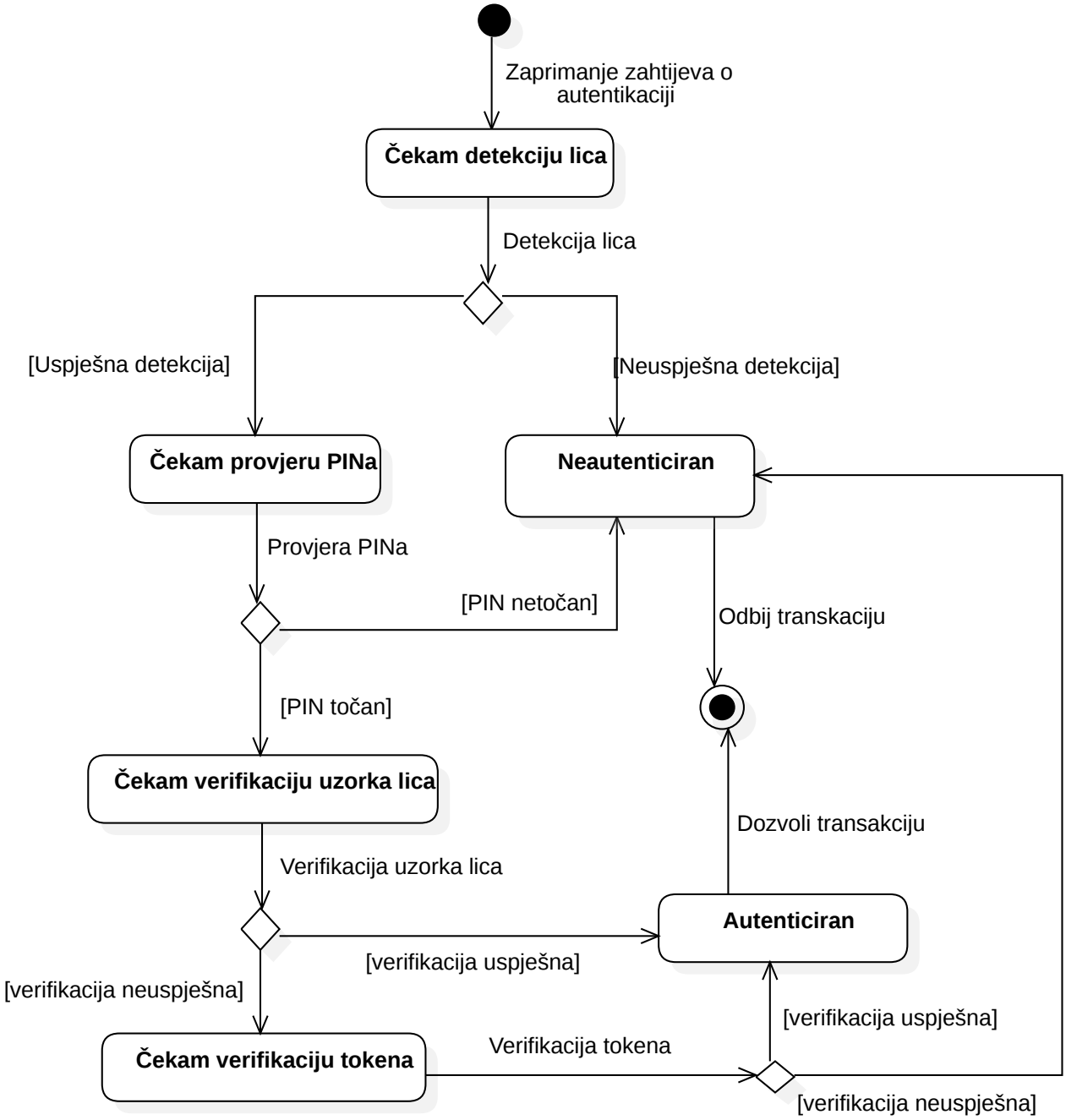
Ovako zamišljen sustav dozvoljava samo određena stanja korisnika prilikom autentikacije. Stanja korisnika ovise o uspješnosti radnji koje su potrebne da bi korisnik prešao iz jednog stanja u drugo, tj., u konačnici, iz neautenticiranog u autenticirano stanje. Pogledajmo dijagram promjena stanja korisnika prilikom autentikacije i radnji koje utječu na promjena stanja na slici 5.20.

Također, u tablici 5.1 dan je pregled dozvoljenih stanja i radnji koje su prethodile kako da bi korisnik došao u to stanje.

Tablica 5.1: Dozvoljena stanja i prethodne readnje

Stanje	**Radnja**
Čekam detekciju lica	Zaprimanje zahtijeva o autentikaciji
Čekam provjeru PINa	Detekcija lica (uspješna)
Čekam verifikaciju uzorka lica	Provjera PINa (PIN točan)
Čekam verifikaciju tokena	Verifikacija uzorka lica (neuspješna)
Autenticiran	Verifikacija uzorka lica (uspješna) ili Verifikacija tokena (uspješna)
Neautenticiran	Detekcija lica (neuspješna) ili Provjera PINa (PIN netočan) ili Verifikacija tokena (neuspješna)

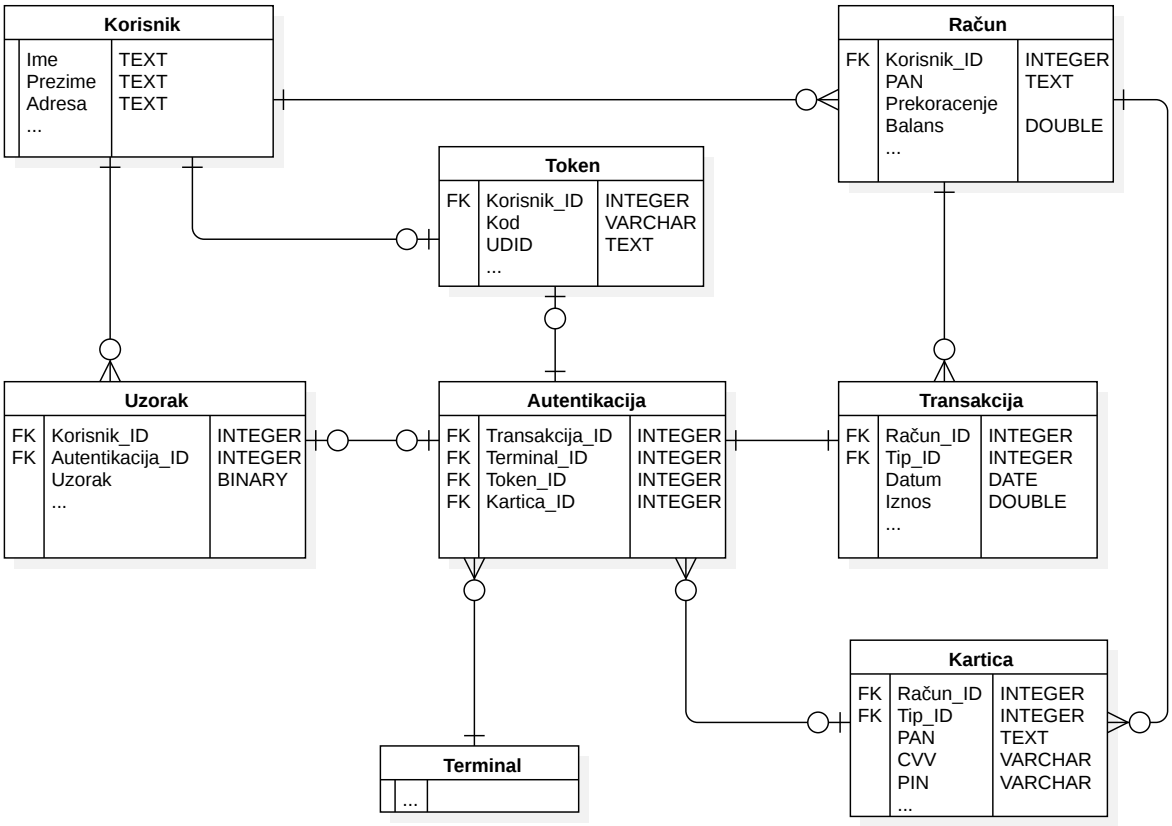
Kao što se možeiščitati iz tablice, odnosno dijagrama, eliminacijske radnje za autentikaciju korisnika su *neuspješna detekcija lica*, *provjera PINa* i *verifikacija tokena*. Iako nam je proces autentikacije intuitivno jasan iz dosadašnjeg izlaganja, postavlja se pitanje zašto se autentikacija korisnik odbacuje ako lice nije detektirano. Primarni razlog je sprječavanje zlouporabe tokena u svrhe autentikacije. Ako bi dozvolili da se korisnik autenticira samo putem mobilnog tokena cijeli sustav zapravo gubi smisao. Uspješnom manipulacijom ili krađom tokena maliciozni korisnik lako bi mogao doći do novčanih sredstava korisnika. Također, forsiranjem detekcije lica, za svaku transakciju može se vrlo jednostavno ustvrditi tko ju je izvršio, a time potvrditi i kredibilitet onoga tko je u navodnoj prevari oštećen.



Slika 5.20: Dijagram promjena stanja korisnika prilikom autentikacije

5.7 Model podataka

Na kraju, ostaje nam još definirati i model podataka. U prethodnim dijagramima dan je osvrt na podatke koji se razmjenjuju u sustavu autentikacije. U nastavku će se formalno definirati odnosi među podacima. Treba imati na umu da se neće ulaziti u detalje platnog sustava već prikazati samo ono što je vezano uz autentikaciju. Ovaj model, isto tako, nije pogodan za direktnu implementaciju sustava već je poglavito ovdje da bi se opisao odnos između entiteta u sustavu. Na dijagramu 5.21 prikazan je ER model podataka.



Slika 5.21: ER model podataka sustava autentikacije

Kako vidimo, *Korisnik* je centralna relacija sustava. *Korisnik* može u datom trenutku imati više *Računa*, a uz *Račun* se vežu *Transakcije* i *Kartice*. Svaka *Transakcija* autenticirana je *Autentikacijom*, dok *Autentikacija* dozvoljava jednu *Transakciju*. Uz *Autentikaciju* se veže *Kartica*, biometrijski *Uzorak* ili mobilni *Token* i Terminal. *Korisnik* ima više *Uzoraka* lica te jedan *Token*.

Pogledajmo sada koje je značenje pojedinih entiteta i koji su mogući atributi koji bi se u tim entitetima čuvali. Tablica:

- Korisnik sadržava sve atribute koji kazuju opće podatke o korisniku u sustavu,
- Račun označava postojanje računa te prati njegovo stanje kroz vrijeme postojanja,

  - atribut PAN je identifikator u globalnom bankovnom, tj. platnom sustavu

- Transakcija pamti prijenos sredstava s računa na račun
- Kartica je identifikacijsko-autentikacijski entitet koji račun identificira PAN-om, odnosno autenticira Korisnika PIN-om i CVV-om
- Autentikacija označava odobrenost transakcije od strane Korisnika, a također prati podatke o Terminalu, Tokenu i Kartici
- Kako je za uspješno autenticiranje potrebno više različitih uzoraka osobe, u tablici Uzorak čuvaju se Uzorci lica korisnika
  - prvotni uzorci unose se kod registracije korisnika, dok se ostali uzorci unose svakom uspješnom autentikacijom, kako je opisano u prethodnim poglavljima
  - kako je sam uzorak često kompleksne naravi, za njega je predviđen binarni okvir
- Token označava prisustvo mobilnog tokena kod Korisnika i odnosi se samo na jednog Korisnika
  - Sadrži aktivacijski kod i UDID uređaja koji u kombinaciji onemogućuju da drugi neovlašteni uređaj preuzme ulogu mobilnog tokena

6 Implementacija prototipa modela

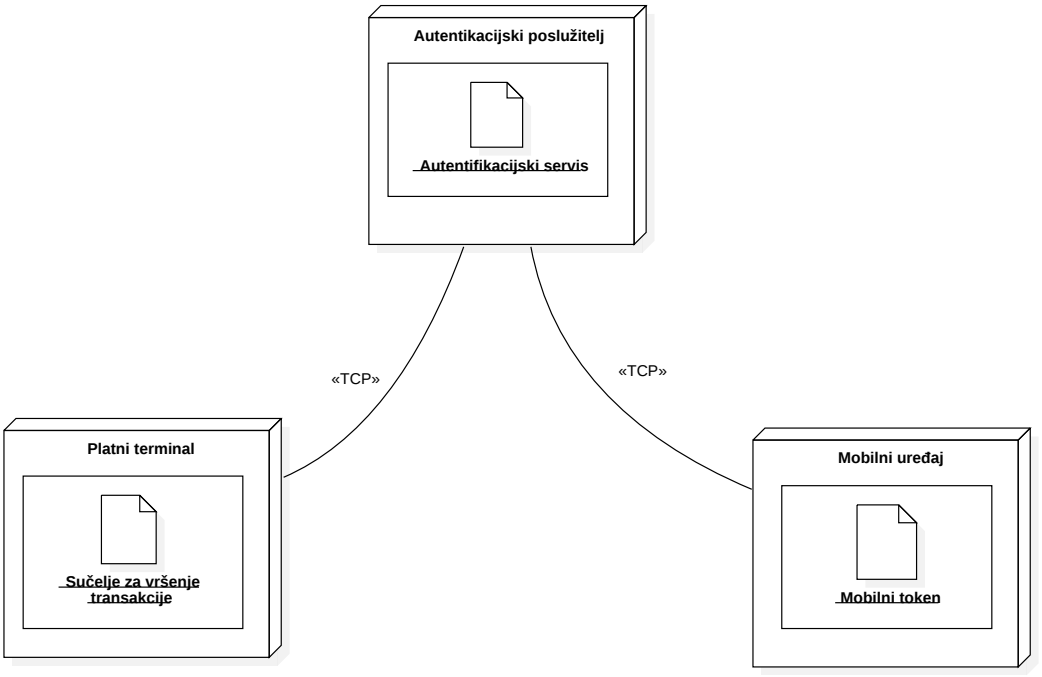
U ovom poglavlju predstavit će se implementacija prototipa ovog sustava. Implementacija ima za cilj pokazati kako se opisani model sustava može realizirati i iskoristiti u stvarnim uvjetima. Ipak, implementacija ne predstavlja puninu stvarne implementacije ovakvog sustava, niti se od nje treba očekivati da pokaže performanse kakve bi stvarni sustav trebao imati. Također, u ovom izlaganju implementacije nisu predstavljene sve pojedinosti ili cjeloviti izvorni kod sustava.

