

Veštačka inteligencija

Biometrijski sistemi za kontrolu pristupa

Mentor: Studenti:

prof. Leonid Stoimenov Milica Martinović 15714 Nikola Ristić 15854

Branislav Jovičić 15660

Sadržaj

1. Uvod................................................................................................................3
2. Biometrijski sistem za kontrolu pristupa resursima bankovnih računa……...5
3. Proces prepoznavanja otiska prsta...................................................................6
4. Rešenja korišćena u procesu prepoznavanja otiska prsta u biometrijskom sistemu za kontrolu pristupa resursima bankovnih računa..............................9
5. Ukratko o neuronskim mrežama...................................................................10
6. Zaključak.......................................................................................................12
7. Literatura.......................................................................................................12
8. Uvod

Biometrija je nauka i tehnologija o merenju i analiziranju bioloških podataka. Odnosi se na metriku povezanu sa karakteristikama ljudskog tela. Koristi se u informacionim tehnologijama kao vid identifikacije i za kontrolu pristupa.

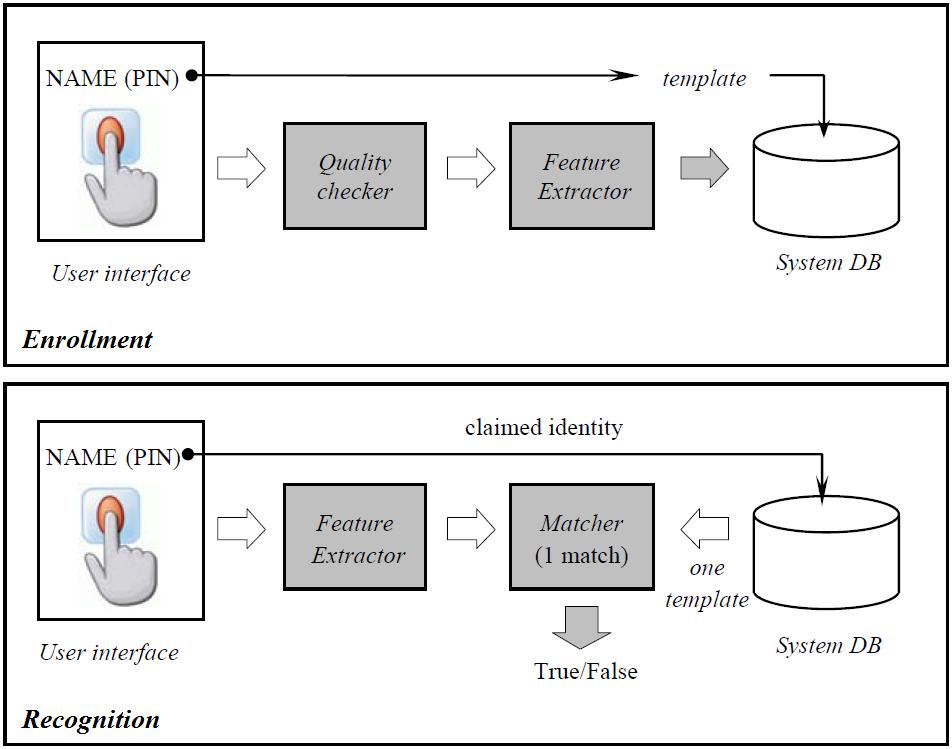
Biometrijski identifikatori su osobene, merljive karakteristike koje se koriste da označe i opišu pojedince. Dele se na fizičke i bihejvioralne. Fizički identifikatori se odnose na oblik tela (otisak prsta, raspored vena u dlanu, prepoznavanje lica, DNK, otisak dlana, geometrija šake, prepoznavanje dužice i mrežnjače, miris i td.), dok se bihejvioralni identifikatori odnose na obrasce ponašanja osobe (način kucanja, stav, pokreti, glas i td.).

Tradicionalni sistemi za kontrolu pristupa uključuju sisteme zasnovane na tokenima, kao što su vozačka dozvola ili pasoš, i sisteme zasnovane na znanju, kao što su šifra ili lični identifikacioni broj. Ovi sistemi ne mogu garantovati da se radi o legitimnim korisnicima, jer ne postoji jaka veza između korisnika i sredstva autentifikacije. Problem nastaje u slučaju njihovog kompromitovanja (krađe, gubljenja, kopiranja i td.). Pošto su biometrijski identifikatori jedinstveni, isti tokom vremena i čvrsto vezani za korisnika, oni predstavljaju pouzdanije rešenje prilikom verifikacije identiteta korisnika.

