Usporedba tetovaža za autentikaciju osoba

Kale, Nika

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nika Kale

USPOREDBA TETOVAŽA ZA AUTENTIKACIJU OSOBA

ZAVRŠNI RAD

Varaždin, 2020.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nika Kale

Matični broj: 46250/17izv

Studij: Informacijski sustavi

USPOREDBA TETOVAŽA ZA AUTENTIKACIJU OSOBA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Petra Grd

Varaždin, svibanj 2020.

Nika Kale

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristila drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Sažetak

U ovom radu opisuje se što je to biometrija, kako je biometrija nastala te koje su to osnovne grane biometrije. U središtu samog rada najviše je autentikacija kao dio biometrije i njeni podsustavi. Budući da je tema ovog rada usporedba tetovaža, opisuje se što je to tetovaža, kako nastaje i od kuda potječe. Također, nakon usvajanja bitnih pojmova, zadnje veliko poglavlje sadrži izradu same aplikacije i alate te metode i funkcije koje su bile korištene. Na samome kraju prikazan je izgled aplikacije kroz nekoliko primjera. Svrha ovog rada je čitatelju približiti pojam biometrije i autentikacije kroz zanimljiv primjer izrade aplikacije za usporedbu tetovaža.

Ključne riječi: biometrija, autentikacija, aplikacija, tetovaža, obrada slike, karakteristike, Python, biblioteke

Sadržaj

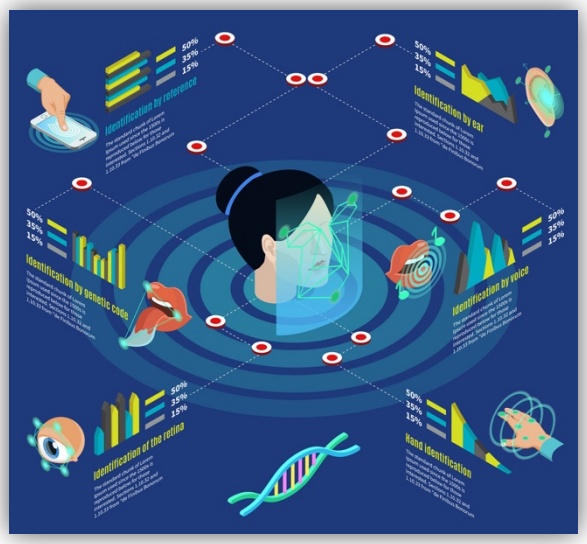
1. Uvod

„U suvremeno doba sposobnost jedinstvenog identificiranja pojedinaca presudno je za ljudsko društvo. Najčešće se koriste tjelesne karakteristike kao što su lice, glas i hod uz druge (npr. lokacija, odjeća) kako bi prepoznali jedni druge.“ (Jain A. K. i sur., 2011) U prošlosti, kada su ljudi živjeli u manjim zajednicama, pojedinci su se jednostavno prepoznavali. Međutim, eksplozija rasta stanovništva popraćena povećanom mobilnošću zahtijevala je razvoj sofisticiranih sustava upravljanja identitetom koji mogu učinkovito bilježiti, održavati i brisati osobni identitet pojedinca.

Počevši s otiscima prstiju prije više od stotinu godina, neprekidno se vrše razna istraživanja u biometriji. „Biometrija je stalno razvijajuća grana znanosti koja je stvorila održivu industriju s velikim očekivanjima za budućnost.“ (Bolle R. M. i sur., 2004) Posljednjih godina tehnologija se poboljšala, a razumijevanje uporabe tehnologije povećava se sa sve većim širenjem iskustva. Upravo je to iskustvo promijenilo fokus biometrijskih tehnologija. To uključuje razmatranje mnogih pitanja, kao što su točnost prepoznavanja, brzina obrade, sigurnost sustava, privatnost, te upotrebljivost sučelja. „Biometrija nije samo novo tehnološko područje opisano s više ili manje uspješnih ispitivanja, biometrija govori o rješavanju ozbiljnih i važnih problema.“ (Bolle R. M. i sur., 2004)

2. Biometrija

Prepoznavanje osoba osnovna je aktivnost u našem društvu. Osiguravanje identiteta i autentičnosti ljudi preduvjet je za mnoge aktivnosti i aplikacije. „Biometrija se odnosi na identifikaciju pojedinca temeljenu na njegovim ili njenim jedinstvenim karakteristikama. Kako bi se što točnije izrazili, možemo reći da je biometrija znanost identificiranja i verificiranja osobe na temelju njenih fizičkih i ponašajnih karakteristika.“ (Haque M.M., 2016) „Fiziološka biometrija kao što je otisak prsta, otisak dlana i slično, pripada fizičkim karakteristikama koje su mjerene u nekom određenom periodu. Biometrija ponašanja, na primjer glas ili potpis, sastoji se od načina na koji se neka radnja provodi s vremenom.“ (searchsecurity.techtarget.com, 2019) Za razliku od fiziološke biometrije, biometrija ponašanja se uči ili stekne tijekom vremena, te ovisi o nečijem stanju uma i podložna je namjernim promjenama. Također, kada govorimo o fiziološkoj biometriji možemo reći da je ona dovoljno „bogata“ kako bi nam jednokratni uzorak mogao biti dovoljan za usporedbu. S druge strane, kod biometrije ponašanja bilo koji dani uzorak nužno nam ne mora dati nikakve podatke o identitetu određene osobe. (Bolle R. M. i sur., 2004)



Slika 1: Prikaz biometrijske identifikacije (vectorstock.com, 2019)

„Budući da se identifikacijske kartice mogu izgubiti, krivotvoriti ili zamijeniti, a lozinke mogu biti zaboravljene ili ugrožene, konvencionalne metode identifikacije, temeljene na jedinstvenim osobnim iskaznicama i identifikacijskim brojevima, nisu dovoljne.“ (Bolle R. M. i sur., 2004) Jasno je da svaka pouzdana pozitivna identifikacija osobe mora podrazumijevati biometrijsku identifikaciju. U današnje vrijeme vlada sve više prihvaća činjenicu da će automatizirana biometrijska autentikacija postati nužna za život i sigurnost građana. Kao što će i druge metode provjere autentičnosti biti sve više u upotrebi, uporaba automatiziranog prepoznavanja lica, prsta glasa i slično postat će sve rasprostranjenija. (Bolle R. M. i sur., 2004)

2.1. Povijest biometrije

„Izraz „biometrija“ izveden je iz grčkih riječi „*bio*“ (život) i „*metrika*“ (za mjerenje). Automatizirani biometrijski sustavi postali su dostupni tek u posljednjih nekoliko desetljeća, zbog značajnog napretka u području računalne obrade. Mnoge od ovih novih automatiziranih tehnika temelje se na idejama koje su izvorno zamišljene prije stotine, čak i tisuće godina.“ (biometricupdate.com, 2019) Dokazi o biometriji prvi put su se pojavili 29.000 godina prije Krista kada su pećinski ljudi svoje crteže potpisivali svojim otiscima prstiju. Babilonci su također koristili metodu potpisivanja s otiscima prstiju, ali na glinenim pločicama.

Prvi zabilježeni dokazi o korištenju biometrijske autentikacije bili su u starom Egiptu. Naime, jedan od administratora tijekom gradnje velike piramide u Gizi pokušao je sistematizirati proces opskrbe radnika hranom. Popis se sastojao od imena radnika, godina, radnih pozicija i slično. Administrator je uočio da ga radnici varaju, te je zaključio da mora početi bilježiti i fizičke i ponašajne karakteristike radnika.

U 14. stoljeću u Kini biometrijska je provjera autentičnosti bila prilično popularna među trgovcima. Tehnologija rane biometrije bila je jednostavna: papir s tintom omogućio je uzimanje otisaka dlana i otisaka stopala pojedinca kako bi ih razlikovali. Zanimljivo je istaknuti da je ovaj način biometrijske autentikacije, unatoč svojoj jednostavnosti, još uvijek u uporabi.