Implementacija je napravljena u obliku samostalnih računalnih aplikacija namijenjenih za POSIX kompatibilne operacijske sustave, odnosno u obliku mobilne aplikacije za iOS operacijski sustav. Dijelovi aplikacije za detekciju i autentikaciju koriste OpenCV[a] implementacije ranije navedenih algoritama. Korišteni programski jezici su Python, C/C++ i Swift 3.

[a] Kako bi sama implementacija algoritma iziskivala popriličnu količinu vremena, u implementaciji je korištena biblioteka OpenCV. Biblioteka je zapravo skup algoritama koji se koristi u području računalnog vida. Sav kod biblioteke dostupan je po BSD licenci otvorenog koda te ga se može koristiti komercijalne i nekomercijalne svrhe.

6.1 Opis prototipa

Implementirani prototip sastoji se od tri komponente: *autentikacijskog servisa*, *platnog terminala* i *mobilnog tokena*. Arhitektura prototipa istovjetna je onoj iz dizajna sustava (dijagram 5.4), tj. sve tri komponente programski su odvojene i komunikacija između njih vrši se putem mreže. Dijagramom razmještaja 6.1 prikazana spomenuta arhitektura implementacije.



Slika 6.1: Dijagram razmještaja prototipa implementacije

Kako se može vidjeti vidjeti na slici 6.1, komponente su povezane mrežom, točnije, TCP vezom. U stvarnom okruženju, platni terminal i autentikacijski servis bili bi povezani internom mrežom te bi sva komunikacija bila kriptiran zbog sigurnosti. Ova trokomponentna arhitektura zahtijeva da Autentikacijski poslužitelj uvijek bude na dostupan, dok se platni terminali i mobilni tokeni na njega spajaju po potrebi.

6.2 Autentikacijski servis

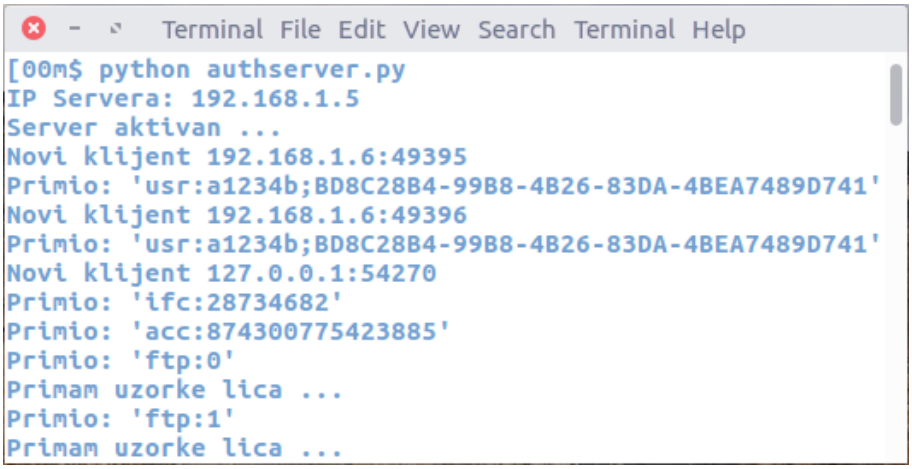
Autentikacijski servis implementiran je kao zasebna poslužiteljska aplikacija. Prije no što bi se korisnik mogao autenticirati pri autentikacijskom servisu, potrebno ga je uvesti u sustav. Kako znamo, pri autentikaciji se novi uzorak uspoređuje sa svim uzorcima u bazi pa je stoga važno da korisnik inicijalno već ima nekoliko uzoraka. Prema tome, od korisnika se uzima set od 10 fotografija lica u različitim pozama i različite veličine.

Nakon što su fotografije uzete, kiristi se ugrađena funkcija za treniranje, tj. kreiranje histograma iz uzoraka lica na fotografijama. Funkcija nakon treniranja generira datoteku u YML formatu koja sadrži vektore za svaki uzorak lica. Kasnije se navedena datoteka učitava i koristi za usporedbu pri svakom autenticiranju korisnika.

Programski kod Primjer strukture i sadržaja YML datoteke koja sadrži histograme uzoraka

```
%YAML:1.0
radius: 1
neighbors: 8
grid_x: 8
grid_y: 8
histograms:
- !!opencv-matrix
rows: 1
cols: 16384
dt: f
data: [ 6.51041651e-03, 1.38888890e-02, 0., 0., 3.90625000e-03,
7.37847248e-03, 4.34027781e-04, 1.38888890e-02, 0., 0., 0., 0.,
0., 4.34027781e-04, 0., 5.64236101e-03, 6.94444450e-03,
1.08506950e-02, 0., 0., 8.68055562e-04, 3.03819450e-03, 0.,
6.51041651e-03, 4.34027781e-04, 0., 0., 0., 4.77430550e-03,
...
```

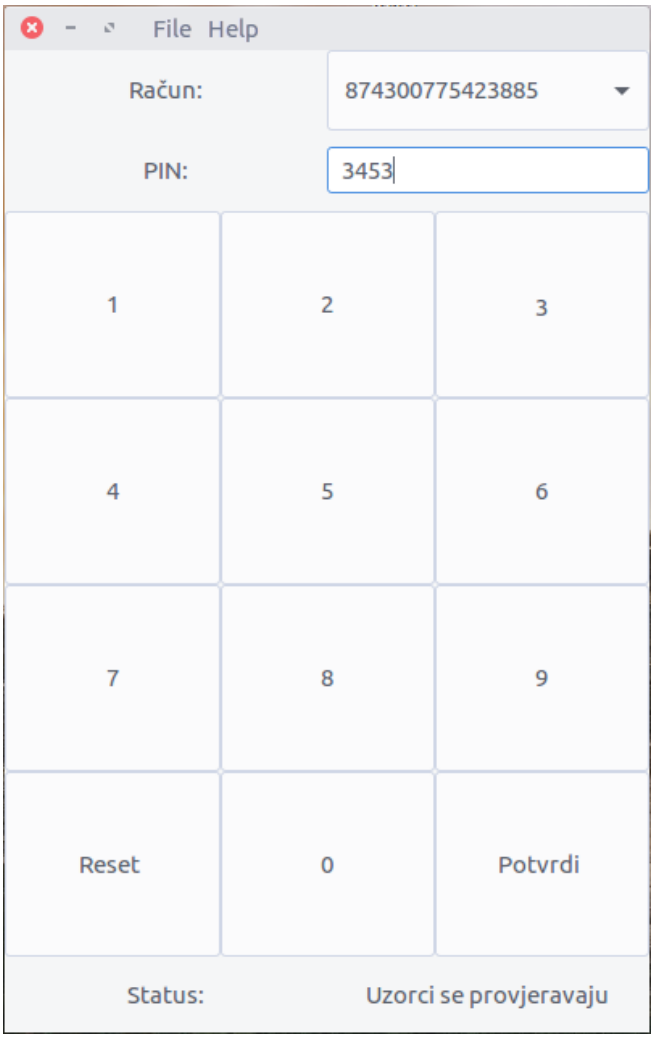
Po pokretanju, autentikacijski servis čeka na spajanje korisnika na zadanom portu, bilo da se radi o terminalu ili tokenu, a kad se korisnik spoji, servis kreira novu dretvu te započinje komunikacija između servera i korisnika. Korisnik šalje prvotni zahtjev, a poslužitelj odgovara s primjerenim odgovorom, već prema zahtjevu korisnika. Protokol komunikacije dan je u poglavlju dizajna modela sustava. Ako se korisnik uspješno autenticirao novim uzorkom, taj uzorak uključuje se u bazu uzoraka, iz već ranije spomenutih razloga. Na slici 6.2 vidi se primjer izlaznih poruka servisa pri autentikaciji korisnika.



Slika 6.2: Izlazne poruke servisa pri autentikaciji korisnika

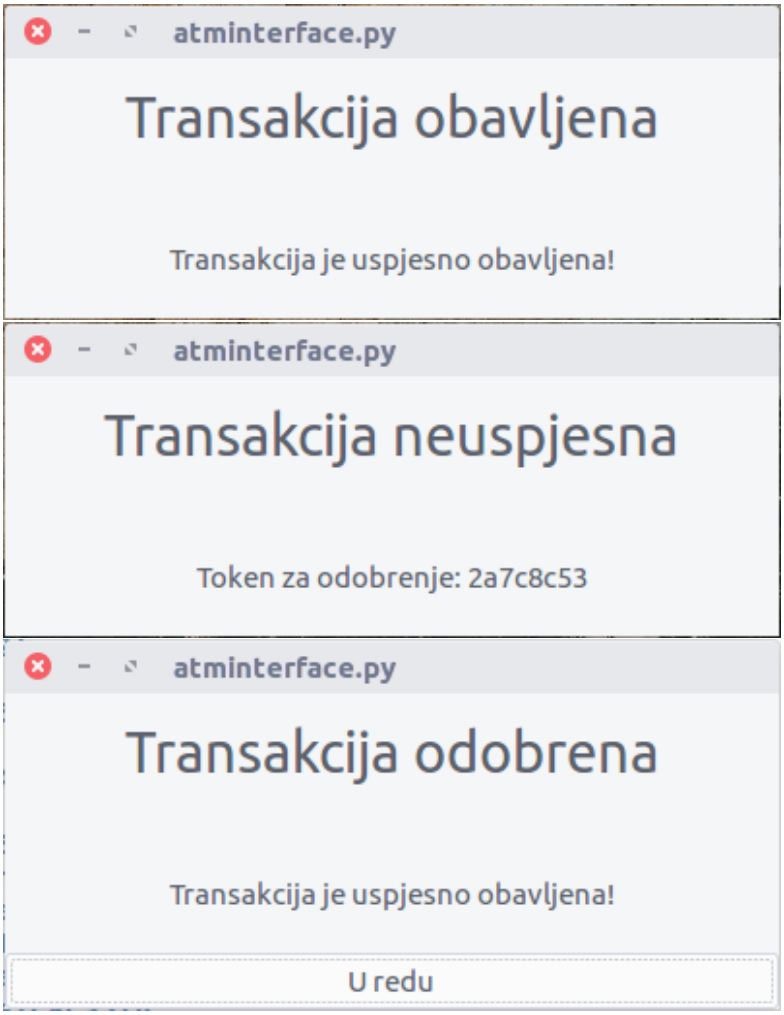
6.3 Transaktron

Platni terminal, u implementaciji nazvan *transaktron*, je također zasebna aplikacija koja simulira bankomat, POS-uređaj ili neki drugi oblik servisa za plaćanje. U prvom koraku korisnik odabire identifikacijski podatak (broj kartice), a u drugom unosi PIN, kao što je prikazano na slici 6.3.



Slika 6.3: Grafičko sučelje platnog terminala.