Biometrija i biometrijski sistemi se danas rutinski koriste u mnogim sferama života (finansijske institucije, mobilni uređaji, forenzika, kontrola pristupa poverljivim informacijama itd.). Međutim, prikupljanje biometrijskih podataka povlači za sobom i pitanje o privatnosti i ciljevima za koje se ti podaci koriste.

Postoje dva pristupa prepoznavanja koji se koriste u biometrijskim sistemima: verifikacija i identifikacija. Biometrijska verifikacija se koristi da bi se potvrdilo da je korisnik osoba za koju tvrdi da jeste. Nakon biometrijskog upoređivanja identitet korisnika se ili potvrđuje ili osporava (1:1 poklapanje). Biometrijska identifikacija se odnosi na postupak pretrage čitave baze podataka kako bi se utvrdio identitet korisnika (1:N pretraga).

Sistem za prepoznavanje biometrijskih osobina je, zapravo, sistem za prepoznavanje šablona (obrazaca, šara) koji uoči osobinu, izdvoji njene odlike i zatim je na osnovu njih uporedi sa ostalim osobinama iz baze. Proces prepoznavanja uključuje dve glavne faze: upis i prepoznavanje. Tokom faze upisa senzor prikuplja željenu osobinu korisnika. Na osnovu prikupljenih podataka izdvaja se reprezentacija, koja se naziva šablon. Taj šablon sadrži sve odlike prikupljene osobine i on se čuva u bazi podataka. Ta baza može biti centralizovana (forenzička analiza) ili se može nalaziti na uređaju korisnika (mobilni telefon). Druga faza je namenjena upoređivanju šablona iz baze sa onim koji se dobije nakon prikupljanja podataka o korisniku koji želi biti prepoznat. Ukoliko sličnost između uzoraka koji se upoređuju prelazi određenu granicu smatra se da je korisnik prepoznat.



1. Biometrijski sistem za kontrolu pritupa resursima bankovnih računa

Korišćenje platnih kartica u trgovini je vrlo jednostavno i brzo i u poslednjih nekoliko godina sve zastupljenije. Bankama omogućuju rasterećenje procesa usluge a korisnicima uštedu u vremenu i sigurnost. Međutim, kako je sigurnost obezbeđena tradicionalnim sistemom za kontrolu koji se zasniva na poznavanju šifre, ta sigurnost može biti kompromitovana.

Kako su biometrijski sistemi za kontrolu pristupa sigurniji i pouzdaniji od tradicionalnih, za kontrolu pristupa resursima bankovnih računa koristiće se biometrijski sistem. Pošto je suština platnih kartica brzina i jednostavnost, koristiće se skeniranje i prepoznavanje otiska prsta.

Naime, prilikom otvaranja računa skeniraće se korisnikov otisak prsta. Nakon toga sledi izdvajanje šablona koji se potom čuva u bazi podataka. Pošto je moguće da se prilikom faze prepoznavanja, iako vrlo retko, desi odbijanje pristupa korisniku kome se pristup ne bi trebalo odbiti (false reject), preporučuje se uzimanje više otisaka istog prsta korisnika (recimo 5). Kasnije se, pri prepoznavanju, upoređuju svi šabloni koji pripadaju korisniku sa onim koji je skeniran prilikom pokušaja pristupa. Na taj način se verovatnoća lažnog odbijanja još više smanjuje. Ovaj proces odgovara fazi upisa.

Prilikom korišćenja platne kartice se uz pomoć jedinstvenog broja kartice iz baze podataka prikupljaju šabloni otiska prsta korisnika kome kartica pripada. Korisnik tada prisloni odgovarajući prst na skener nakon čega se prikuplja biometrijski identifikator na osnovu koga se pravi šablon za upoređivanje. Tada nastupa proces upoređivanja datog šablona sa svim šablonima iz baze podataka koji pripadaju korisniku čija je kartica. Ako se dati šablon poklopi sa bilo kojim šablonom iz baze tada je verifikacija uspešna i korisnik može pristupiti resursima svog računa preko platne kartice. Međutim, kako može doći, iako vrlo retko, do situacije da je verifikacija uspela, a nije trebalo da uspe (false accept), preporučuje se da se zajedno sa prepoznavanjem otiska prsta koristi i šifra. Šifru bi korisnik ukucao tek nakon što se otiskom prsta potvrdi pripadnost platne kartice, i ukucana šifra bi se uporedila sa onom iz baze koja je vezana za račun korisnika kome kartica pripada. Na taj način bi se sistem dodatno osigurao. Ovaj proces odgovara fazi prepoznavanja.