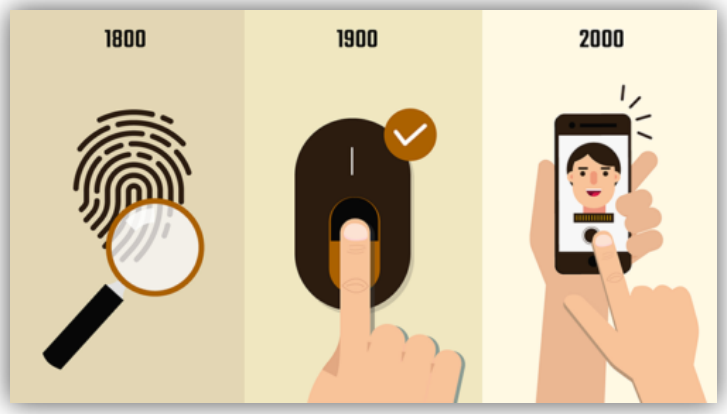
Antropolog Alphonse Bertillon 1870. godine tražio je način kako da identificira osuđene zločince. Upotrijebio je ne samo otiske dlana i otiske stopala, već i pokrete tijela i sve vrste tragova na tijelu. Kreirao je mnoge forenzičke tehnike kao što su ispitivanje dokumenata, sustav za očuvanje otisaka prsta i balistike, fiksiranja mjesta događaja i mnoge druge. Njegove ideje, poznate kao „Bertillonage“, postale su popularne u američkim i britanskim policijskim snagama i pomogle su kod smanjenja kruga osumnjičenih. Najzanimljivija činjenica je da su otisci prstiju, trenutno najpopularniji način biometrije, uključeni u Bertillonov sustav, međutim sam Bertillon nije smatrao da je to važno. (biometricupdate.com, 2019)

Sir Francis Galton 1892. godine razvio je sustav klasifikacije za otiske prstiju. Napisao je detaljnu studiju otisaka prstiju u kojima je predstavio novi sustav klasifikacije koristeći otiske sa svih deset prstiju. Karakteristike (detalji) koje je Galton koristio za identifikaciju pojedinaca i danas se koriste. Ti se detalji često nazivaju Galtonovim detaljima.

Goldstein, Harmon i Lesk 1980. godine razvili su ideju prepoznavanja lica. Koristili su 21 specifični marker kao što je boja kose, debljina usana itd. za automatizaciju prepoznavanja lica. Također, iste godine, pojavio se prvi model ponašajnih komponenti govora. Izradio ga je dr. Joseph Perkell. koji je u svojem radu koristio X-zrake. Ručno mjerenje i izračunavanje predstavljalo je jedini problem ovih modela. (biometricupdate.com, 2019)

Prvi komercijalni sustavi za prepoznavanje geometrije ruku postali su dostupni ranih 1970- ih. To su bili prvi komercijalno dostupni biometrijski sustavi od primjene otiska prsta u kasnim 1960 – ima. Implementacija ovih sustava ima tri glavne svrhe: fizičku kontrolu pristupa, vrijeme i dolazak i osobnu identifikaciju. Tek 1980. godine se izraz „biometrija“ počeo koristiti za opisivanje metoda automatizirane identifikacije pojedinca.

„Sustav prepoznavanja lica postavljen je 2001. godine na Super Bowl-u u pokušaju identifikacije „traženih“ pojedinaca koji ulaze na stadion. Zanimljivo je da, korištenjem tog softvera, 19 osoba sa kriminalnim dosjeom je identificirano.“ (biometricupdate.com, 2019) Također, 2013. godine Apple Inc. predstavili su „Touch ID“ značajku koja omogućuje prepoznavanje otiska prsta radi otključavanja mobitela, kupnje aplikacija i slično. Kroz godine biometrijski sustavi se sve više unaprjeđuju i razvijaju, a njihov doprinos je sve veći. Od 2013. godine pa sve do danas biometrija je postala neizbježan dio naših života.



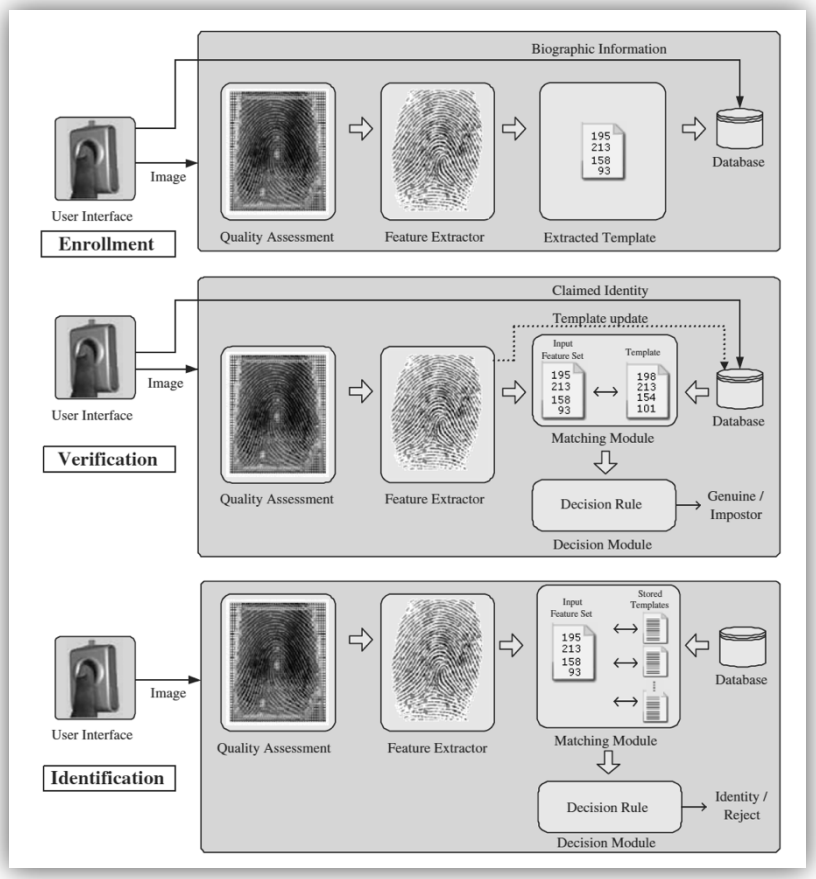
Slika 2: Biometrija kroz povijest (m2sys.com, 2019)

2.2. Biometrijski podsustavi

„Svaki biometrijski sustav provjere identiteta možemo promatrati kao sustav prepoznavanja uzoraka. Sastoji se od biometrijskih čitača ili senzora, ekstraktora za izračunavanje atributa i matrica za usporedbu dva skupa biometrijskih značajki.“ (Jain A. K. i sur., 2011) Sustav provjere autentičnosti sastoji se od dva podsustava:

- Sustav za upis (*engl. Enrollment*)
- Sustav za autentikaciju (*engl. Authentication*)
    - Verifikacija (*engl. Verification*)
    - Identifikacija (*engl. Identification*)

„Tijekom faze upisa dobivamo biometrijske podatke o pojedincu i pohranjujemo ih u bazu podataka zajedno s njegovim identitetom. Uobičajeno je da se dobiveni podaci obrađuju kako bi se izvukle vidljive i svojstvene karakteristike pojedinca. U mnogim se slučajevima pohranjuje samo skup značajki, dok se sirovi biometrijski podaci odbacuju.“ (Jain A. K. i sur., 2011)



Slika 3: Prikaz biometrijskih podsustava (Jain A. K. i sur., 2011)

Sustav za autentikaciju je glavna tema cjelokupnog rada te će se tom podsustavu posvetiti cijelo poglavlje kako bi ga se detaljno objasnilo.

3. Autentikacija

„Biometrijska autentikacija oblik je sigurnosti koji mjeri i odgovara biometrijskim značajkama korisnika da provjeri je li osoba koja pokušava pristupiti određenom sustavu ili uređaju ovlaštena za to.“ (iovation.com, 2019) Već smo ranije u ovom radu napomenuli da postoje fizičke i ponašajne karakteristike koje su jedinstvene za svaku osobu. Ako se biometrijske značajke korisnika koji pokušava pristupiti uređaju podudaraju s karakteristikama odobrenog korisnika, pristup uređaju je odobren. „Uobičajene vrste biometrijske provjere autentičnosti sve se više ugrađuju u uređaje, posebno računala i pametne telefone. Vlada i privatne korporacije u sigurnim područjima također koriste tehnologije biometrijske autentikacije, a najpotrebnije je zračnim lukama i državnim granicama.„ (iovation.com, 2019)

3.1. Podsustavi autentikacije

3.1.1. Identifikacija

„Identifikacija se temelji na biometrijskim karakteristikama i temelji se samo na biometrijskim podacima. Sustav ima mogućnost pretraživanja biometrijske baze podataka kako bi utvrdio postoje li unosi iz baze podataka koji se podudaraju s uzorkom promatranog subjekta.“ (Bolle R. M. i sur., 2004) Izlaz čini popis identifikatora koji nalikuju ulaznim biometrijskim karakteristikama. Takav biometrijski identifikacijski sustav može se koristiti na dva različita načina, pozitivnom identifikacijom i negativnom identifikacijom.