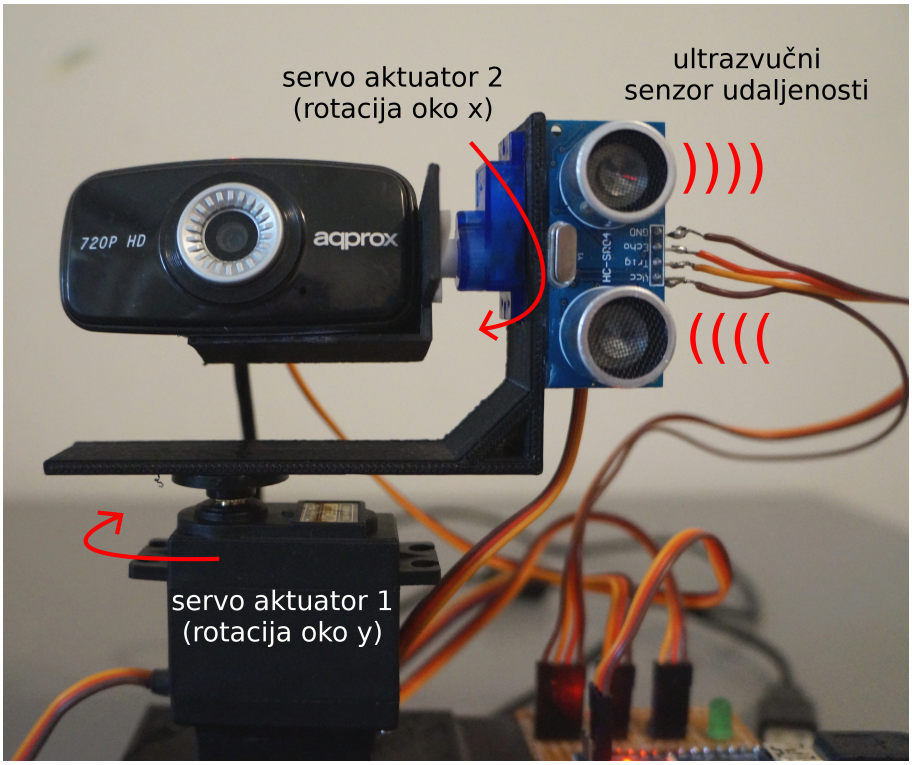
Nakon odabira identifikacijskog podatka, terminal pokreće modul za detekciju lica i uzimanje uzoraka. Taj modul zasebni je dio koda implementiran u C++ programskom jeziku zbog efikasnosti i brzine. Modul također komunicira s hardverskim sklopovljem koje zakreće kameru prema licu korisnika i prati ga dok se pribavi dostatna količina uzoraka - u implementaciji je određeno da se uzima 5 uzastopnih uzoraka kako bi se povećale šanse za valjanu autentikaciju. Konačno, nakon slanja uzoraka i PIN-a, autentikacijski servis vraća rezultat koji može biti uspješna autentikacija, neuspješna autentikacija ili čekanje na potvrdu tokenom (prikaz 6.4).



Slika 6.4: Primjeri poruke o rezultatu transakcije.

6.4 Senzor za prilagođeno uzimanje uzoraka lica

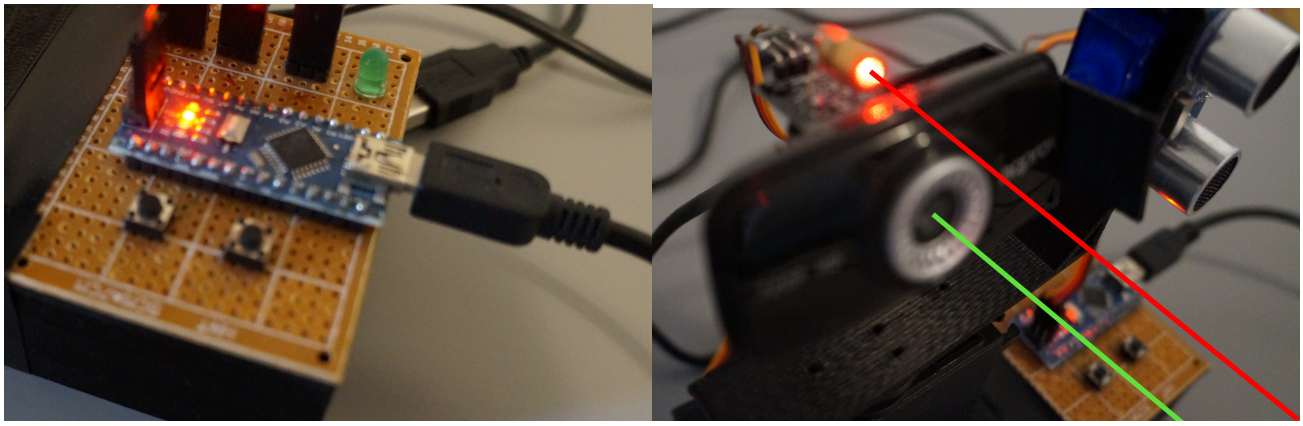
U poglavlju rada gdje se raspravljalo o prilagođenom uzimanju uzorka slike opisan je model uređaja za istu namjenu. Za svrhe testiranja napravljen je prototip uređaja opisanog u modelu (prikaz 6.5).



Slika 6.5: Uređaj za prilagođeno uzimanje uzoraka.

Princip rada konkretnog uređaja je sljedeći; detekciju objekata na video snimci u realnom vremenu, kao i njeno usmjeravanje, prema opisu iz modela, obavlja, u slučaju prototipa, računalo ili računalni sustav platnog terminala, dok mikrokontroler, elektronički sklop na uređaju, u komunikaciji s računalom upravlja s oba servo aktuatora (motora) koja pomiču objektiv kamere, lasersku diodu i ultrazvučni senzor udaljenosti. U slučaju da se lice osobe inicijalno ne nalazi u kadru, platni terminal inicira pronalaženje najbližeg objekta putem ultrazvučnog senzora, a kada je najbliži objekt pronađen, kamera se pomiče vertikalno i pokušava detektirati lice. Po pronalasku lica (prikaz 6.6), platni terminal uzima uzorke, a transakcija se nastavlja. Sva komunikacija između računalnog sustava i mikrokontrolera obavlja se putem serijskih portova uređaja.

Slika 6.6: Pronalazak i usmjeravanje objektiva prema licu.



Slika 6.7: Slika elektroničke pločice s tipkalima, led diodom za signalizaciju i konektorima (desno) i laserske diode povrh objektiva (lijevo). Pravac laserske zrake usklađen je s centrom slike koju kamera pokriva kako bi se lakše demonstriralo praćenje objekata u prostoru.

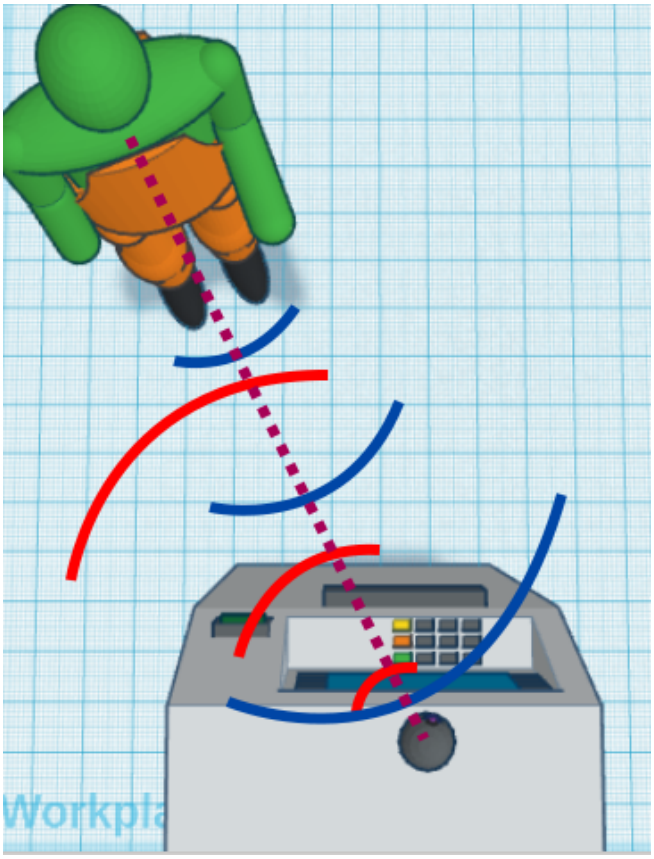
U sljedećem isječku programskog koda prikazan je jednostavni mehanizam upravljanja pomoću serijskog porta između računala i mikrokontrolera. Pogonski program dobiva instrukcije o pomicanju objektiva od računala, te ih izvršava pozivanjem funkcija za pogon motora.

Programski kod Čitanje sa serijskog ulaza i pomicanje prema primljenim instrukcijama

```
switch (Serial.read()) {
case 1:
moveRight(servoLR.read());
break;
case 2:
moveLeft(servoLR.read());
break;
case 3:
moveUp(servoUD.read());
break;
...
```

6.4.1 Pronalaženje osobe pomoću ultrazvučnog senzora

U modelu je definiran opći princip pronalaženja osobe u prostoru. U ovom prototipu taj će se princip konkretizirati rotacijom ultrazvučnog senzora udaljenosti za kut detekcije, kreirajući tako sonar kratkog dometa (prikaz 6.8).



Slika 6.8: Ilustracija pronalaženja osobe pomoću mjerenja udaljenosti ultrazvukom.

Mjerenje udaljenosti moguće je zbog valnih svojstava zvuka u nekom mediju, a pogotovo se ovdje misli na svojstvo odbijanja valova od nekog predmeta i vraćanju vala ka izvoru. Medij je u ovom slučaju zrak, a kako brzina širenja zvuka u zraku na uobičajenim temperaturama neznatno varira, tj. moguće je za ovu namjenu uzeti konstantnu vrijednost (343 m/s na 20 °C), lako je odrediti i samu udaljenost (Elecfreaks, 2017):

$$s[m] = \frac{\Delta t[s] \times 343[m/s]}{2}, \tag{6.1}$$

gdje je $\Delta t[s]$ apsolutna vrijednost razlike u vremenu odašiljanja i primanja odaslanog zvuka.

Budući da senzor mjeri samo određeni kut, potrebno ga je rotirati kako bi se pokrio prostor kojeg se želi skenirati. Konkretno, u hipotezi H2 rada postavljen je kut od 120°, kao kut izvan kojeg nije moguće koristiti uređaj. Kada se odredi najbliža točka, objektiv se rotira u smjeru iste.

Programski kod Funkcija za određivanje udaljenosti

```
int getDistance(){

        long returnTime;

        // Puštanje zvuka na 10us
        digitalWrite(sonarTrigger, HIGH);
        delayMicroseconds(10);
        digitalWrite(sonarTrigger, LOW);

        // Čekanje na povratak zvuka i mjerenje vremena
        returnTime = pulseIn(sonarEcho, HIGH);

        // Vraćanje udaljenosti u cm
        return returnTime*0.034/2;
}
```

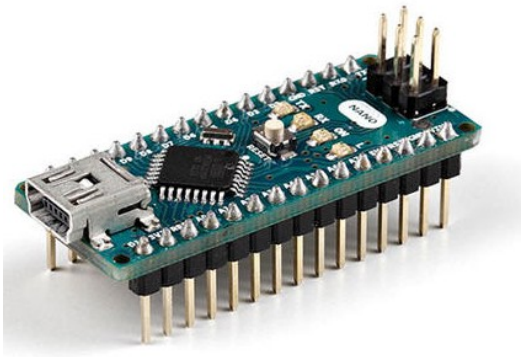
6.4.2 Tehnička specifikacija komponenti

Pomični senzor realiziran je pomoću sljedećih komponenti:

- Arduino Nano - *integrirani elektronički sklop (mikrokontroler)*,
- Approx APPWC03HD 720p HD - *web kamera*,
- TowerPro MG995 55g - *servo aktuator*,
- TowerPro SG90 9g - *servo aktuator*,
- HC-SR04 - *ultrazvučni senzor udaljenosti*,
- Keyes KY-008 - *laserska dioda (650nm, 5mW) (slika 6.7)*,
- PCB pločica za prototipiranje (5 × 7cm) (slika 6.7),
- 2x tipkala (prekidači),
- led dioda, i
- trožilni i četverožilni kablovi.

Arduino Nano

Arduino Nano (slika 6.9) dio je obitelji Arduino mikrokontrolera. Arduino je otvorena platforma za kreiranje elektroničkih prototipova široke namjene. U srcu platforme je mikročip ATmega328 - 8-bitni mikrokontroler baziran na RISC arhitekturi s frekvencijom od 16 MHz, 32 opća registra i integriranim Flash (32KB), SRAM (2KB) i EEPROM (1KB) memorijama za pohranu programa i podataka (Zenzerović, 2015).



Slika 6.9: Arduino Nano mikrokontroler.

U tablici 6.1 dana je detaljna tehnička specifikacija mikrokontrolera preuzeta sa stranica proizvođača (https://www.arduino.cc/en/Main/ArduinoBoardNano).

Tablica 6.1: Detaljna tehnička specifikacija Arduino Nano mikrokontrolera

Mikrokontroler	ATmega328
Arhitektura	AVR RISC
Radni napon	5 V
Flash memorija	32 KB (2KB se koriste za bootloader)
SRAM	2 KB
Takt procesora	16 MHz
Analogni I/O pinovi	8
EEPROM	1 KB
DC snaga po I/O pinu	40 mA
Ulazni napon	7-12 V
Digitalni I/O pinovi	22
PWM izlazi	6
Potrošnja	19 mA
PCB veličina	18 x 45 mm
Masa	7 g

Approx APPWC03HD 720p HD

Za uzimanje uzoraka iskorištena je HD web kamera. Razlog korištenja specifičnog modela (APPWC03HD) je laka ugradbenost, kvaliteta slike i niska cijena. Maksimalna rezolucija kamere iznosi 1280 × 720 px uz 30 sličica u sekundi (FPS), što su dostatne performanse za realizaciju ovog prototipa.