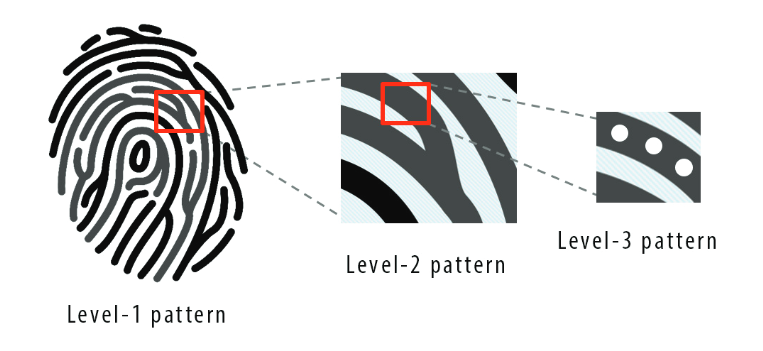
Osobine sistema:

* unimodalni sistem u kome se koristi prepoznavanje otiska prsta
* zbog dodatne sigurnosti se koristi i šifra
* koristi se proces verifikacije (1:1 poklapanje)
* sistem je sigurniji od tradicionalnog sistema

1. Proces prepoznavanja otiska prsta

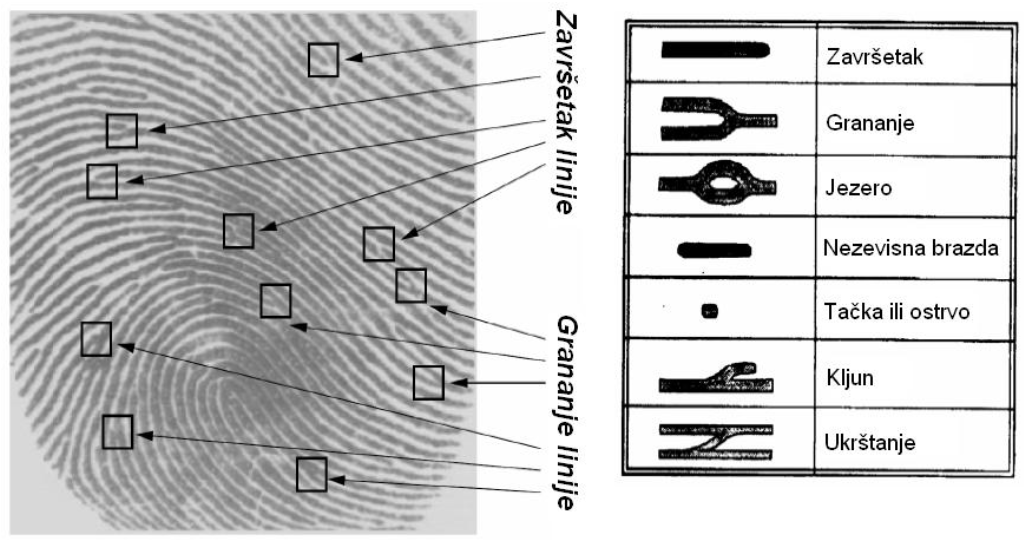
Prepoznavanje otiska prsta je jedna od najstarijih i najpoznatijih biometrijskih tehnologija. Razvoj računarske tehnologije omogućio je proširenje spektra primene ove tehnologije. Čitači otiska prsta mogu biti veoma mali i relativno niske cene. Zbog toga, ali i činjenice da se lako integrišu u tradicionalne identifikacione sisteme, je ova tehnologija široko rasprostranjena.

Prepoznavanje otiska prsta se ne vrši prostim poređenjem slika otisaka. Mnogo bolji način je izdvajanje karakterističnih tačaka na osnovu kojih se poređenje vrši. Otisak prsta je fizička osobina koja može biti sagledana kao skup šara oformljenih grebenima na koži prsta. Kada se digitalizuje može se iskoristiti za identifikovanje osobe na osnovu jedinstvenih karakteristika svakog otiska. Šare na koži prsta delimo na tri kategorije. Kategorije se razlikuju po kompleksnosti i načinu na koji pomažu prilikom prepoznavanja.