Pozitivna identifikacija se odnosi na utvrđivanje da se pojedinac nalazi u određenoj bazi podataka. Pogreške koje se mogu učiniti su lažno prihvaćanje (*engl. False Accept*) i lažno odbacivanje (*engl. False Reject*). Kada se subjekt smatra lažno prihvaćenim, dolazi do ranjivosti sustava jer uljezi ulaze u sustav ili ako je subjekt odbijen znači da je odbačen uljez. (Bolle R. M. i sur., 2004)

Negativna identifikacija znači utvrđivanje da subjekt nije u negativnim bazama podataka. Nazivamo je još i provjeravanje (*engl. Screening*) jer je uneseni subjekt pregledan u odnosu na biometrijsku bazu podataka. Ovo je sustav gdje se događaju lažne negativne pogreške (*engl. False Negative*) i lažne pozitivne pogreške (*engl. False Positive*) tj. nedostatak podudaranja i lažno otkivanje podudarnosti. (Bolle R. M. i sur., 2004)

3.1.2. Verifikacija

„Osnovna razlika između verifikacije i identifikacije je u tome što se predstavljeni biometrijski sustav uspoređuje samo s jednim upisanim biometrijskim entitetom. Iako još uvijek postoji velika upisana populacija, korisnik daje token koji pokazuje jedan biometrijski identifikator iz baze podataka radi usporedbe.“ (Bolle R. M. i sur., 2004) Kao i identifikacijski sustav, verifikacijski sustav ima pristup biometrijskoj bazi podataka. Ta baza podataka sadrži biometrijske identifikatore povezane sa subjektom. Međutim, za razliku od sustava identifikacije, kod sustava verifikacije svaki je biometrijski identifikator povezan sa različitim biometrijskim identifikatorom. Postoje dvije moguće konfiguracije baze podataka, centralizirana baza podataka i distribuirana baza podataka.

„Centralizirana baza podataka pohranjuje biometrijske karakteristike upisanih entiteta. Korisnik navodi identitet koji omogućava pronalaženje odgovarajućeg biometrijskog predloška. To se uspoređuje s novo predstavljenim biometrijskim uzorkom.“ (Bolle R. M. i sur., 2004)

„Distribuirana baza podataka pohranjuje biometrijske podatke na distribuirani način. Nema potrebe za održavanjem glavne kopije biometrijske baze podataka. Subjekt predstavlja neki biometrijski uređaj koji sadrži jedan biometrijski identifikator, izravno u sustav. Na primjer, provlačenjem magnetske kartice ili korištenjem pametne kartice.“ (Bolle R. M. i sur., 2004)

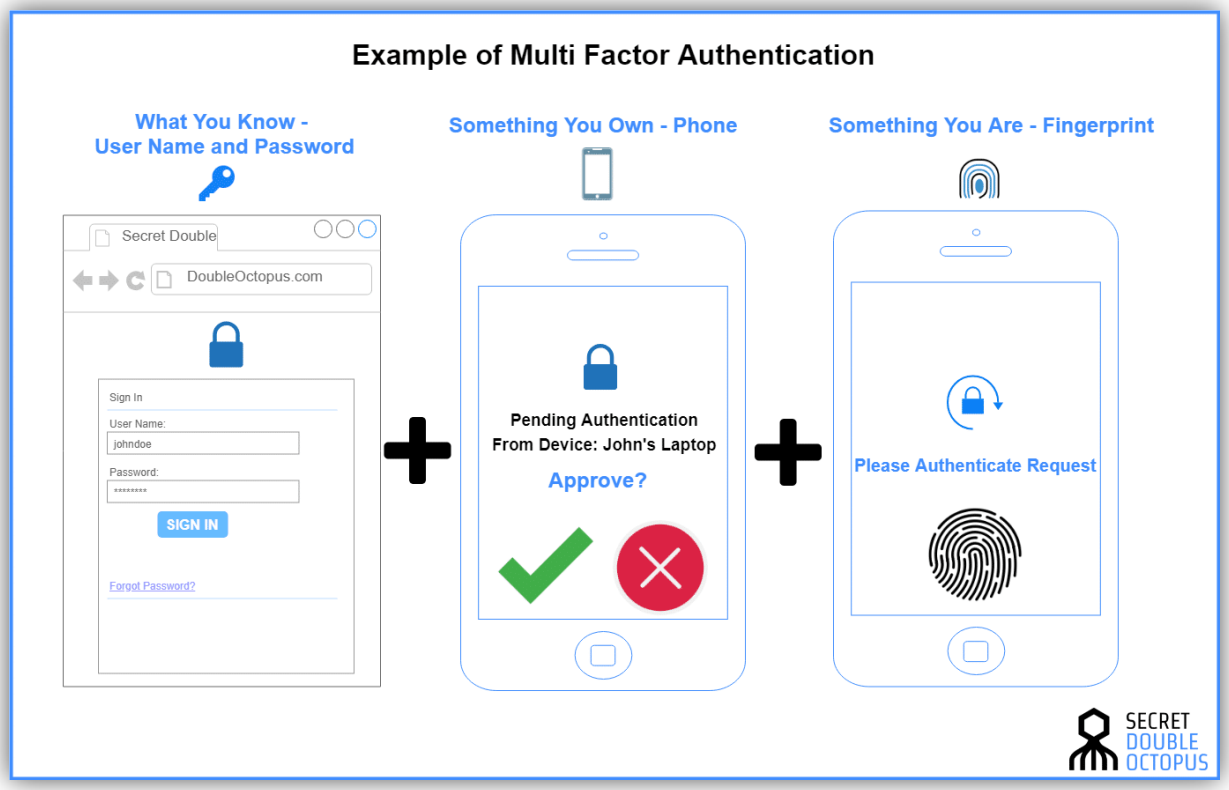
3.2. Metode autentikacije

3.2.1. Autentikacija jednim faktorom (*engl. Single Factor Authentication*)

„Autentikacija jednim faktorom postupak je osiguranja pristupa određenom sustavu, poput mreže ili web stranice koji identificiraju korisnika koji zahtijeva pristup putem samo jedne kategorije dokumenata.“ (Haque M. M., 2016) Jedan od glavnih problema ove metode je to što korisnici ne znaju i ne razumiju kako napraviti jake i lako pamtljive lozinke ili podcjenjuju potrebu za sigurnošću. Kratke i slabe lozinke se mogu vrlo lako probiti za čak nekoliko minuta što ih čini jednako neučinkovitim kao da lozinke uopće nema. Korisnike treba poticati na stvaranje dugih, ali pamtljivih izraza. Dodavanje velikih slova, brojeva i možda nekoliko posebnih znakova uvelike povećava učinkovitost same lozinke. (Haque M. M., 2016)

3.2.2. Autentikacija s više faktora (*engl. Multi Factor Authentication*)

„Autentikacija s više faktora postupak je kontrole pristupa računalu u kojoj se korisniku omogućuje pristup tek nakon što uspješno predloži nekoliko zasebnih dokaza mehanizmu provjere autentičnosti barem dvije od sljedećih kategorija: znanje (nešto što znaju), posjedovanje (nešto što imaju) i pripadnost (nešto što jesu).“ (Haque M. M., 2016) Autentikacija s više faktora koristi dvije ili više neovisnih dokumenata: što korisnik zna (lozinka), što korisnik ima (sigurnosni token) i što korisnik jest (biometrijska provjera). Cilj je stvoriti slojevitu obranu i otežati neovlaštenoj osobi pristup cilju poput fizičke lokacije, računala, mreže ili baze podataka. Ukoliko je barem jedan od faktora ugrožen ili probijen, napadač ipak ima barem još jednu prepreku za probijanje prije nego što uspješno provali u određeni sustav. (Haque M. M., 2016)



Slika 4: Primjer MFA (doubleoctopus.com, 2019)

4. Tetovaža

„Ožiljci, oznake i tetovaže (*engl. Scars, marks and tattoos - SMT*) sve se više koriste za identifikaciju osumnjičenih i žrtava u forenzici i agencijama za provođenje zakona.“ (Lee J. E. i sur., 2008) Naročito se ističu tetovaže jer privlače pažnju svojim vizualnim demografskim karakteristikama kao i sve većom rasprostranjenošću. Tetovaže pružaju više diskriminirajućih podataka od tradicionalnih demografskih pokazatelja kao što su dob, visina, spol i rasta za identifikaciju osoba. Mnogi ljudi se odluče na tetoviranje kako bi se razlikovali od drugih, prikazali svoju osobnost ili pokazali da pripadaju nekoj grupi. Mogli bi reći da prisutnost tetovaža dovodi do sveobuhvatnijeg razumijevanja podrijetla i vjerovanja nekog pojedinca.

4.1. Definicija i porijeklo tetovaže

„Tetovaže su trajni oblici umjetnosti tijela koji pripadaju mnoštvu različitih kultura diljem svijeta.“ (authoritytattoo.com, 2019) Ljudi koriste tetovaže više od 5000 godina kako bi se razlikovali jedni od drugih, a do nedavno je praksa tetoviranja bila ograničena na skupine poput motociklista, mornara i članova bandi. Međutim, u suvremeno doba sve manje se tetovaža povezuje s lošom reputacijom te populacija tetovaža naglo raste. Najveća je popularnost među mlađim dijelom stanovništva i to u dobi između 18 i 29 godina. Smatra se da u toj dobi preko 36% posto mladih ima barem jednu tetovažu.