Slika 6.10: Approx APPWC03HD.

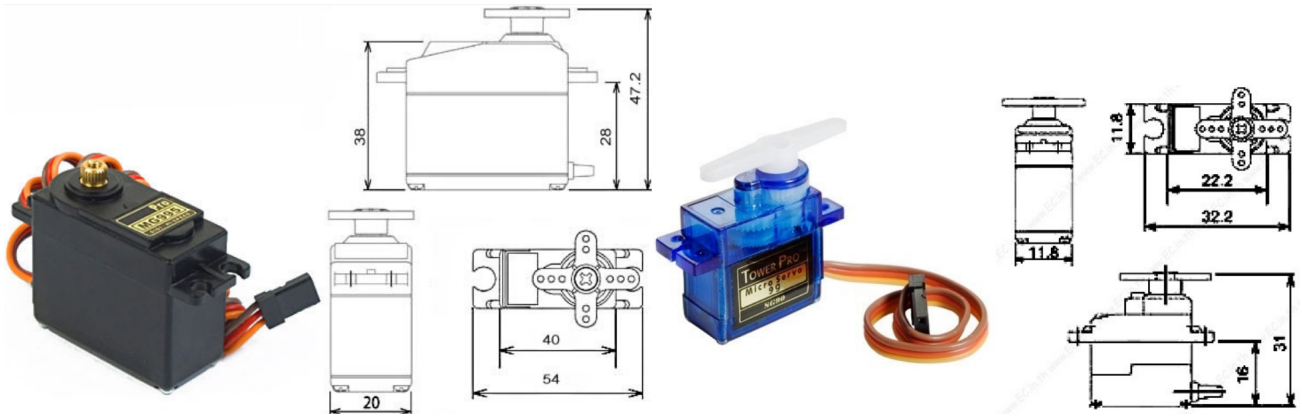
U tablici 6.2 dana je detaljna tehnička specifikacija web kamere preuzeta sa stranica (https://www.amazon.es/Approx-APPWC03HD-WebCam-color-plateado/dp/B00N3NVK32).

Tablica 6.2: Detaljna tehnička specifikacija Approx APPWC03HD 720p HD

Video rezolucija	1280 x 720 px
Sličica u sekundi	30
Fotografije	2 Mpx
Ulazni napon	5 V
PCB veličina	2,5 x 6,3 x 13 cm
Masa	82 g

TowerPro MG995 i SG90 servo aktuatori

Za rotacije objektiva, lasera i senzora udaljenosti korištena su dva aktuatora, TowerPro MG995 i TowerPro SG90. Oba aktuatora rade po istom principu, s time da MG995 ima veću snagu, što je i razlog njegove uporabe. Naime, kako aktuator koji senzore rotira po y osi mora nositi gotovo cijelu konstrukciju i elektroniku iznad sebe, bilo je potrebno uporabiti motor veće snage. Za rotaciju objektiva po x osi bio je dovoljan slabiji model - SG90, jer isti zakreće samo nosač i objektiv kamere. Posebnost servo aktuatora je mogućnost okretanja osovine motora u obje strane. Unatoč tome maksimalni kut zakretanja je ograničen.



Slika 6.11: Aktuatori MG995 (lijevo) i SG90 (desno).

U tablici 6.3 dana je detaljna tehnička specifikacija navedenih aktuatora preuzeta sa stranica proizvođača (http://www.electronicoscaldas.com/datasheet/MG995_Tower-Pro.pdf, http://www.micropik.com/PDF/SG90Servo.pdf).

Tablica 6.3: Detaljna tehnička specifikacija aktuatora

Model	**MG995**	**SG90**
Masa	55g	9g
Maksimalni zakret	120^o	180^o
Maksimalni moment	8.5 Ncm (4.8V), 10 Ncm (6V)	1.8 Ncm
Dimenzije	40.7 x 19.7 x 42.9 mm	22.2 x 11.8 x 31 mm
Maksimalna brzina	0.2 s/60^o (4.8V), 0.16 s/60^o (6V)	0.1 s/60^o
Maksimalna radna temperatura	55 ^{o}C	55 ^{o}C
Ulazni napon	4.8 - 7.2V	5V

HC-SR04 senzor udaljenosti

Senzor udaljenosti koristi se za aproksimaciju pozicije osobe u prostoru mjerenjem udaljenosti okoline pod različitim kutevima. Senzor se sastoji od odašiljača i primatelja putem kojih se određuje udaljenost.

Slika 6.12: HC-SR04 senzor udaljenosti

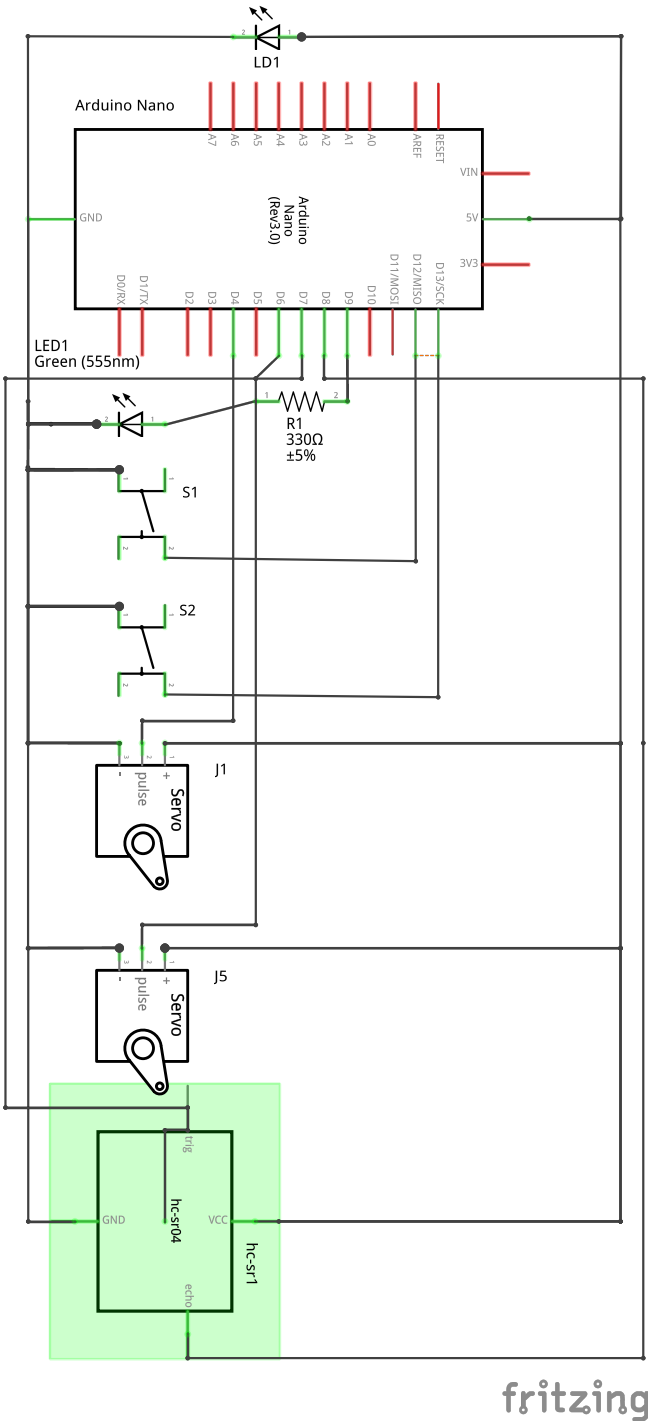
U tablici 6.4 dana je detaljna tehnička specifikacija HC-SR04 senzor preuzeta sa stranica proizvođača (http://www.micropik.com/PDF/HCSR04.pdf).

Tablica 6.4: Detaljna tehnička specifikacija HC-SR04

Frekvencija zvuka	40 kHz
Snaga	15 mA
Maksimalna udaljenost	4 m
Minimalna udaljenost	2 cm
Kut vala	15^o
Minimalno vrijeme odašiljanja	10 μs
Ulazni napon	5 V
Dimenzija	45 x 20 x 15 mm

6.4.3 Elektronička shema

Prikaz 6.13 opisuje elektroničku shemu spajanja gore navedenih komponenti s mikrokontrolerom.

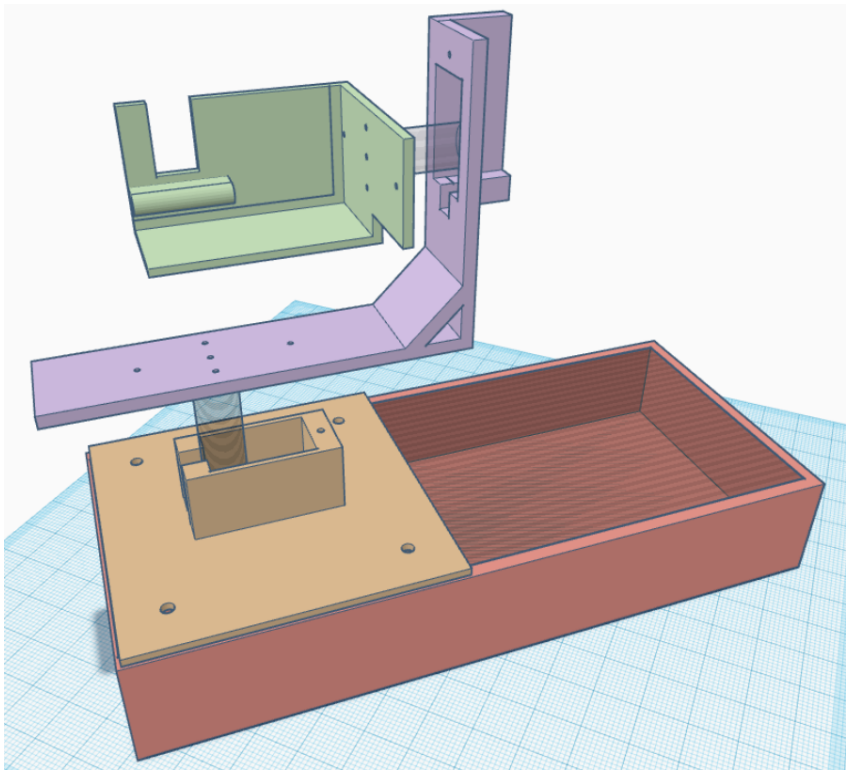


Slika 6.13: Elektronička shema pomične kamere.

6.4.4 Konstrukcija uređaja

Da bi uređaj mogao biti funkcionalan, bilo je potrebno konstruirati kućište u koje će se moći ugraditi elektroničke komponente i pomoću kojega će se moći vršiti funkcije zakretanja. U svrhu toga napravljen je 3D model (prikaz 6.14) iz sljedećih dijelova:

- baza kućišta (crvena) - *sadrži elektroniku i utege koji uređaj za vrijeme rotiranja drže na mjestu*,
- nosač konstrukcije (žuta) - *ugrađuje motor i podržava gornju konstrukciju*,
- rotacijski okvir (ljubičasta) - *montira se na donji motor, ugrađuje motor za x rotaciju, podržava objektiv, njegov nosač i senzor udaljenosti, rotira se po* y,
- nosač objektiva (zelena) - *podržava objektiv kamere i lasersku diodu iznad objektiva, rotira se po* x.



Slika 6.14: 3D model printane konstrukcije.