Šare prve kategorije definišu tok grebena na površini prsta. Na osnovu njih se otisak prsta može klasifikovati u jednu od 5 prepoznatljivih klasa. Šare ove kategorije se koriste da bi se ubrzao process identifikacije tako što se od svih otisaka eliminišu oni koji ne pripadaju odgovarajućoj klasi. Kako naš sistem vrši verifikaciju, a ne identifikaciju, šare ove kategorije se neće uzimati u obzir.

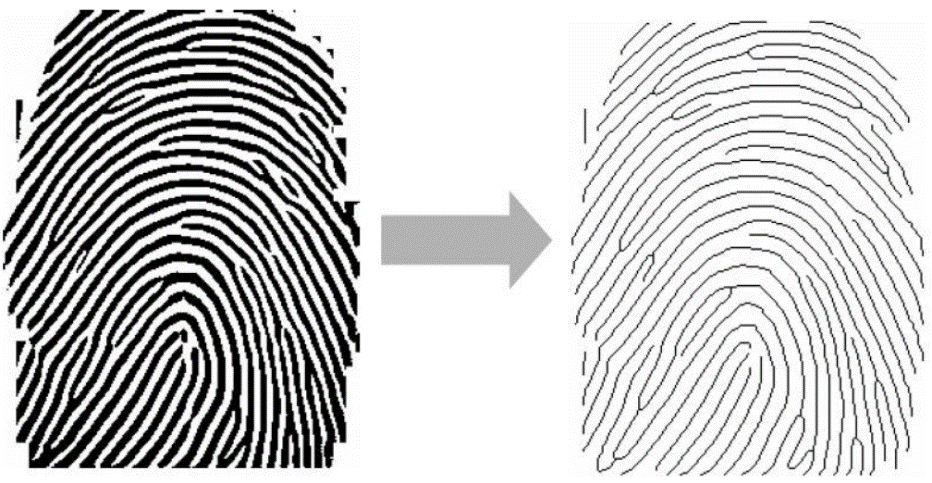
Šare druge kategorije predstavljaju lokalizovane karakteristike grebena. Ove šare čine svaki otisak prsta jedinstvenim i zbog toga ćemo se usredsrediti na prepoznavanje i izdvajanje ovih šara. Neki od tipova ovih šara su:



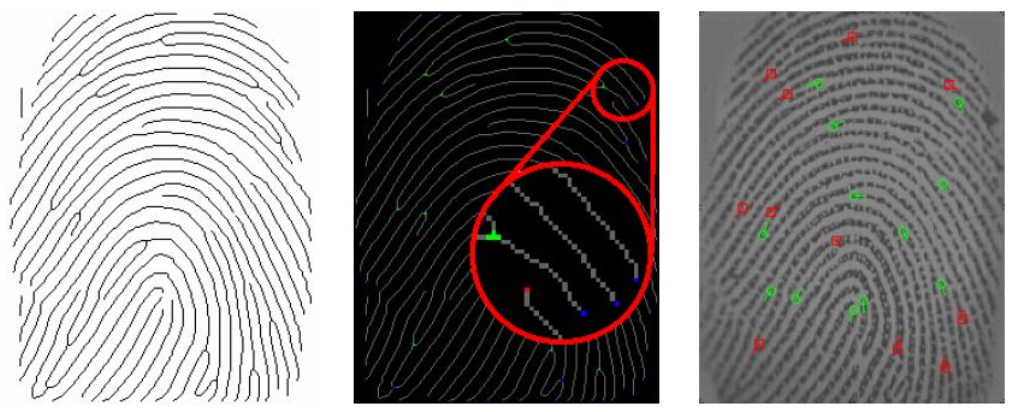
Kako ova biometrijska tehnologija postoji dugi niz godina, vremenom se došlo do zaključka da je za upoređivanje otiska prsta dovoljno prepoznati završetke i grananja. Zato će i naš sistem obraćati pažnju samo na ove tipove šara.

Šare trećeg nivoa se uglavnom koriste u forenzici i obezbeđuju najveću preciznost poklapanja uzoraka.

Pre nego što se dođe do identifikovanja i izdvajanja karakterističnih tačaka otiska potrebno je obraditi rezultat skeniranja, odnosno sliku otiska. Obrada se vrši kroz nekoliko koraka: poboljšanje kvaliteta snimka (redukcija šuma), binarizacija, istanjivanje. Istanjivanje je vrlo važno jer olakšava otkrivanje karakterističnih tačaka. Ovom obradom se ulazna slika pretvara u matricu 0 i 1, gde 1 označava greben. Ovim postupkom se širina grebena svodi na jedan piksel. Iako je ovaj korak vrlo važan za izdvajanje karakterističnih tačaka, može doći do grešaka u predstavljanju grebena, pa je potrebno dodatno obraditi sliku nakon ovog postupka.