Postoje dokazi da je tetoviranje drevni umjetnički oblik, nakon što su pronađene tetovaže na mumificiranoj koži. „Vjeruje se da su najstariji dokazi o ljudskim tetovažama iz razdoblja između 3370. i 3100. godina prije Krista. Širom zapadne Kine u provinciji Xingjian otkrivene su mumije s tetoviranom kožom koje potječu još od 2100. godine prije Krista.„ (authoritytattoo.com, 2019) Unutar drevnih kineskih običaja tetoviranje se smatralo divljačkim i bilo je izrazito stigmatizirano.

Za razliku od Kine, u Samoi, tetoviranje predstavlja dio kulturne tradicije već tisućama godina. Povijest tetoviranja u Samoi idealan je primjer kako tetovaže mogu biti sastavni dio kulture. Neki čak vjeruju da moderna engleska riječ „*tetovaža*“ potječe od samoanske riječi za tetovažu „*tatau*“. „Tradicija tetoviranja rukom prakticira se više od dvije tisuće godina, a tehnike i alati koji su korišteni nisu se promijenili sve do danas. Vještina tetoviranja uči se i prenosi se s oca na sina. Kada su tetovaže kompletne, predstavljaju i slave predanost kulturi i velikoj izdržljivosti.“ (authoritytattoo.com, 2019)

Sve do sredine 20. stoljeća tetovaže nisu bile vrlo česte niti društveno prihvatljive. Do tada bile su rezervirane za mali broj populacije. Potpuno tetovirani ljudi postali su popularna atrakcija sama po sebi.

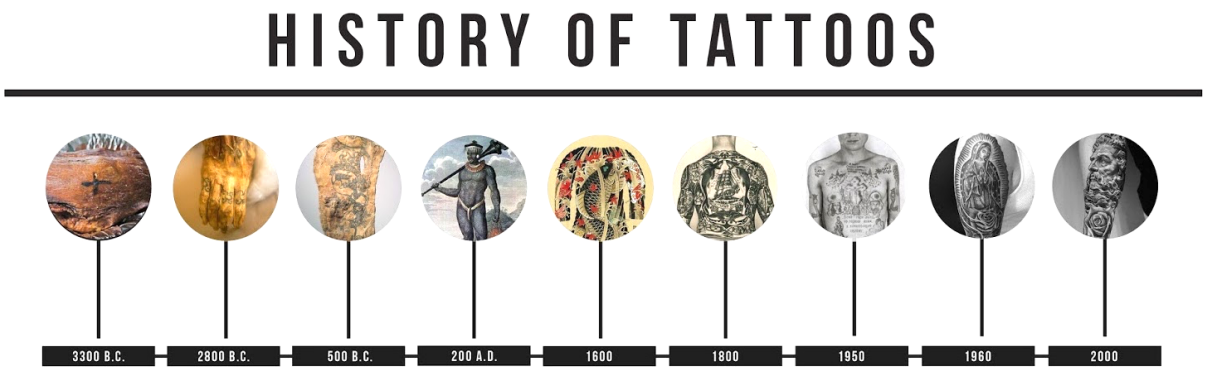
„Na početku 20. stoljeća tetovaže se moglo vidjeti većinom na mornarima. Tetovaža sidra imala je simboliku pripadanja, jednom kada su se pridružili mornarici tetoviranje je bilo znak dobrodošlice." (authoritytattoo.com, 2019) Također, mnoge tetovaže na mornarima služile su u identifikacijske svrhe, ukoliko su pali preko broda ili se utopili.

Kroz 1920 – te godine kozmetičke tetovaže postale su vrlo popularne među ženama. Mnoge žene bi tetovirale popularne trendove šminkanja na licu jer je šminka u to vrijeme bila preskupa za kupnju. Uobičajene kozmetičke tetovaže uključivale su obrve i obrub oko usana kao efekt olovke za usne. Tradicionalno dizajnirane tetovaže još uvijek nisu bile društveno prihvatljive i bile su vrlo rijetke. Također, žene bi svoje kozmetičke tetovaže držale u tajnosti.

Norman Keith Collins bio je prvi koji je, 1940-tih, tetovaži dao boje stvarajući vlastite pigmente i dodajući ih svojim tetovažama. Klasični dizajn ovog desetljeća obilježili su odvažni motivi i obilje boja. Taj bitni pomak u dizajnu tetovaža potaknuo je porast prihvaćanja tetovaža. Povećana popularnost značila je da dekorativna tinta izlazi iz sjene.

Tek 1970-tih godina su tetovaže bile doista prihvaćene i postale sve popularnije u društvu. Više tetovaže nisu bile samo za odmetnike društva, već su ih obični ljudi redovito željeli na svome tijelu. Simboli mira i poruke mira bili su posebno popularni u ovom desetljeću. Također, pojavio se novi stil sa detaljnim dizajnom koji je dobivao sve veću popularnost.

„Za sada, 2010-tih godina, trendovi su povezani i s dizajnom i s lokacijom tetovaže. Najpopularnije su male tetovaže na neobičnim mjestima poput prsta ili iza ušiju. Također, mnogi žele duhovite i kreativne tetovaže za razliku od prijašnjih desetljeća kada je tradicija prevladavala." (authoritytattoo.com, 2019)



Slika 5: Tetovaže kroz povijest
(kateharmsworthresearch.blogspot.com, 2017)

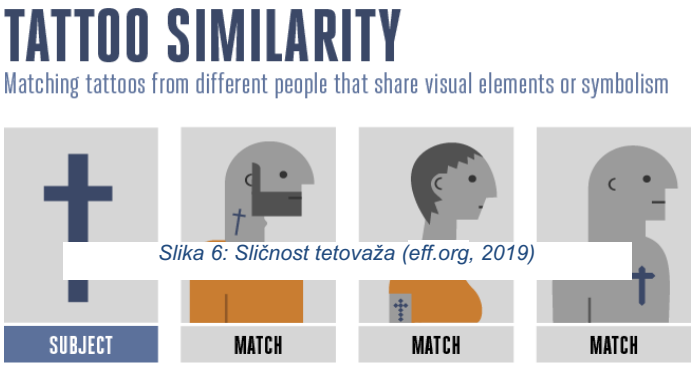
4.2. Prepoznavanje tetovaža (*engl. Tattoo Recognition*)

„Tehnologija prepoznavanja tetovaža koristi slike tetovaža ljudi kako bi ih identificirali i otkrili informacije o njima poput religije, političkih uvjerenja i pridružili ih osobama sa sličnim tetovažama.“ (eff.org, 2019) Iako je još u razvoju, tehnologiju razvijaju privatne tvrtke uz potporu saveznih agencija, državnih zakona i sveučilišta. Prepoznavanje tetovaža oblik je biometrijske tehnologije u istoj kategoriji kao i prepoznavanje lica, otiska prsta i skeniranja šarenice.

Prepoznavanje tetovaža funkcionira na sličan način kao i prepoznavanje lica. Jednom kada se slika tetovaže uhvati i pošalje u sustav, softver za prepoznavanje stvara matematički prikaz i analizira ga za određene detalje. Taj se prikaz uspoređuje se s onima koji se nalaze u slikama u već postojećoj bazi podataka. Ljudi također mogu ove slike označiti određenim meta podacima kako bi ih dodatno opisali ili kategorizirali.

„Kada se prikupljaju podaci za sustav često se bilježe višestruke slike pojedinca, a može se također snimiti lica ljudi ili cijela njihova tijela. Te su tetovaže često označene meta podacima o tetovaži, uključujući položaj na tijelu i boju tinte.“ (eff.org, 2019) Sustav označavanja sadrži desetine kodova za kategorizaciju slika tetovaže, u rasponu od općih kategorija poput političkih simbola i sportskih ikona. Uz to, softver može preuzimati slike pronađene na internetu te time popuniti još više svoju bazu podataka.

Iako su u policiji već dugo koristili tetovaže za identifikaciju osumnjičenih, automatizirana tehnologija učinila bi puno više. Prije automatizacije, prepoznavanje tetovaža često je uključivalo održavanje knjiga s fotografijama. Posljednjih godina policijske uprave započele su digitalizaciju tih slika i dodavanje podataka u bazu podataka, zajedno s označenim meta podacima. „U nedavnom istraživanju koje financira FBI, NIST je identificirao nekoliko specifičnih primjena tehnologije prepoznavanja tetovaža od strane policije.“ (eff.org, 2019) Oni uključuju prepoznavanje osobe po njihovim tetovažama, kao i identificiranje osumnjičenog čije su tetovaže djelomično uhvaćene na kamerama.