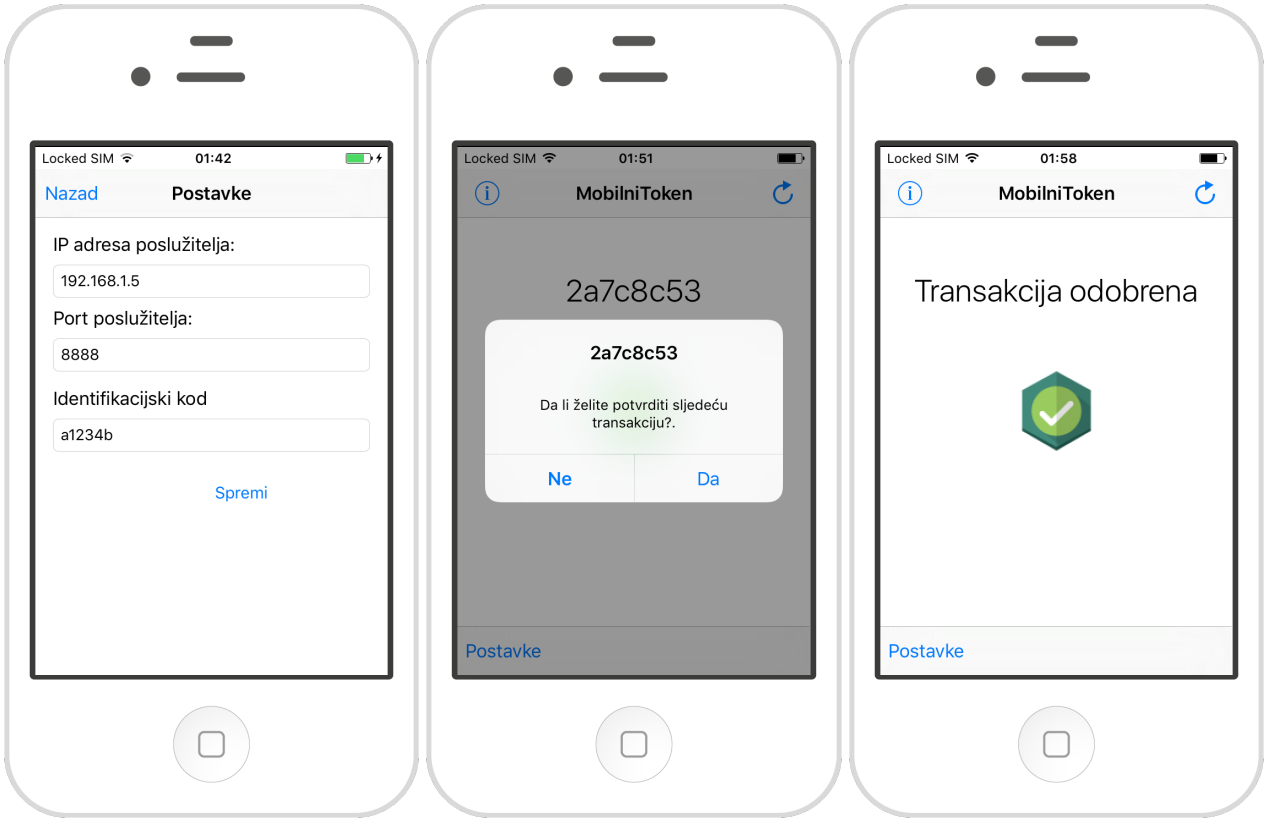
Print modela napravljen je putem 3D printera s filamentom od ABS plastike. Konačno, na konstrukciju su montirane i elektroničke komponente. Spajanje 3D printanih dijelova s elektronikom napravljeno je s adhezivnim sredstvom za plastiku.

6.5 Token

Mobilni token aplikacija je za mobilne uređaje koja komunicira s autentikacijskim servisom i dopušta transakciju ako verifikacija lica propadne.

Prije nego što se aplikacija može koristiti na mobilnom uređaju, uređaj valja registrirati u platnom sustavu. Registracija se odvija tako da se korisniku da tajni registracijski kod, a po njegovim unosu u mobilnu aplikaciju ista autentikacijskom servisu šalje unikatni identifikator uređaja, tzv. UDID, čime se onemogućuje da drugi uređaj preuzme ulogu mobilnog tokena (7.1).

Na istoj slici može se primijetiti da je moguće unijeti IP adresu i port autentikacijskog servisa. Ovo zapravo u stvarnoj aplikaciji ne bi bilo prisutno, no zbog fleksibilnosti i mogućnosti kasnijih promjena je ostavljeno.



Slika 6.15: Unos aktivacijskog koda i ostalih parametara (lijevo), upit za odobrenjem transakcije (sredina) i status izvršenja transakcije (desno).

7 Testiranje

Nažalost, u trenutku pisanja rada nije bilo resursa da se cjelokupni implementirani sustav testira sa stvarnim korisnicima te da se prikupe korisnička iskustva i mišljenja, koja bi su svakom slučaju bila važan element u odlučnosti implementacije u stvarnom svijetu. Unatoč tome, u svrhe potvrde zadanih hipoteza, testiranje sustava temeljeno je na provjeri točnosti prepoznavanja algoritmom implementiranim u prototipu sustava (LBPH) te provjeri rada uređaja za olakšano uzimanje uzoraka. Ovakvi rezultati testiranja bi nam u tehničkom pogledu trebali odgovoriti na pitanje o potvrdi hipoteza te da li je implementaciju sustava moguće primijeniti u praksi.

7.1 Testiranje algoritma prepoznavanja

Kako bi rezultati testiranja bili što objektivniji i reprezentativniji, korištena je već pripremljena baza uzoraka lica - *The Extended Yale Face Database B*, preuzeta sa http://vision.ucsd.edu/~iskwak/ExtYaleDatabase/ExtYaleB.html. Navedena baza sadrži 65 uzoraka lica za 38 osoba, tj. 2470 uzoraka lica ukupno. Uzorci osoba razlikuju se prema raznim uvjetima iluminacije - potpuno vidljivo lice parcijalno zatamnjenje i potpuno zatamnjenje. Set fotografija za jednu osobu podijeljen je na dva dijela; jedan od 32, a drugi od 33 fotografije. Iz kontrolnog seta od 32 fotografije kreirana je YML baza LBPH histograma putem implementiranog softvera.

Dakle, imamo:

- set svih 2470 fotografija 38 osoba (*ukupni set*),
- set fotografija za pojedinu osobu (*yaleBN*, $N \in 01, \ldots, 39$), koji je podijeljen na dva podseta:
  - set od 32 originalne fotografije lica koje su korištene u kreiranju baze histograma (*kontrolni set*),
  - set od 33 fotografije na kojima je ista osoba kao i u kontrolnom setu, iako su fotografije različite (*pozitivni set*), i
- set od 2405 fotografija 37 osoba koje su različite od osobe čiji se set u tom trenutku testira (*negativni set*).

Testiranje implementiranog sustava autenticiranja (LBPH algoritma) napravljeno je na sljedeći način; nakon što su kreirane baze histograma za svaku osobu putem kontrolnog seta, isti taj set je uporabljen

Slika 7.1: Primjeri uzoraka lica kakvi su prisutni u Yale setu.

za testiranje prepoznavanja kako bi se ustvrdilo da sustav korektno prepoznaje sve uzorke. Naime, kod kontrolnog seta očekivana stopa prepoznavanja je 100%, tj. Hi-kvadrat test bi za svaki uzorak u kontrolnom setu trebao rezultirati udaljenošću 0. Nakon toga, isto testiranje ponavljamo prvo s pozitivnim, a onda i s negativnim setom. Pretpostavka je da će pozitivni test, za razliku od kontrolnog, imati manju stopu prepoznavanja, tj. da će Hi-kvadrat test rezultirati udaljenošću većom od 0. Isto tako, pretpostavljamo da će negativni set rezultirati znatno manjom ili čak nepostojećom stopom prepoznavanja, tj. udaljenost uzoraka bi trebala biti isključivo veća nego kod uzoraka u pozitivnom setu.

Potvrda ove pretpostavke značila bi da sustav radi korektno i očekivano. Konačno, dobivenom metrikom mogli bi ustvrditi da li je potvrđena hipoteza H1 iz uvoda rada. S tim u vezi, prilikom testiranja bilježeni su podaci koji će omogućiti donošenje zaključka o gore postavljenim tvrdnjama. Podaci su:

- prosjek svih udaljenosti uzoraka u danom setu (*prosječna udaljenost*),
- maksimalna udaljenost koju je postigao neki uzorak u setu (*maksimalna udaljenost*),
- minimalna udaljenost koju je postigao neki uzorak u setu (*minimalna udaljenost*),
- broj uzoraka čija je udaljenost manja od prosječne udaljenosti pozitivnog seta (*broj manjih*),
- broj uzoraka čija je udaljenost veća od prosječne udaljenosti pozitivnog seta (*broj većih*).

Primijetimo, u posljednja dva podatka u gornjoj listi u obzir se uzima prosječna udaljenosti pozitivnog seta. Naime, ta vrijednost nam je mjerodavna jer simulira uvjete u realnom svijetu, tj. prosječna udaljenosti svih pozitivnih uzoraka trebala bi dati okvirnu vrijednost praga koji bi neki uzorak svrstao kao pozitivno prepoznat ili negativno prepoznat. U stvarnom sustavu vrijednost praga se može skalirati prema politici ili metodi fluktuacije prema visini transakcije.

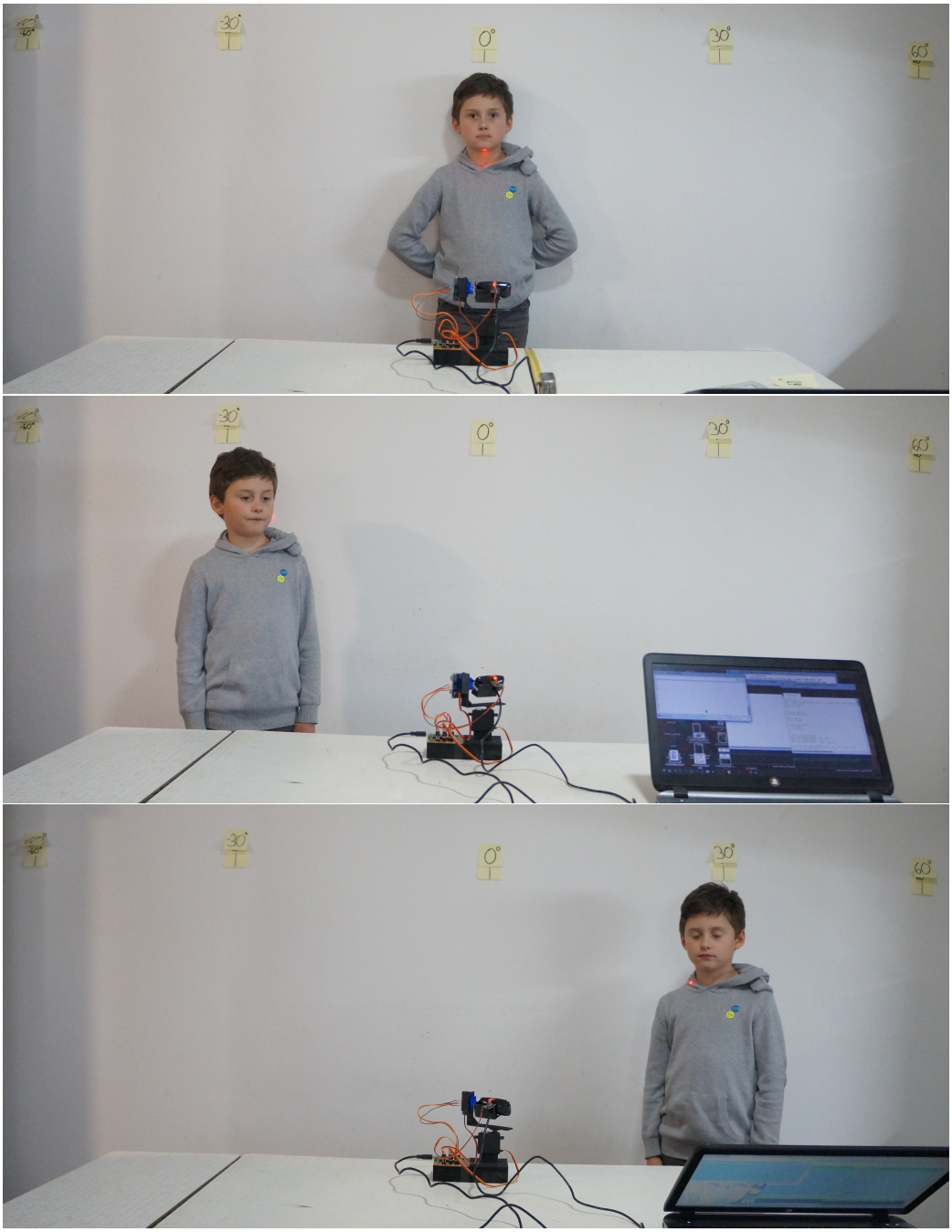
7.2 Testiranje uređaja za olakšano uzimanje uzoraka

Da bi se mogla testirati istinitost hipoteze H2, načinjen je test od dvije komponente. Prva je testiranje pronalazak osobe u prostoru unutar zadanog kuta do 120°, a drugi je detekcija i praćenje lica u kadru.

7.2.1 Testiranje pronalaska osobe u prostoru

Za testiranje je upotrebljen uređaj konstruiran u poglavlju koje opisuje implementaciju prototipa, a test je postavljen na sljedeći način. U zatvorenom prostoru je pomoću kutomjera i laserske projekcije izmjeren kut od 120° uz markere postavljene na: 60°, 30°, 0°, -30° i -60°. U zadanom kutu je potom iscrtan kružni isječak polumjera 100 cm, 50 cm i 25 cm. Uređaj je postavljen u centar kružnice, tj. u vrh kuta.

Osoba (testni subjekt) pomicala se po postavljenim markerima i zadanim polumjerima, što ukupno čini 15 mjernih pozicija. Između svakog pomaka uređaj za uzimanje uzoraka pokušao je pronaći i laserom poentirati na poziciju osobe. Kod testa su se bilježile uspješnost pronalaska, tj. odmak od markera na kojem je osoba stajala. Testiranje je je za svaki marker, odnosno polumjer rađeno 3 puta. Testiranje je prikazano na slici 7.2.



Slika 7.2: Testiranje pronalaska osobe pomoću ultrazvučnog senzora.