Nakon što je slika obrađena sledi izdvajanje karakterističnih tačaka na osnovu kojih se vrši upoređivanje.

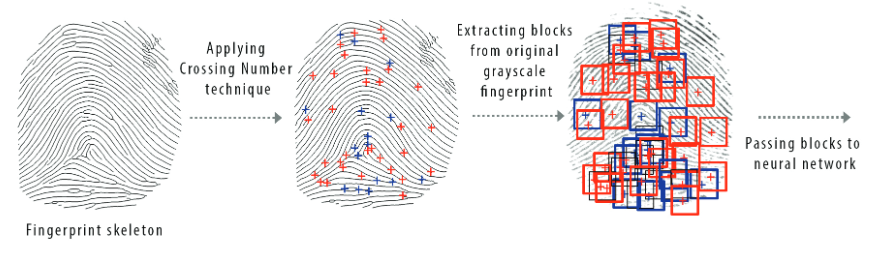


Poslednji korak je upoređivanje izdvojenih karakterističnih tačaka (tačnije njihovih pozicija, tipa, orijentacije) sa karakterističnim tačkama otisaka iz baze podataka.

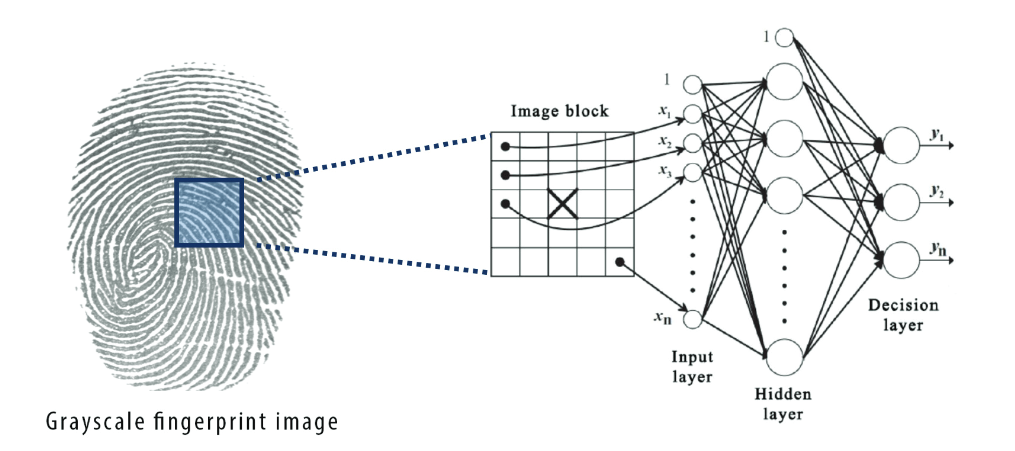
1. Rešenja korišćena u procesu prepoznavanja otiska prsta u biometrijskom sistemu za kontrolu pristupa resursima bankovnih računa

Pravilan rad biometrijskih sistema se u velikoj meri zasniva na pravilnom izdvajanju karakterističnih tačaka. Klasični sistemi izdvajaju te tačke na osnovu slike sa istanjenim grebenima. Zbog ovog pristupa može doći do izdvajanja pogrešnih karakterističnih tačaka. Takođe, takvi sistemi rade znatno lošije ukoliko je ulazna slika lošeg kvaliteta. Zbog ovih razloga, preporučuje se korišćenje veštačkih neuronskih mreža za prepoznavanje tih tačaka.

Sistem bi i dalje koristio istanjeni prikaz grebena na površini prsta, ali samo kako bi izdvojio pozicije mogućih karakterističnih tačaka. Naime, sistem bi izdvojio segmente slike (blokove piksela) za koje se veruje da sadrže karakteristične tačke. U centru segmenta bi se nalazio mogući kraj grebena ili mesto gde se greben deli. Kada se odrede svi segmenti slike sa istanjenim grebenima, tada se poklapajući segmenti originalne slike šalju neuronskoj mreži da bi se klasifikovala karakteristična tačka. Na taj način je moguće pouzdanije izdvajanje tačaka, čak i ako je slika lošijeg kvaliteta.