Slika 6: Sličnost tetovaža (eff.org, 2019)

5. Aplikacija

Praktični dio ovog rada sastoji se od izrade aplikacije koja uspoređuje dvije tetovaže. U nastavku ovog rada opisan je postupak izrade, navode se svi programi i biblioteke koje su se koristile te je na kraju prikazan finalni izgled i rješenje ove aplikacije.

5.1. Programski jezik i biblioteke

Python je programski jezik koji je nastao tek 90-tih godina te je danas prvi na listi najkorištenijih programskih jezika. Koristi se za razvoj web aplikacija, softver-a, matematiku i znanost općenito pa tako i za biometriju. Kompatibilan je s velikim brojem operacijskih sustava (npr. Windows, Mac, Linux, itd.), te ima vrlo sličnu sintaksu engleskom jeziku koja programerima omogućava pisanje programa s puno manje redaka koda nego u ostalim programskim jezicima. Upravo zbog te jednostavnosti pisanja i pristupačnosti samog programskog jezika ova aplikacija rađena je u Python-u.

Biblioteke korištene u programskom kodu:

i. PyQt
   - PyQt je jedan od poznatijih „okvira rada“ (*engl. Framework*) za kreiranje grafičkih korisničkih sučelja. Temelj mu je Qt framework te je dostupan na svim operacijskim sustavima. Qt nije namijenjen samo za kreiranje grafičkih sučelja već i za SQL baze podataka, XML, SVG i slično. Qt također uključuje i Qt Designer o kojem će biti nešto više u idućem poglavlju.

ii. OpenCV
   - OpenCV je biblioteka za računalni vid (*engl. Computer vision*) i strojno učenje (*engl. Machine learning*) koja sadrži preko 2 500 optimiziranih algoritama. Ti algoritmi koriste se za prepoznavanje lica ili objekata, praćenje objekata u pokretu i u ovom slučaju za prepoznavanje i usporedbu tetovaža.

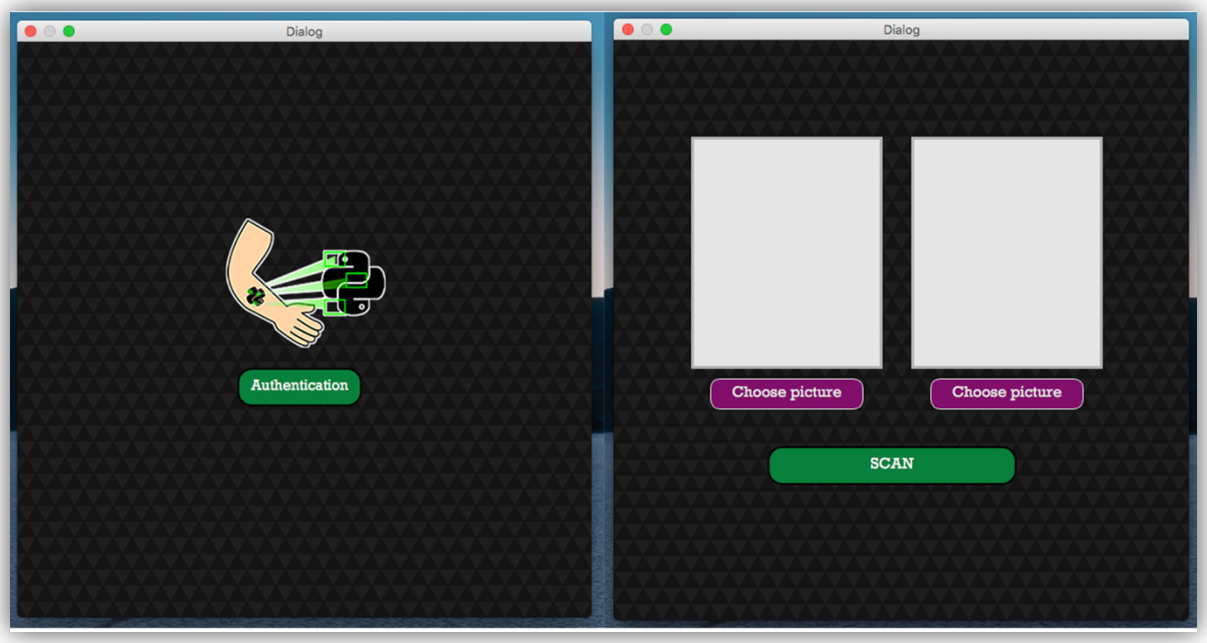
iii. Numpy
   - Numpy je osnovna biblioteka za znanstveno računanje u Python-u. Sadrži sofisticirane funkcije, linearnu algebru, Fourierovu transformaciju, i slično. Također, Numpy je potreban i kada implementiramo OpenCV.

Slika 7: Logo biblioteka (logo.wine, 2020)

5.2. Izrada grafičkog korisničkog sučelja

Prva faza u izradi aplikacije je izrada grafičkog korisničkog sučelja. Kao što je navedeno u poglavlju prije, za grafičko korisničko sučelje (GUI) korišten je PyQt5 točnije Qt Designer. Qt Designer služi za dizajniranje grafičkog sučelja. Nakon što se kreira dizajn, pomoću terminala pretvara se napravljeni dizajn u Python kod. Pristupačan je jer olakšava samu izradu dizajna, a moguće je dodati i nove GUI kontrole napisane u Python-u.

Grafičko korisničko sučelje ove aplikacije ima vrlo jednostavan i pristupačan dizajn budući da je u glavnom fokusu njena funkcionalnost. Na slici 8 može se vidjeti kako sučelje izgleda. Slika lijevo prikazuje početni prozor koji se korisniku otvara kada pokrene aplikaciju, a zatim pritiskom na gumb „*Authentication*“ otvara se prozor na slici desno.



Slika 8: Prikaz grafičkog korisničkog sučelja

Programski kod:

```
class MainPocetna(QDialog):

    def __init__(self):
        super(MainPocetna, self).__init__()
        loadUi('pocetna.ui', self)
        self.authenticationButton.clicked.connect(self.move)

    def move(self):
        from prva import MainPrva
        theclass = MainPrva()
        theclass.exec_()
```

Stvorena je klasa „*MainPocetna*“ u kojoj se pomoću „*loadUi*“ otvara prije spomenut dizajn za početnu stranicu.

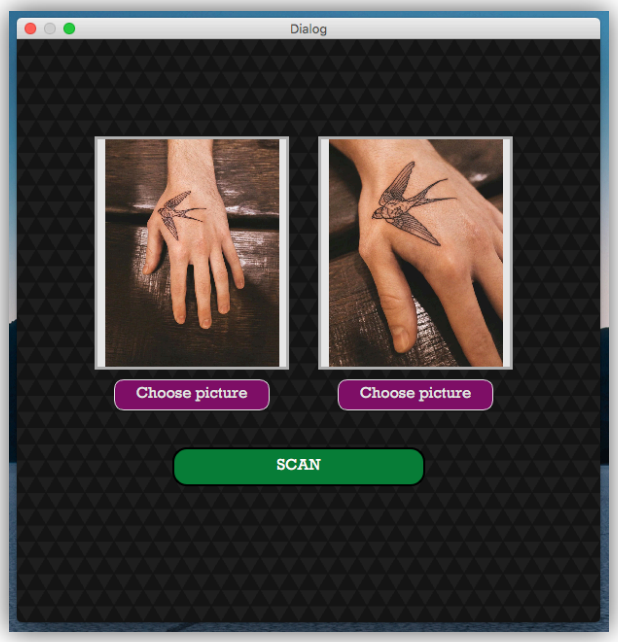
Budući da se ne radi sve u istom prozoru, moramo imati funkciju „*move*“ koja otvara novi prozor. Kako je ovdje riječ o dvije odvojene *.py* datoteke, u funkciji je potrebno importirati klasu „*MainPrva*“ (ona se nalazi u drugoj datoteci) koja inicijalizira otvaranje drugog prozora. Tu funkciju se poveže s gumbom „*Authentication*“ tako da svaki put kada se taj gumb pritisne otvori se drugi prozor.

Kako bi se uopće mogle uspoređivati slike, najprije je bilo potrebno naći način kako učitati te slike. U Qt Designeru su napravljene dvije oznake (*engl. Label*) koje se mogu vidjeti na slici 8 (slika desno). Gumb ispod slike je povezan sa funkcijom *setImage2* koja u oznaku sprema pixmap određene slike. Pixmap pohranjuje i prikazuje grafičku sliku kao pravokutni niz vrijednosti piksela u boji (skraćenica za „pixel map“).