7.2.2 Testiranje detekcije i praćenje lica u kadru

I za ovo testiranje korišten je implementirani uređaj, a test se sastojao od sljedećeg. Uređaj je postavljen 1 metar od plohe na kojoj su prezentirani uzorci lica. Na plohi je postavljeno blago zakrivljeno uže duljine 80 centimetara na kojeg je stavljen pomični nosač za fotografije. Uže je namjerno postavljeno blago zakrivljeno kako bi se simulirali horizontalni i vertikalni pomaci lica. Uzeto je 38 fotografija lica iz Yale baze, od svake

osobe po jedna. Iste su stavljene na nosač i vučene konstantnom brzinom (slika 7.3).

Prilikom provođenja testa bilježen je uspjeh pronalaska lica u kadru i uspješnost praćenja od početne do završne točke, tj. za svaku fotografiju provjerilo se može li je uređaj pratiti ili fotografija može izaći iz vidljivog kadra.

Slika 7.3: Testiranje detekcije i praćenja lica u prostoru.

8 Rezultati

U poglavlju koje slijedi izloženi su rezultati testiranja i njihova interpretacija. Također, navedene su napomene koje bi se uz dobivene rezultate trebale uzeti u obzir kako bi se mogle procijeniti stvarne performanse budućeg sustava temeljnog na ovom modelu. U zaključku su ovi rezultati uspoređeni s predviđanjima u hipotezama i ciljevima rada.

8.1 Rezultati testiranja algoritma prepoznavanja

Rezultati, prema gore navedenim smjernicama, prikazani su u tablici 8.1. Ovi rezultati sumiraju rezultate za sve dobivene setove, dok su u dodatku A prikazani rezultati za svaki set zasebno. Sumirani rezultati dobro opisuju populaciju dobivenih rezultata, u što se možemo uvjeriti uvidom u zasebne rezultate. Stoga će se sumirane rezultate koristiti u daljnjoj interpretaciji. Za bolju predodžbu dobivenih vrijednosti, na slici 8.1 prikazani su rezultati za svaki pojedini uzorak te skupno u obliku histograma za setove yaleB02, yaleB22 i yaleB32.

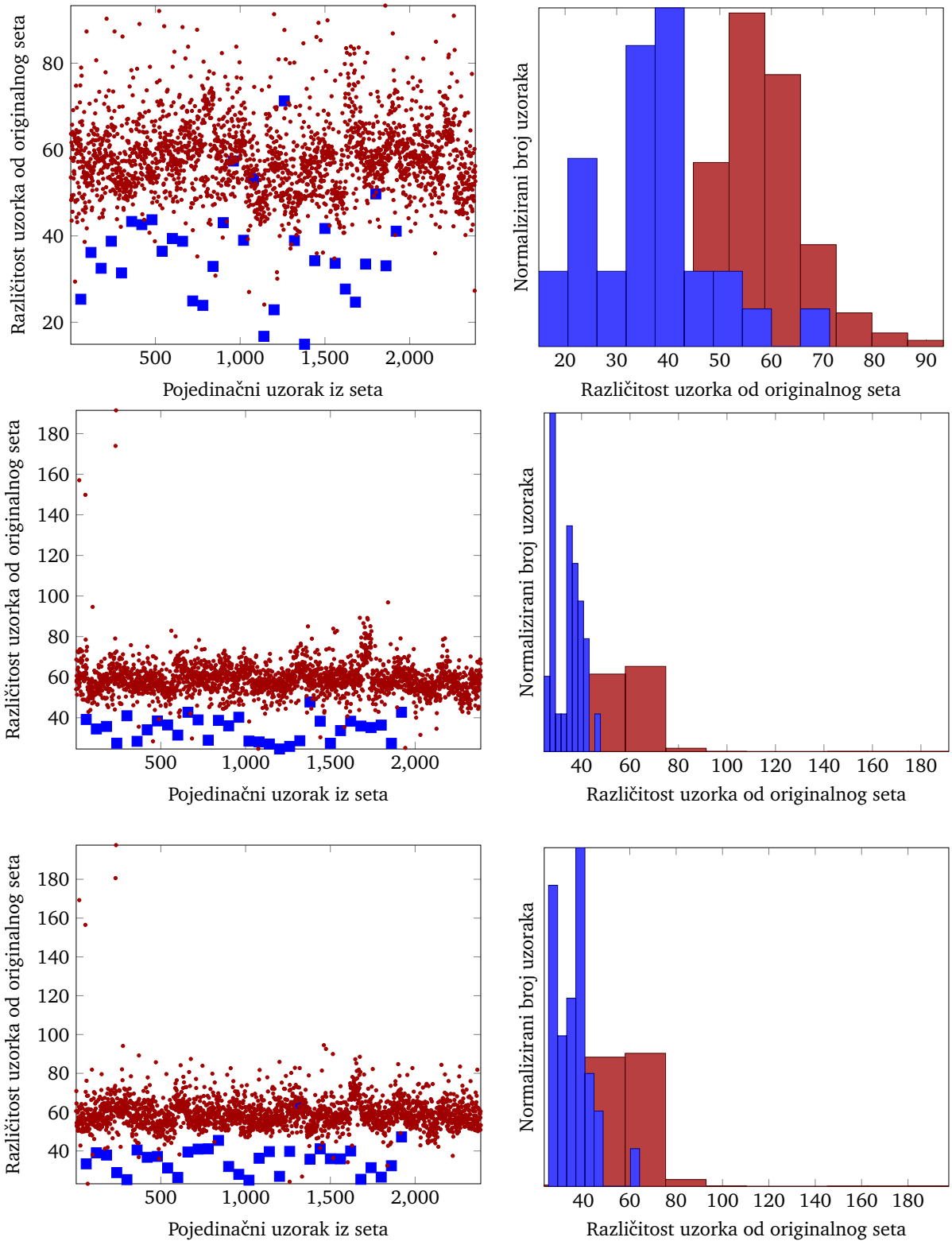
Tablica 8.1: Rezultati testiranja LBPH algoritma.

	Originalni set	**Pozitivni set**	**Negativni set**
prosječna udaljenost	0	**37.6740299879**	56.5236755275
maksimalna udaljenost	0	129.578582767	198.944277206
minimalna udaljenost	0	13.3318214046	7.13393216202
broja manjih	1243 (100%)	684 (56.5756824%)	287 (0.3163441%)
broj većih	0	525 (43.4243176%)	90437 (99.6836559%)

Kako je bilo moguće i pretpostaviti, originalni set u potpunosti je prošao testiranje, tj. udaljenost svih uzoraka lica manja je od prosjeka i iznosi 0. Ovime potvrđujemo korektnost rada implementacije algoritma.

Što se tiče pozitivnog seta, koji je zapravo mjerodavni test, prosječna udaljenost iznosila je približno 37.67. Ako bi za vrijednost praga uzeli prosjek pozitivnog seta, tada bi korisnik u cca. 56.57% slučajeva bio prihvaćen kao valjan, a u ostalih cca. 43.42% odbijen kao nevaljan (FRR). Gledajući apsolutno, na 1000 transakcija korisnik bi bio uspješno autenticiran 565 puta, dok bi 434 puta morao koristiti dodatne opcije autentikacije.

Kod negativnog seta, prosječna udaljenost iznosila je cca. 56.52, dok je broj manjih vrijednosti od prosjeka pozitivnog seta bio 0.31% (FAR). Odbačenih je u negativnom setu 99.68%. Gledajući apsolutno, na 1000 transakcija, 996 pokušaja zlouporabe bilo bi neuspješno, dok bi 31 pokušaj bio uspješan.



Slika 8.1: Grafički prikaz rezultata za za pozitivne (plavo) i negativne (crveno) setove usporedno. Lijevi graf prikazuje različitost uzoraka za svaki uzorak pojedinačno, dok desni graf pokazuje normalizirani histogram uzoraka prema različitost. Grafovi prikazuju rezultate za setove yaleB02, yaleB22 i yaleB32 respektivno.

8.2 Rezultati testiranja uređaja pronalaska osobe u prostoru

Tablica 8.2 prikazuje rezultate testiranja pronalaska osobe u prostoru. U tablici su navedeni kutevi za koje se pouzdanost (odmak od markera u stupnjevima) mjerila te udaljenost od senzora. Za svaku točku mjerenja su zbog pouzdanosti rađena 3 puta, pa je i svako pojedinačno mjerenje prikazano u tablici.

Tablica 8.2: Rezultati testiranja pronalaska osobe u prostoru

Kut/Udaljenost	25 cm			50 cm			100 cm		
	Odmak od markera cca.								
Mjerenja	I	II	III	I	II	III	I	II	II
60°	5°	17°	2°	12°	35°	20°	20°	23°	15°
30°	7°	2°	6°	68°	10°	12°	10°	4°	40°
0°	0°	2°	2°	10°	7°	2°	60°	7°	5°
-30°	12°	30°	10°	3°	0°	15°	2°	5°	13°
-60°	25°	10°	8°	8°	20°	22°	52°	20°	10°

U tablici 8.3 izračunati su i prosječni odmaci za sva tri testiranja, kako bu de mogao utvrditi trend točnosti u ovisnosti o kutu i udaljenosti.

Tablica 8.3: Prosječni odmak od markera prema tablici 8.2

Kut/Udaljenost	25 cm	50 cm	100 cm
	Prosjek odmaka u stupnjevima		
60°	8	22.3333333333	19.3333333333
30°	5	30	18
0°	1.3333333333	6.3333333333	24
-30°	17.3333333333	6	6.6666666667
-60°	14.3333333333	16.6666666667	27.3333333333

8.3 Rezultati testiranja detekcije i praćenje lica u kadru

Kako se može vidjeti iz tablice 8.4, sve slike lica uspješno su detektirane u kadru, tj. detekcija lica za 38 uzoraka iznosi 100%, dok je praćenje lica izvršeno je s uspješnošću od 89.4736842%, tj, 4 od 38 uzoraka nije uspješno praćeno do završne točke.

Tablica 8.4: Rezultati testiranja detekcije i praćenja lica.

Fotografija iz seta	Lice detektirano	Uspješno praćeno
yaleB01	Da	Da
yaleB02	Da	Da
yaleB03	Da	Da
yaleB04	Da	Da
yaleB05	Da	Da
yaleB06	Da	Ne
yaleB07	Da	Da
yaleB08	Da	Da
yaleB09	Da	Da
yaleB10	Da	Da
yaleB11	Da	Da
yaleB12	Da	Da
yaleB13	Da	Ne
yaleB15	Da	Da
yaleB16	Da	Da
yaleB17	Da	Da
yaleB18	Da	Da
yaleB19	Da	Da
yaleB20	Da	Da
yaleB21	Da	Da
yaleB22	Da	Da
yaleB23	Da	Da
yaleB24	Da	Da
yaleB25	Da	Da
yaleB26	Da	Da
yaleB27	Da	Da
yaleB28	Da	Da
yaleB29	Da	Da
yaleB30	Da	Da
yaleB31	Da	Ne
yaleB32	Da	Da
yaleB33	Da	Ne
yaleB34	Da	Da
yaleB35	Da	Da
yaleB36	Da	Da
yaleB37	Da	Da
yaleB38	Da	Da
yaleB39	Da	Da

8.4 Interpretacija rezultata

Prije no što se donese konačno mišljenje o dobivenim rezultatima, uzmimo nekoliko stvari u obzir. Rezultati dobiveni u ovom testiranju ne mogu biti ogledalo performansi stvarnoga sustava već su samo pokazatelj izvedivosti. Također, dobiveni rezultati pod jakim su utjecajem tehničke izvedbe pa ih se stoga ne može uzeti kao generalno mjerodavne za implementirane algoritme i metode. Osim toga:

- u setovima je polovina uzoraka bilo parcijalno, ili skoro u potpunosti zamračeno, dok bi stvarni sustav posjedovao tehnologiju koja bi eliminirala promjene iluminacije (dodatno osvjetljenje), ili bi se prilagodba tražila od korisnika,
- u setovima su uzorci poprilično dobre kvalitete, dok kvaliteta uzoraka uzetih korisničkim kamerama ili kamerama na POS uređajima i bankomatima može varirati.

Testiranje prepoznavanja polučilo je dobre rezultate, pogotovo u pogledu eliminacije lažnih korisnika. Kao problem nameće se broj valjanih korisnika koji bi se mogli autenticirati, no ovo nije toliko zabrinjavajuće, budući da je za granicu uzeta vrlo sigurna aritmetička sredina valjanih uzoraka. Pomicanjem te granice prihvatljivosti sustav se može ugoditi tako da bude siguran, ali i upotrebljiv za većinu korisnika. Svakako, u svrhu sekundarne autentikacije moguć je mobilni token pa stoga nema zabrinutosti za nemogućnost vršenja transakcije.

Kod testiranja pronalaženja osobe u prostoru, može se primijetiti generalna korelacija porasta odmaka od markera u proporciji sa udaljenošću od senzora. U nekim slučajevima, kao što je to kod $-30°$, postoji i neslaganje s tim pravilom, što nam ukazuje na probleme s tehničkom izvedbom. Unatoč tome, kao što je iz rezultata vidljivo, senzor u većini slučajeva ipak može odrediti poziciju osobe unutar 1 metra u $120°$ pa je stoga i metoda predstavljena u modelu valjana.