Segmenti slike koji se prosleđuju neuronskoj mreži su dimenzija 11x11 piksela, tako da neuronska mreža sadrži 121 ulaz (po jedan za svaki piksel segmenta). Nakon toga sledi drugi nivo koji se sastoji iz 200 skrivenih neurona. Izlaz iz neuronske mreže predstavljaju dva neurona koja formiraju vektor kojim se enkodira klasa druge kategorije šara (završetak ili grananje grebena).



Nakon što se izdvoji vektor karakterističnih tačaka sledi proces upoređivanja tog vektora sa vektorom iz baze podataka. Za proces upoređivanja koristiće se BOZORTH3 algoritam. BOZORTH3 je jedan od najboljih javno dostupnih open-source algoritama za otkrivanje poklapanja.

1. Ukratko o neuronskim mrežama

Neuronska mreža je jedan oblik implementacije sistema veštačke inteligencije, koji predstavlja sistem koji se sastoji od određenog broja međusobno povezanih procesora ili čvorova, ili procesnih elemenata koje nazivamo veštačkim neuronima.

Telo neurona naziva se čvor ili jedinica. Svaki od neurona ima lokalnu memoriju u kojoj pamti podatke koje obrađuje. Podaci koji se obrađuju su lokalni podaci kao i oni koji se primaju preko veze. Podaci koji se ovim kanalima razmenjuju su obično numerički.

Arhitektura neuronske mreže predstavlja specifično povezivanje neurona u jednu celinu. Struktura neuronske mreže se razlikuje po broju slojeva. Prvi sloj se naziva ulazni, a poslednji izlazni, dok se slojevi između nazivaju skriveni slojevi. Najčešće ih ima tri. Prvi sloj, tj. ulazni je jedini sloj koji prima podatke iz spoljašnje sredine, sledeći (skriveni) prosleđuje relevantne podatke do trećeg (izlaznog) sloja. Na izlazu trećeg sloja dobijamo konačan rezultat. Složenije neuronske mreže imaju više skrivenih slojeva. Slojevi su međusobno potpuno povezani.

Slojevi komuniciraju tako što se izlaz svakog neurona iz prethodnog sloja povezuje sa ulazima svih neurona narednog sloja. Znači, svaki čvor ima nekoliko ulaza i jedan izlaz. Jačina veza kojom su neuroni povezani naziva se težinski faktor (weight).

Značaj neuronskih mreža je u tome da mogu paralelno da obrađuju podatke, čije komponente su nezavisne jedne od drugih. Istovremeno radi više procesorskih jedinica, da bi rezultati njihove obrade prešli na sledeće jedinice (neurone). Neuronske mreže se ne programiraju, već se treniraju, tako da je potrebno dosta vremena za njihovo obučavanje, pre nego što počnu da se koriste.

Primena neuronskih mreža: obrada senzornih signala, prepoznavanje oblika, obrada slike, robotika i automatsko upravljanje, raspoznavanje i sinteza govora, obrada prirodnh jezika, obrada znaja i drugo.



1. Zaključak

Korišćenje biometrijskih tehnologija u velikoj meri privlači pažnju i dovodi u pitanje privatnost korisnika ali i svrhu u koju se koriste ovakve tehnologije. Međutim, razvoj ovih tehnologija i sistema koji ih koriste proizilazi iz činjenice da ovi sistemi imaju ogromnu primenu u sve većem broju sfera života.

U ovom radu predstavljen je jedan takav sistem koji omogućava veću bezednost korisnika i njihovih novčanih sredstava, koristeći efikasna, bezbedna i proverena rešenja koja su razvijana nekoliko godina.

1. Literatura
2. Biometrics, dostupno na: https://en.wikipedia.org/wiki/Biometrics
3. Биометрија, dostupno na: https://sr.wikipedia.org/sr-ec/Биометрија
4. Šta je biometrija, dostupno na: http://www.secamcctv.rs/biometrija/
5. Identifikacioni sistemi, Prepoznavanje otiska prsta, dostupno na: https://www.ucg.ac.me/skladiste/blog\_7446/objava\_21244/fajlovi/Prepoznavenje otiska prsta.pdf
6. Neuronske mreže, dostupno na: https://sh.wikipedia.org/wiki/Neuronske\_mreže
7. Fingerprint recognition system using artificial neural network as feature extractor: Design and performance evaluation – Pavol Marak, Alexander Hambalik, Mathematical Institute, Slovak Academy of Sciences