Programski kod:

```
def setImage2(self):
        self.fileName1, _ = QtWidgets.QFileDialog.getOpenFileName(None,
                            "Select Image", "", "Image Files (*.png *.jpg
                            *jpeg *.bmp);;All Files (*)")
        if self.fileName1:
            pixmap = QtGui.QPixmap(self.fileName1)
            pixmap = pixmap.scaled(self.img2Label.width(),
                     self.img2Label.height(), QtCore.Qt.KeepAspectRatio)
            self.img2Label.setPixmap(pixmap)
            self.img2Label.setAlignment(QtCore.Qt.AlignCenter)
```

Na kraju kako bi se prikazala slika u korisničkom sučelju, vrijednost pixmap-e je dodijeljena oznaci. Krajnji rezultat kako izgleda kada se učita slika u oznaku može se vidjeti na slici broj 9.



Slika 9: Prikaz učitanih slika (instagram.com, 2020)

5.3. Pred-procesiranje slika

Drugu fazu izrade aplikacije čini pred-procesiranje slika. Tetovaže su specifične zbog broja linija kojima su rađene. Kako bi se jasno moglo vidjeti gdje su točno linije prvo je potrebno pixmap koji sadrži vrijednosti učitane slike pretvoriti u *grayscale*. Za razliku od pixmap-a gdje su vrijednosti boje piksela, podaci u grayscale slici sadrže samo jedan kanal koji može predstavlja intenzitet, svjetlinu ili gustoću slike. Kod takvih slika samo pozitivne vrijednosti imaju smisla. „Tipična grayscale slika koristi k=8 bitova po pikselu i vrijednosti intenziteta u rasponu od [0, 255], gdje 0 predstavlja minimalnu svjetlinu (crna), a 255 maksimalnu svjetlinu (bijela)“. (Bača M. i sur., 2019) Budući da se koristi OpenCV biblioteka, programski kod za pretvaranje u grayscale sliku je poprilično trivijalan.

Programski kod:

```
img0 = cv2.imread(self.fileName1)
img1 = cv2.imread(self.fileName2)
gray1 = cv2.cvtColor(img0, cv2.COLOR_BGR2GRAY)
gray2 = cv2.cvtColor(img1, cv2.COLOR_BGR2GRAY)
```

Može se vidjeti iz isječka programskog koda da nakon što se pročitaju slike pomoću funkcije *cv2.cvtColor* mijenjamo im se boja. Funkcija poprima dvije vrijednosti, prva je slika koja se mijenja (img0), a druga boja u koju se mijenja što je u ovom slučaju grayscale (cv2.COLOR_BGR2GRAY).

Slika 10: Grayscale slika

Idući korak u pred-procesiranju slika za daljnju izradu aplikacije je detektiranje rubova na slici. Kao što je već spomenuto, kako bi se moglo uspoređivati karakteristike potrebno je znati gdje su na slici sve rubovi. Budući da se radi s tetovažama, rubovi će biti svugdje gdje su nacrtane linije. Biblioteka OpenCV ima funkciju „*cv2.Canny*“ koja se koristi za detekciju rubova.

„Canny Edge Detection“ je algoritam kojim se detektiraju rubovi na slici. Sam algoritam prolazi kroz nekoliko faza:

i. Budući da je otkrivanje rubova osjetljivo na šum na slici, prvo se mora pomoću 5x5 Gaussovog filtera ukloniti sav šum s određene slike.
ii. Izoštrena slike se zatim filtrira s Sobel-ovom matricom u vodoravnom i okomitom smjeru kako bi dobili prvu derivaciju u vodoravnom smjeru (G_x) i okomitom smjeru (G_y). Nakon toga se dobiva gradijent i smjer ruba pomoću jednadžbe:

$$Edge\_Gradient(G) = \sqrt{G_x^2 + G_y^2}$$

$$Angle(\theta) = tan^{-1}\left(\frac{G_y}{G_x}\right)$$

iii. Nakon što se dobije smjer gradijenta, traže se i uklanjaju neželjeni pikseli koji ne mogu predstavljati rub. Za svaki piksel se gleda je li on lokalni maksimum u njegovoj blizini u smjeru gradijenta.
iv. Zadnja faza je provjera koji su rubovi stvarno rubovi pomoću dvije „*threshold*“ vrijednosti, *maxVal* i *minVal*. Svi rubovi s intenzitetom gradijenta većim od *maxVal* su sigurno rubovi, dok oni ispod *minVal* sigurno nisu rubovi.

OpenCV sve navedeno, cijeli algoritam, stavlja u jednu funkciju *cv2.Canny()* te time olakšava pronalaženje rubova na slici. Primjer se može vidjeti na slici 12.

Slika 12: Detekcija rubova

5.4. FLANN algoritam

Treća faza, ujedno i najvažnija, je implementacija algoritma kojim se traže zajedničke karakteristike slika. FLANN je skraćenica za „*Fast Library for Aporiximate Nearest Neighbors*“. Kao što i sam naziv kaže, FLANN je biblioteka za brzo pretraživanje najbližih susjeda u više-dimenzionalnim prostorima. Sadrži skup algoritama koji najbolje rade brzu pretragu najbližih susjeda. Također, sadrži sustav koji odabire koji je algoritam najprigodniji ovisno o skupu podataka nad kojim ga želimo provesti. FLANN biblioteka je pisana u programskom jeziku C++, ali je prilagođena za korištenje u drugim programskim jezicima kao na primjer C, MATLAB i Python. Budući da je ovaj programski kod pisan u Python-u, FLANN se implementira preko biblioteke OpenCV.

Za početak se moraju pronaći sve glavne karakteristike na slici. Karakteristike se općenito definiraju kao poddomena slike koja je često u obliku izoliranih točaka, kontinuiranih krivulja ili povezanih područja. U ovom slučaju pod karakteristike smatraju se sve linije tetovaže. Budući da su u ranijem dijelu koda izolirani rubovi na slici, tj. pronađene su linije, sada ih je potrebno detektirati i izdvojiti korištenjem SIFT funkcije. Osim što pronalazi glavne karakteristike, također pronalazi i glave deskriptore slike (npr. boja, oblik, tekstura i slično).

Programski kod:

```
sift = cv2.xfeatures2d.SIFT_create()

kp0, des0 = sift.detectAndCompute(gray1, None)
kp1, des1 = sift.detectAndCompute(gray2, None)
```

Nakon što se kreira SIFT funkciju potrebno je implementirati FLANN algoritam.

FLANN algoritam uzima dva parametra: objekt *index* i objekt *search*. Ovi parametri određuju ponašanje indeksa i objekata pretraživanja koje FLANN interno koristi kako bi izračunao podudaranje. Također, ovi parametri nude razumnu ravnotežu između točnosti i brzine obrade podataka. Unutar FLANN algoritma koristimo „*kernel density tree*“ (kd-tree). To je algoritam indeksiranja s pet stabala koja FLANN paralelno obrađuje.

Programski kod:

```
FLANN_KDTREE = 1
index = dict(algorithm=FLANN_KDTREE, trees=5)
search = dict(checks=50)

FLANN = cv2.FlannBasedMatcher(index, search)
matches = FLANN.knnMatch(des0, des1, k=2)
```

Nakon što su na svakoj slici pomoću SIFT funkcije i FLANN algoritma pronađene karakteristike, potrebno ih je usporediti s karakteristikama druge slike. Za pronalaženje dobrih podudaranja korišten je „*Lowe's ratio test*“. Jedina razlika je što se umjesto fiksne vrijednosti parametra *i* uzeo raspon vrijednosti od 0.1 do 0.6, ali o tome nešto više u idućem poglavlju.

Programski kod:

```
for i in range(1, 7, 1):
    best_matches = []
    i = i/10
    X.append(i)
    for m, n in matches:
        if m.distance < i * n.distance:
            best_matches.append(m)
            if(i==0.6):
                good_matches.append(m)
    Y.append(len(best_matches))
```

Prvo se povezuju ključne točke slike 1 (*des0*) s dvije ključne točke slike 2 (*des1*). Pretpostavljajući da ključna točka slike 1 ne može imati više od jednog ekvivalenta na slici 2, zaključujemo da ta dva podudaranja ne mogu oba biti ispravna što znači da je jedno od njih pogrešno. Ako se slijedi „*Lowe's ratio test*“ zna se da podudaranje s manjom udaljenosti je ono koje se uzima pod dobro podudaranje. Međutim, ukoliko se dobro podudaranje ne može razlikovati od npr. šuma na slici, tada se i to podudaranje odbacuje budući da ne pridonosi rezultatu.