Testiranje detekcije i praćenja pokazalo je da i ovaj rani prototip nudi iznimno dobre rezultate pa onda i ovu funkcionalnost modela označavamo kao valjanu.

Konačno, uzevši sve navedeno u obzir, zaključujemo da se implementacija sustava može dalje razmatrati. U zaključnom poglavlju navest će se pravac daljnjeg istraživanja u svrhu poboljšavanja ovih rezultata.

9 Zaključak

U uvodu rada postavljene su sljedeće hipoteze čije će se potvrđivanje sada zaključno razmotriti.

Hipoteza 1 (H1) - *Uvođenjem biometrijske provjere lica u platni sustav, kao dodatne mjere verifikacije, maliciozni korisnici bit će prepoznati u više od 90% slučajeva.*

Kod testiranja prototipa uzeta je sigurna granica aritmetičke sredine pozitivnog seta uzoraka, što je, sumiravši sve rezultate testiranja rezultiralo time da su uzorci malicioznih korisnika prepoznati u 99% slučajeva. Iako je uzeta ovako striktna granica, jasno je da se ista može spustiti do razine gdje se omogućuje da se više valjanih korisnika može autenticirati, što je i predstavljeno metodom fluktuacije granice prihvatljivosti u ovisnosti o visini transakcije. Ovim razmatranjem potvrđujemo hipotezu H1.

Hipoteza 2 (H2) - *Konstruirani pomični senzor pronalazi položaj osobe izvan vidljivog polja kamere, unutar kuta od 120° i udaljenosti 1 metra te prepoznaje i prati pomake lica do udaljenosti od 1 metra.*

Za testiranje hipoteze H2 osmišljeni su testovi koji se direktno tiču izjava od kojih je hipoteza sačinjena, a to su:

1. "*konstruirani pomični senzor pronalazi položaj osobe izvan vidljivog polja kamere, unutar kuta od 120° i udaljenosti 1 metra*", i
2. "*prepoznaje i prati pomake lica do udaljenosti od 1 metra*".

Kod testiranja prve izjave, "*konstruirani pomični senzor pronalazi položaj osobe izvan vidljivog polja kamere, unutar kuta od 120° i udaljenosti 1 metra*", test je pokazao kako konstruirani senzor uspješno pronalazi položaj, ali uz određena odstupanja. Kako hipoteza rada ne propisuje granice dozvoljenih odstupanja, prvenstveno jer se radi o vrlo ranom prototipu, isti neće utjecati na njenu potvrdu,

Testiranje druge izjave, "*konstruirani pomični senzor pronalazi položaj osobe izvan vidljivog polja kamere, unutar kuta od 120° i udaljenosti 1 metra*", također je potvrđeno prezentiranim rezultatima, gdje je uspješnost ovoga testa pokazala većom od 89%.

Sukladno dobivenim rezultatima i njihovoj interpretaciji, može se potvrditi da su, uz razmatranja i pretpostavke navedene u radu, hipoteze H1 i H2 potvrđene.

Dizajnom sustava pokazano je da integracija ovakvog sustava u postojeći platni sustav nije jako složeni zadatak, naprotiv, današnja je tehnologija na dovoljno visokoj razini, a biometrijska znanost dostatno razvijena pa se nameće zaključak da jedino što je potrebno za uvođenje ovakvog sustava je volja njegovih glavnih aktera, korisnika i financijskih ustanova.

Iako je već napomenuto, glavni doprinos ovoga rada očituje se u osmišljenom modelu povećanja sigurnosti u platnom sustavu koji vodi posebnu brigu za prilagođenost korisnicima i jednostavnost korištenja. S tim uvezi, specifični doprinosi rada jesu:

- *cjelokupnost rješenja u globalnom platnom sustavu,*
- *dizajn biometrijskog autentikacijskog podsustava za karakteristiku lica,*
- *olakšavanje uzimanja uzoraka lica pomoću modela rotirajućeg senzora,*
- *upravljanje sigurnošću u pogledu fluktuacije prihvatljivosti uzoraka u skladu s visinom transakcije.*

Prvi od problema koji bi se mogao pojaviti jest privola korisnika. Naime, potrebno bi bilo provesti preliminarno istraživanje tržišta i testni sustav uvesti za manji dio korisnika. Ovo bi nam omogućilo da se dođe do mišljenja korisnika o tome da li bi sustav bio prihvatljiv, a ujedno bi se ukazalo na probleme koji nisu bili razmotreni i znani tijekom dizajna i implementacije.

Sljedeći problem je i korektnost rada sustava. Rezultati testiranja pokazali su da bi trenutna implementacija u nešto manje od polovine slučaja odbacila valjanog korisnika. Da bi se ovo izbjeglo, potrebno je razmotriti korištenje više metoda za provjeru lica, čime bi se onda odgovornost rasteretila s jedne metode na više njih, a konačna odluka donosila bi se konsenzusom. S tim u vezi, treba razmotriti i korištenje metoda umjetne inteligencije koje bi svakako mogle dati doprinos radu sustava.

U konačnici, valja spomenuti kako je jedan od najvažnijih faktora zapravo isplativost integracije. Ako se uvođenje ovakvog sustava ne bi pokazalo isplativim, teško bi bilo za pretpostaviti da bi ga financijske institucije uopće razmotrile. Ujedno je o ovoj temi i najteže govoriti jer na to utječe i veliki broj drugih faktora.

U opisu trenutnog platnog sustava navedeno je da je šteta koja se nanosi neovlaštenim transakcija iznosi više od 6 milijardi američkih dolara samo za europsko i američko tržište. Također, spomenuto je i to da je uvođenjem EMV zaštite broj neovlaštenih transakcija pao. Prema tome, može se naslutiti kako će uvođenjem provjere korisnika, taj iznos svakako i dalje opadati, naravno, uz pretpostavku da će se sam sustav i dalje razvijati.

Ono što kod razmatranja isplativosti svakako treba uzeti u obzir su i nemjerljive beneficije uvođenja sustava, a to su prije svega veći osjećaj sigurnosti kod korisnika, razvitak i stjecanje iskustva u području primjene biometrije, a naposljetku globalni razvoj unifikacija platnog sustava.

Literatura

[Ahonen et al. 2006] AHONEN, Timo ; HADID, Abdenour ; PIETIKAINEN, Matti: Robust Real-time Object Detection. Iz: *IEEE transactions on pattern analysis and machine intelligence* (2006). – URL http://ieeexplore.ieee.org/document/1717463/. – Posjećeno 16.08.2016.

[American Express Company 2012] AMERICAN EXPRESS COMPANY: *American Express Announces U.S. EMV Roadmap to Advance Contact, Contactless and Mobile Payments*. 2012. – URL http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx. – Posjećeno 15.08.2016.

[Authorize.Net LLC 2015] AUTHORIZE.NET LLC: *What data is stored on a payment card's magnetic stripe?* 2015. – URL http://go.2checkout.com/payment-system-simplified. – Posjećeno 17.03.2016.

[Bača 2015] BAČA, Miroslav: *Bilješke sa predavanja iz kolegija Odabrane teme iz biometrije, poglavlje: Uvod*. 2015. – URL http://elfarchive1415.foi.hr/pluginfile.php/60358/mod_resource/content/1/otb_1.pdf. – Posjećeno 16.08.2016.

[Bača et al. 2006] BAČA, Miroslav ; ČUBRILO, Mirko ; RABUZIN, Kornelije: Using Biometric Characteristics to Increase ITS Security. Iz: *Promet - Traffic & Transportation* (2006). – URL http://www.fpz.unizg.hr/traffic/index.php/PROMTT/article/view/970/820. – Posjećeno 17.08.2016.

[Business Insider, Inc 2017] BUSINESS INSIDER, INC: *Samsung S8 will use facial recognition for payments*. 2017. – URL http://www.businessinsider.com/samsung-s8-will-use-facial-recognition-for-payments-2017-3. – Posjećeno 26.03.2017.

[CARNet CERT i LS&S 2003] CARNET CERT ; LS&S: *Upravljanje sigurnosnim rizicima*. 2003. – URL http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf. – Posjećeno 06.07.2016.

[CARNet CERT i LS&S 2006] CARNET CERT ; LS&S: *Biometrija*. 2006. – URL http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-167.pdf. – Posjećeno 16.08.2016.

[Datta et al. 2016] DATTA, Asit K. ; DATTA, Madhura ; BANERJEE, Pradipta K.: *Face Detection and Recognition Theory and Practice*. Boca Raton : CRC Press, 2016

[Delac i Grgić 2004] DELAC, Kresimir ; GRGIĆ, Mislav: A survey of biometric recognition methods. Iz: *ELMAR* (2004). – URL https://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/survey.pdf. – Posjećeno 17.08.2016.

[Dobša 2017] DOBŠA, Jasminka: *Testiranje hipoteza, jedan uzorak*. 2017. – URL https://elf.foi.hr/mod/resource/view.php?id=42574. – Posjećeno 05.04.2017.

[Elecfreaks 2017] ELECFREAKS: *Ultrasonic Ranging Module HC-SR04 Manual*. 2017. – URL http://www.micropik.com/PDF/HCSR04.pdf. – Posjećeno 16.04.2017.

[EMVCo LLC 2016a] EMVCO LLC: *About EMV*. 2016. – URL https://www.emvco.com/about_emv.aspx. – Posjećeno 13.08.2016.

[EMVCo LLC 2016b] EMVCO LLC: *Worldwide EMV Deployment Statistics*. 2016. – URL https://www.emvco.com/about_emvco.aspx?id=202. – Posjećeno 13.08.2016.

[European Central Bank 2015] EUROPEAN CENTRAL BANK: *Fourth report on card fraud*. 2015. – URL https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf. – Posjećeno 14.08.2016.

[Fitzakerley 2015] FITZAKERLEY, Janet: *Eyelid movements*. 2015. – URL http://www.d.umn.edu/~jfitzake/Lectures/DMED/Vision/Optics/Blinking.html. – Posjećeno 29.03.2017.

[Grd 2015] GRD, Petra: *Two-dimensional face image classification for distinguishing children from adults based on anthropometry*. 2015. – URL http://services.foi.hr/thesis_phd/rad_grd.pdf. – Posjećeno 13.04.2017.

[Gulati i Srivastava 2007] GULATI, Ved P. ; SRIVASTAVA, Shilpa: *The Empowered Internet Payment Gateway*. 2007. – URL http://www.iceg.net/2007/books/2/10_342_2.pdf. – Posjećeno 30.09.2015.

[Hemery et al. 2008] HEMERY, Baptiste ; MAHIER, Julien ; PASQUET, Marc ; ROSENBERGER, Christophe: Face Authentication For Banking. (2008). – URL https://hal.archives-ouvertes.fr/file/index/docid/255972/filename/Rosenberger-FaceAuthenticationForBanking.pdf. – Posjećeno 03.04.2017.

[Hrvatska narodna banka 2014] HRVATSKA NARODNA BANKA: *Platne kartice i kartične transakcije: Statistika platnog prometa*. 2014. – URL https://www.hnb.hr/documents/20182/255177/ap-redpub-pkkt-pdf-h-pkkt_2014/d1e9412b-cbe0-4bdb-9b0d-b744e73251e1. – Posjećeno 08.10.2015.

[Katsaggelos i Cummings 2016] KATSAGGELOS, Aggelos K. ; CUMMINGS, Joseph: *Coursera online predavanja - Fundamentals of Digital Image and Video Processing*. 2016. – URL https://www.coursera.org/course/digital. – Posjećeno 07.06.2016.

[Kossler 2013] KOSSLER, Thomas: *How Credit Card Processing Works: The Payments System Simplified*. 2013. – URL http://go.2checkout.com/payment-system-simplified. – Posjećeno 07.10.2015.

[Kossman 2014] KOSSMAN, Sienna: *4 ways crooks cash in on your personal and financial data*. 2014. – URL http://www.creditcards.com/credit-card-news/4-ways-crooks-cash_in-financial-data-1264.php. – Posjećeno 14.08.2016.

[Krebs 2016] KREBS, Bryan: *All about skimmers*. 2016. – URL http://krebsonsecurity.com/all-about-skimmers/. – Posjećeno 16.08.2016.

[Kumar i Vijayaragavan 2014] KUMAR, K. S. ; VIJAYARAGAVAN, S.: New Secured Architecture for Authentication in Banking Application. (2014). – URL https://www.ijirset.com/upload/2014/february/23_New.pdf. – Posjećeno 03.04.2017.

[Li i Jain 2011] LI, Stan Z. ; JAIN, Anil K.: *Handbook of Face Recognition, Second Edition*. London : Springer, 2011

[Lopez 2010] LOPEZ, Laura S.: Local Binary Patterns applied to Face Detection and Recognition. (2010). – URL http://upcommons.upc.edu/bitstream/handle/2099.1/10772/PFC_LauraSanchez_(LBP_applied_to_FaceDetection%26Recognition).pdf. – Posjećeno 18.08.2016.

[Malviya 2014] MALVIYA, Deepa: Face Recognition Technique: Enhanced Safety Approach for ATM. (2014). – URL http://www.ijsrp.org/research-paper-1214/ijsrp-p3633.pdf. – Posjećeno 03.04.2017.