Udaljenost između dvije točke je ključna kako bismo raspoznali dobre od loših podudaranja.

```
if m.distance < i * n.distance
```

Udaljenost *m.distance* predstavlja udaljenost između ključne točke i njezinog najboljeg podudaranja, a *n.distance* je udaljenost između ključne točke i drugog najboljeg podudaranja. U OpenCV-u „*knnMatch*“ funkcija vraća podudarnosti od najboljih do najgorih, tako da će prva podudaranost uvijek imati najmanju udaljenost. Kolika je točno ta najmanja udaljenost koristimo već prije spomenuti parametar *i*. Ukoliko je *m.distance* manji od *n.distance* uzima se u obzir kao dobro podudaranje, u suprotnom ga se zanemaruje.

5.4.1. Metoda najmanjih kvadrata

Prilikom ispisivanja broja dobrih podudaranja za različite vrijednosti parametra *i* s kojim množimo udaljenost između dvije točke, može se vidjeti da je ovisnost broja dobrih podudaranja o parametru *i* linearna. Kako ne postoji određeni *i* koji bi dao najbolji rezultat za sve slike, računa se za *i* u rasponu od 0.1 do 0.6 te se zapisuje broj dobrih podudaranja za svaki od slučajeva. Dobiveni skup podataka obrađuje se metodom najmanjih kvadrata, odnosno primjenjuje se linearna regresija na podatke.

Uzmemo li kvadrat vertikalnog odstupanja svake točke od teorijskog pravca, metodom najmanjih kvadrata se pronalazi najvjerojatniji pravac, onaj za koji je suma kvadrata odstupanja minimalna. Od nekog pravca $y = ax + b$ točka (x_i, y_i) odstupa za ε_i odnosno:

$$y_i = ax_i + b + \varepsilon_i$$

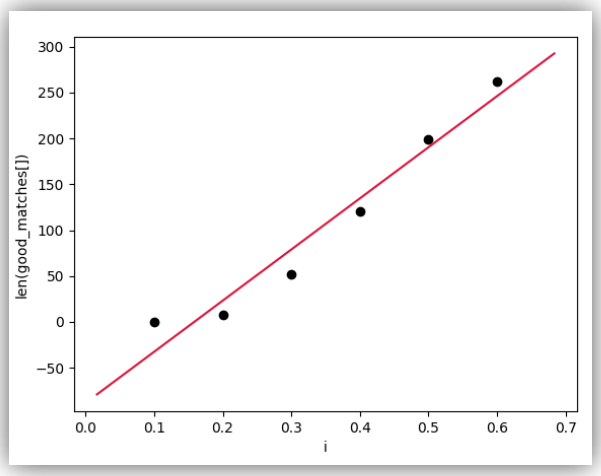
$$S(a,b) \equiv \sum_{i=1}^{n} {\varepsilon_i}^2 = min$$

Izvod koeficijenata pravca *a* i b, kao i pripadnih nepouzdanosti za te koeficijente, je matematički zahtjevan proces te je pisanje gotovih formula u našem slučaju suvišno. Također, izvod počinje računanjem 5 suma te primjenom tih suma kako bi izračunali koeficijente i nepouzdanosti. Isječak programskog koda u kojem se računaju koeficijenti prikazan je ispod.

Programski kod:

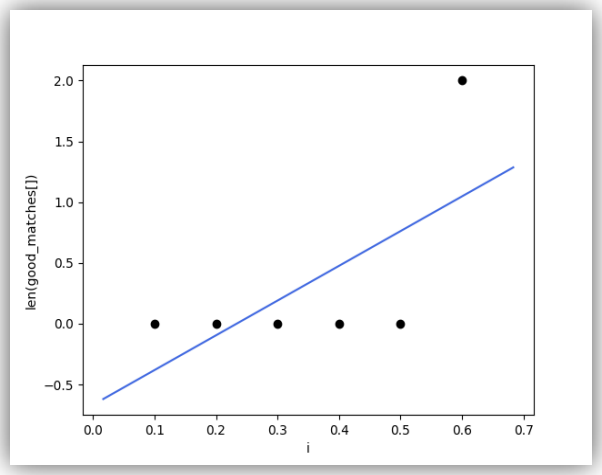
```
for i in range(len(Datax)):
            sumx = sumx + Datax[i]
            sumy = sumy + Datay[i]
            sumx2 = sumx2 + (Datax[i])**2
            sumy2 = sumy2 + (Datay[i])**2
            sumxy = sumxy + (Datax[i] * Datay[i])
        a = ((n*sumxy - sumx*sumy)/(n*sumx2 - (sumx)**2))
        b = ((sumx2*sumy - sumx*sumxy)/(n*sumx2 - (sumx)**2))
        Ma = np.sqrt((1/(n-2))*(((n*sumy2 - (sumy)**2)/(n*sumx2 -
             (sumx)**2))-(a)**2))
        Mb = Ma*np.sqrt((1/n)*sumx2)
```

Na slici 13 može se vidjeti primjena metode na dvije slike koje imaju veliku podudaranost. Broj dobrih podudaranja je za svaku vrijednost parametra *i* vrlo blizu pravcu regresije.



Slika 13: MNK - dobra podudaranost

Na slici 14 može se također vidjeti primjerna metode na dvije slike, međutim u ovom slučaju se dobiva vrlo malena podudaranost. Iako se za i = 0,6 pronađu dobre točke, za razliku od nižih vrijednosti parametara i, broj nađenih točaka je vrlo malen.



Slika 14: MNK - loša podudaranost

Završni postotak se dobiva tako da se podijeli broj dobrih podudaranja dobivenih za parametar *i = 0.6* sa točkom na pravcu koja ima istu x koordinatu. Ovim postupkom se uzima u obzir ukupan dobiveni broj točaka, ali se istovremeno pridjeljuje težina svim izmjerenim točkama sa manjim (strožim) parametrom *i*.

Iako je ova metoda vrlo pouzdana za obradu podataka kada se očekuje linearno ponašanje, jako je teško dobiti postotak veći od 99% budući da bi to zahtijevalo da se sve izmjerene točke poklapaju skoro savršeno sa pravcem regresije.

5.5. Prikaz finalnog rješenja

U zadnjoj fazi izrade ove aplikacije jedino što je preostalo je crtanje dobrih podudaranja i ispisivanje postotka podudaranja. Također, bit će prikazana tri primjera kako ova aplikacija radi, za 100 postotno podudaranje, za neki određeni postotak i za slike koje se uopće ne podudaraju.

Iako je već u prethodnom poglavlju opisano na kojim način dobivamo postotak podudaranja, u kodu prikazano ispod može se vidjeti kako to izgleda u samom programskom kodu.

Programski kod:

```
pogodak = round( ((a*0.6 + b)/Y[5])*100, 0)
            text = "Match: {} %".format(pogodak)
            self.label.setText(text)
```

Dakle, izračunati se postotak dodjeljuje *text*-u, a *text* oznaci *setText* koja to zatim prikazuje.

Crtanje dobrih podudaranja radi se već gotovom funkcijom unutar OpenCV biblioteke *cv2.drawMatches.*

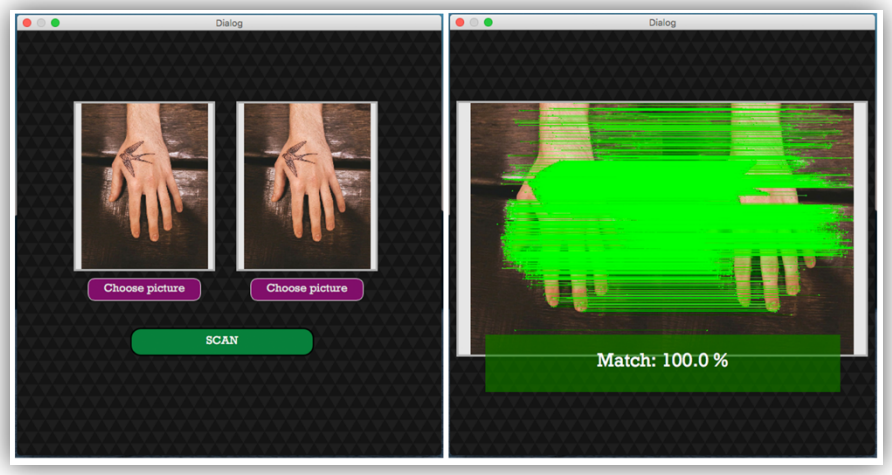
Programski kod:

```
img_matches = cv2.drawMatches(
                img0, kp0, img1, kp1, good_matches, None,
                matchColor=(0, 255, 0), singlePointColor=None)
```

Ova funkcija za parametre uzima sliku 1 (*img0*) i sliku 2 (*img1*), sve ključne točke na slici (*kp0* i *kp1*) i dobra podudaranja (*good_matches*). Budući da je određeno što je točno podudaranost, ne crta sve ključne točke već crta i povezuje zelenim linijama samo dobra podudaranja.

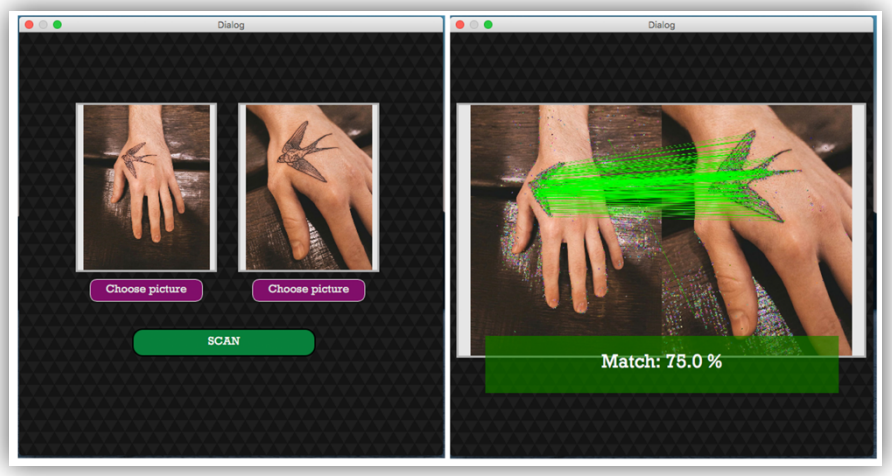
U nastavku su prikazana, kao što je već spomenuto, tri primjera kako naša aplikacija radi:

i. 100% podudaranje



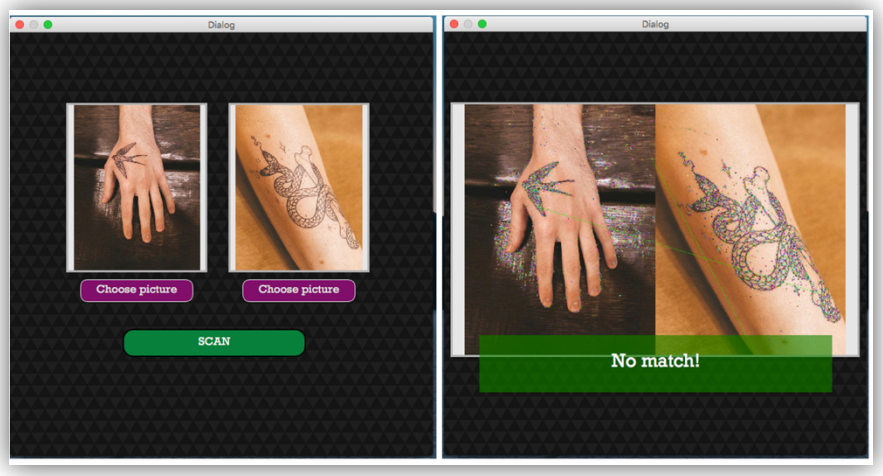
Slika 15: Prikaz 100% podudaranja tetovaža

ii. Određeni postotak podudaranja



Slika 16: Prikaz 75% podudaranja tetovaža

iii. Nema podudaranja



Slika 17: Prikaz ne podudaranja tetovaža

6. Zaključak

U prvom dijelu ovoga rada govorilo se o biometriji, kako je ona nastala, te o njenim podsustavima. Autentikacija, kao jedan od bitnijih podsustava, opširno je opisana i prikazano je kako ju se sve može primjenjivati. Još jedna od bitnih tema koja je spomenuta su tetovaže. Kroz njihovu zanimljivu povijest nastojalo se čitatelju približiti što su to tetovaže te da su u nekim dijelovima svijeta nešto više od tabu-teme. U glavnom fokusu ovog rada je izrada same aplikacije koja uspoređuje tetovaže. Kroz postupak izrade mogla se primijetiti uloga koju matematika kao grana ima čak i u svijetu programiranja. Također, korištenjem raznih biblioteka i objašnjavanjem istih, čitatelju se pokušala predočiti zanimljivost nastanka ove aplikacije.

Osobno smatram da je biometrija jedna od zanimljivijih grana u znanosti. Nadam se da sam svojim radom biometriju uspjela približiti onima koji se još nisu susreli s njom.

7. Popis literature

[1] ai.eecs.umich.edu (2020) *Pixmaps.* Preuzeto 20. svibnja 2020. s http://ai.eecs.umich.edu/people/dreeves/misc/lispdoc/cg/pixmaps/pixmap.htm

[2] authoritytattoo.com (2019) *History & Origin of Tattoos.* Preuzeto 26. studenog 2019. s https://authoritytattoo.com/history-of-tattoos/

[3] Bača M., Grd P. (2019) *Digitalna obrada slike.* Kolegij „Odabrane teme iz biometrije“, Fakultet organizacije i informatike, Varaždin

[4] biometricupdate.com (2019) *History of Biometrics.* Preuzeto 22. studenog 2019. s https://www.biometricupdate.com/201802/history-of-biometrics-2

[5] Bolle R. M., Connell J. H., Pankanti S., Ratha N. K., Senior A. W. (2004) *Guide to Biometrics.* New York: Springer.

[6] doubleoctopus.com (2019) *Multi Factor Authentication (MFA).* Preuzeto 26. studenog 2019. s https://doubleoctopus.com/security-wiki/authentication/multi-factor-authentication/

[7] eff.org (2019) *Tattoo Recogniton.* Preuzeto 26. studenog 2019. s https://www.eff.org/pages/tattoo-recognition

[8] Haque M.M. (2016) *Biometric Authentication: Comparative Study of Different Biometrics Features and Recent developments of Multifactor Authentication Biometrics Technology.* Bangladesh University of Professionals: Information Security.

[9] heimdalsecurity.com (2019) *Biometric Authentication Overview, Advantages & Disadvantages*. Preuzeto 22. studenog 2019. s https://heimdalsecurity.com/blog/biometric-authentication/

[10] Howse J., Minichino J. (2020) *Learning OpenCV 4 Computer Vision with Python 3 Third Edition.* Birmingham, Mumbai: Packt Publishing.

[11] instagram.com (2020) *Tattoo room.* Preuzeto 25. travnja 2020. s https://www.instagram.com/tattoorroom/

[12] iovation.com (2019) *Biometric Authentication.* Preuzeto 22. studenog 2019 s https://www.iovation.com/topics/biometric-authentication

[13] Jain A. K., Ross A. A., Nandakumar K. (2011) *Introduction to Biometrics.* New York Dordrecht Heidelberg London: Springer.

[14] kateharmsworthresearch.blogspot.com (2017) *History of Tattoos Timeline.* Preuzeto 26. studenog 2019. s http://kateharmsworthresearch.blogspot.com/2017/10/history-of-tattoos-timeline.html

[15] Lee J. E., Jain A. K., Jin R. (2008) *Scars, Marks and Tattoos (SMT): Soft Biometric for Suspect and Victim Identification.* Michigan State University: Computer Science and Engineering.

[16] logo.wine (2020) *PyQt Logo Download.* Preuzeto 20. svibnja 2020. s https://www.logo.wine/logo/PyQt

[17] m2sys.com (2019) *Biometrics: History, Origin & How It Affects Our Lives.* Preuzeto 25. studenog 2019. s http://www.m2sys.com/blog/important-biometric-terms-to-know/the-history-of-biometrics-technology/

[18] Makek M. (2016) *Metoda najmanjih kvadrata.* Kolegij „Statistika i osnovna mjerenja“, Prirodoslovno-matematički fakultet, fizički odsjek, Zagreb

[19] numpy.org (2020) *Numpy.* Preuzeto 20. svibnja 2020. s https://numpy.org

[20] opencv-python-tutroals.readthedocs.io (2020) *Canny Edge Detection.* Preuzeto 20. svibnja 2020 s https://opencv-python-tutroals.readthedocs.io/en/latest/py_tutorials/py_imgproc/py_canny/py_canny.html

[21] opencv.org (2020) *About OpenCV.* Preuzeto 20. svibnja 2020. s https://opencv.org/about/

[22] riverbankcomputing.com (2020) *What is PyQt?* Preuzeto 20. svibnja 2020. s https://www.riverbankcomputing.com/software/pyqt/

[23] searchsecurity.techtarget.com (2019) *Biometrics.* Preuzeto 25. studenog 2019. s https://searchsecurity.techtarget.com/definition/biometrics

[24] stackoverflow.com (2019) *How Does the Lowe's ratio test work?.* Preuzeto 21. svibnja 2020. s https://stackoverflow.com/questions/51197091/how-does-the-lowes-ratio-test-work

[25] vectorstock.com (2019) *Isometric biometric authorization infographics vector image.* Preuzeto 22. studenog 2019. s https://www.vectorstock.com/royalty-free-vector/isometric-biometric-authorization-infographics-vector-21181113

[26] w3schools.com (2020) *Python Introduction*. Preuzeto 20. svibnja 2020. s https://www.w3schools.com/python/python_intro.asp