[Maroshi 2015] MAROSHI, Vera: *Beskontaktno plaćanje, prednosti i mane*. 2015. – URL https://www.progreso.hr/blog/beskontaktno-placanje/. – Posjećeno 29.03.2017.

[MasterCard, Inc 2016] MASTERCARD, INC: *Mastercard Makes Fingerprint and 'Selfie' Payment Technology a Reality in Latin America*. 2016. – URL http://newsroom.mastercard.com/tag/selfie-payments/. – Posjećeno 26.03.2017.

[MasterCard Payment Gateway Services Ltd 2016] MASTERCARD PAYMENT GATEWAY SERVICES LTD: *3D Secure*. 2016. – URL http://www.mastercard.com/gateway/implementation_guides/3D-Secure.html. – Posjećeno 17.03.2016.

[Middlehurst 2015] MIDDLEHURST, Charlotte: *China unveils world's first facial recognition ATM*. 2015. – URL http://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html. – Posjećeno 26.03.2017.

[Murdoch et al. 2010] MURDOCH, Steven J. ; DRIMER, Saar ; ANDERSON, Ross ; BOND, Mike: Chip and PIN is Broken. Iz: *IEEE Symposium on Security and Privacy* (2010). – URL https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf. – Posjećeno 17.08.2016.

[Nacionalni CERT 2016a] NACIONALNI CERT: *O phishingu*. 2016. – URL http://www.cert.hr/phishing. – Posjećeno 14.08.2016.

[Nacionalni CERT 2016b] NACIONALNI CERT: *O socijalnom inženjeringu*. 2016. – URL http://www.cert.hr/socijalni_inzenjering. – Posjećeno 14.08.2016.

[Parmar i Mehta 2013] PARMAR, Divyarajsinh N. ; MEHTA, Brijesh B.: Face Recognition Methods & Applications. (2013). – URL https://arxiv.org/pdf/1403.0485.pdf. – Posjećeno 03.04.2017.

[Payments Cards & Mobile 2015] PAYMENTS CARDS & MOBILE: *Card Fraud Report 2015*. 2015. – URL http://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alaric_Fraud-Report_2015.pdf. – Posjećeno 14.08.2016.

[PCI Security Standards Council LLC 2010] PCI SECURITY STANDARDS COUNCIL LLC: *Data Security Standard: Navigating PCI DSS*. 2010. – URL https://www.emvco.com/about_emvco.aspx?id=202. – Posjećeno 14.08.2016.

[Sood et al. 2013] SOOD, Aditya K. ; BANSAL, Rohit ; ENBODY, Richard J.: Cybercrime: Dissecting the State of Underground Enterprise. Iz: *IEEE Computer Society* (2013). – URL http://adityaksood.secniche.org/papers/IEEE_IC_dissecting_the_state_of_underground_ent.pdf. – Posjećeno 16.08.2016.

[Tekstilno-tehnološki fakultet 2008] TEKSTILNO-TEHNOLOŠKI FAKULTET: *Hi-kvadrat test*. 2008. – URL http://www.ttf.unizg.hr/b-news/news_upload_files/2008/vijest_03-04-2008_47f4d185d0744/Hi_kvadrat%20testovi.pdf. – Posjećeno 01.09.2016.

[UNIQUL 2013] UNIQUL: *Face recognition payments*. 2013. – URL http://uniqul.com/worlds-first-face-recognition-payment-system/. – Posjećeno 26.03.2017.

[US Patent & Trademark Office 2016] US PATENT & TRADEMARK OFFICE: *Image Analysis for User Authentication*. 2016. – URL http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=20160071111.PGNR.. – Posjećeno 26.03.2017.

[Valstar 2015] VALSTAR, Michel: *EXTRA BITS: Faces and Edges - video predavanje*. 2015. – URL https://www.youtube.com/watch?v=v-gkPTvdgYo. – Posjećeno 01.09.2016.

[Viola i Jones 2001] VIOLA, Paul ; JONES, Michael J.: Robust Real-time Object Detection. Iz: *Cambridge Research Laboratory* (2001). – URL http://www.hpl.hp.com/techreports/Compaq-DEC/CRL-2001-1.pdf. – Posjećeno 16.08.2016.

[Zenzerović 2015] ZENZEROVIĆ, Paolo: *Arduino kroz jednostavne primjere, II. izdanje*. Zagreb : Hrvatska zajednica tehničke kulture, 2015

Popis slika

Popis tablica

A Dodatak: detaljni rezultati testiranja algoritma prepoznavanja

Na sljedećim stranicama dani su zasebni rezultati testiranja koje je provedeno u poglavlju rezultati. U tablici A.1 dani su rezultati testiranja LBPH algoritma za kontrolni set, u A.2 za pozitivni set, a u A.3 za negativni set (za svaku osobu).

Tablica A.1: Rezultati testiranja LBPH algoritma za kontrolni (originalni) set za svaku osobu.

Set	Prosj. slič.	Maks. udalj.	Min. udalj.	Broj manjih	Broj većih
yaleB01	0.0	0.0	0.0	33	0
yaleB02	0.0	0.0	0.0	33	0
yaleB03	0.0	0.0	0.0	33	0
yaleB04	0.0	0.0	0.0	33	0
yaleB05	0.0	0.0	0.0	33	0
yaleB06	0.0	0.0	0.0	33	0
yaleB07	0.0	0.0	0.0	33	0
yaleB08	0.0	0.0	0.0	33	0
yaleB09	0.0	0.0	0.0	33	0
yaleB10	0.0	0.0	0.0	33	0
yaleB11	0.0	0.0	0.0	31	0
yaleB12	0.0	0.0	0.0	30	0
yaleB13	0.0	0.0	0.0	31	0
yaleB15	0.0	0.0	0.0	32	0
yaleB16	0.0	0.0	0.0	32	0
yaleB17	0.0	0.0	0.0	32	0
yaleB18	0.0	0.0	0.0	32	0
yaleB19	0.0	0.0	0.0	33	0
yaleB20	0.0	0.0	0.0	33	0
yaleB21	0.0	0.0	0.0	33	0
yaleB22	0.0	0.0	0.0	33	0
yaleB23	0.0	0.0	0.0	33	0
yaleB24	0.0	0.0	0.0	33	0
yaleB25	0.0	0.0	0.0	33	0
yaleB26	0.0	0.0	0.0	33	0
yaleB27	0.0	0.0	0.0	33	0
yaleB28	0.0	0.0	0.0	33	0
yaleB29	0.0	0.0	0.0	33	0
yaleB30	0.0	0.0	0.0	33	0
yaleB31	0.0	0.0	0.0	33	0
yaleB32	0.0	0.0	0.0	33	0
yaleB33	0.0	0.0	0.0	33	0
yaleB34	0.0	0.0	0.0	33	0
yaleB35	0.0	0.0	0.0	33	0
yaleB36	0.0	0.0	0.0	33	0
yaleB37	0.0	0.0	0.0	33	0
yaleB38	0.0	0.0	0.0	33	0
yaleB39	0.0	0.0	0.0	33	0

Tablica A.2: Rezultati testiranja LBPH algoritma za pozitivni set za svaku osobu.

Set	Prosj. slič.	Maks. udalj.	Min. udalj.	Broj manjih	Broj većih
yaleB01	38.6251839545	86.5950928212	24.2751590586	15	17
yaleB02	35.1182352732	57.3404824578	14.9080349576	21	11
yaleB03	37.3690550532	79.6897658972	25.1486508333	19	13
yaleB04	37.0698736799	69.9966114273	25.3223683848	20	12
yaleB05	36.7702885634	69.569051973	25.8068013353	20	12
yaleB06	36.8297525819	55.2342903483	23.618839701	17	15
yaleB07	37.6633624783	56.3506530554	27.3264794142	17	15
yaleB08	37.9498465871	53.8809724994	25.5929160072	18	14
yaleB09	34.2308695109	57.1258758169	13.3318214046	21	11
yaleB10	37.1696924435	50.7448029341	25.6594428707	18	14
yaleB11	33.3114191832	47.4209027161	22.8277680835	21	9
yaleB12	33.9646908982	81.7514156755	22.046325359	23	7
yaleB13	41.5116253933	56.611591393	24.7985268433	8	22
yaleB15	41.4908011022	129.578582767	25.4687748123	18	14
yaleB16	39.5137817514	96.1165905283	24.4780779407	17	14
yaleB17	39.7108599087	66.6484425424	25.5147100401	13	19
yaleB18	36.6138939616	82.2117574456	24.5809642071	19	13
yaleB19	38.7368394595	87.1884993225	25.8651261192	18	14
yaleB20	39.6186324709	88.2661594422	26.3814468	17	15
yaleB21	38.8941403869	99.7116110698	26.3435549288	16	16
yaleB22	34.0824701581	47.7800247695	24.6083222831	21	11
yaleB23	36.5043601933	88.7991098562	24.387406183	21	11
yaleB24	37.7310613797	90.3042910917	25.2229599701	20	12
yaleB25	35.4789843936	52.4634231067	24.5926444888	21	11
yaleB26	37.895333369	82.0480205343	25.7731157286	19	13
yaleB27	38.8332905129	104.592058985	25.0059421874	21	11
yaleB28	37.9587795447	58.5488989499	24.6489501222	18	14
yaleB29	38.4689677661	108.216372067	23.8442476925	19	13
yaleB30	34.4975606132	50.7776719112	24.8492292491	23	9
yaleB31	39.0475841167	122.012684115	23.5891651201	16	16
yaleB32	37.6059381685	61.8680733462	26.3150778484	16	16
yaleB33	37.1193044271	92.9449070372	25.5997614892	21	11
yaleB34	40.2591236763	68.6413023801	24.5088911258	15	17
yaleB35	40.1534970028	91.0676143104	25.7712834432	19	13
yaleB36	40.0132744642	54.065604	24.5016506518	12	20
yaleB37	38.2916230658	49.6509519045	26.1920075898	14	18
yaleB38	37.9532028684	53.8330139164	26.3711911462	14	18
yaleB39	37.348784264	85.5205498345	25.5761799556	18	14

Tablica A.3: Rezultati testiranja LBPH algoritma za negativni set za svaku osobu.

Set	Prosj. slič.	Maks. udalj.	Min. udalj.	Broj manjih	Broj većih
yaleB01	53.9372507635	192.566080487	34.8190869633	10	2377
yaleB02	58.1799415348	88.1316763311	24.0974525316	13	2374
yaleB03	54.2564657614	191.664927775	35.1560487572	3	2384
yaleB04	55.3852159139	185.663870386	34.152589526	8	2379
yaleB05	63.9481232484	135.721435458	39.7622368024	0	2387
yaleB06	53.6369565761	194.769336193	20.5051865999	13	2374
yaleB07	54.4608431889	187.292056974	26.4011458031	15	2372
yaleB08	55.8314262336	149.123695346	13.940834148	13	2374
yaleB09	55.235198216	197.184293436	22.596824013	12	2375
yaleB10	54.915005487	195.253196766	33.4009270669	4	2383
yaleB11	55.1551547405	188.210174106	26.890831914	7	2384
yaleB12	54.9529659731	198.944277206	37.9416799629	0	2392
yaleB13	68.216939622	186.671714708	22.874118127	3	2388
yaleB15	57.5918935468	193.26628008	35.7879828148	5	2383
yaleB16	54.7445187501	197.265578625	35.1161895184	8	2381
yaleB17	54.116817311	190.906351672	10.8106199507	14	2374
yaleB18	56.8692653377	192.860187334	33.3426910768	11	2377
yaleB19	54.0857415742	190.400894268	36.915582025	2	2385
yaleB20	54.3247600095	194.867371116	33.4009270669	8	2379
yaleB21	59.48107289	192.033198851	37.6554254706	1	2386
yaleB22	58.6310277165	191.485781405	24.7207517379	9	2378
yaleB23	55.2414638758	195.771003563	37.3044511424	1	2386
yaleB24	57.0385303781	194.911523817	36.6107170602	5	2382
yaleB25	54.9515290502	194.873189538	16.5067495433	23	2364
yaleB26	55.6727764049	192.634028262	36.849497539	1	2386
yaleB27	61.4356915096	194.355450237	36.8335565376	1	2386
yaleB28	59.5905449903	196.385781224	13.1762936553	13	2374
yaleB29	56.6376841763	195.295331175	37.5157958744	1	2386
yaleB30	53.9596751393	188.342853767	18.9862666089	7	2380
yaleB31	57.552989045	198.52763777	40.2639794945	0	2387
yaleB32	59.5329331143	197.597083882	23.1015246644	9	2378
yaleB33	53.8893852359	193.827597458	37.1967711604	1	2386
yaleB34	56.6854385118	194.240985421	11.0845440035	13	2374
yaleB35	57.0767836155	189.861080477	37.0958720882	1	2386
yaleB36	54.9190460048	194.532617702	15.8787664502	13	2374
yaleB37	54.9116443969	187.768427481	7.13393216202	9	2378
yaleB38	53.9515721788	192.099547573	12.5815737527	19	2368
yaleB39	56.883293263	191.366524142	16.4158547651	11	2376