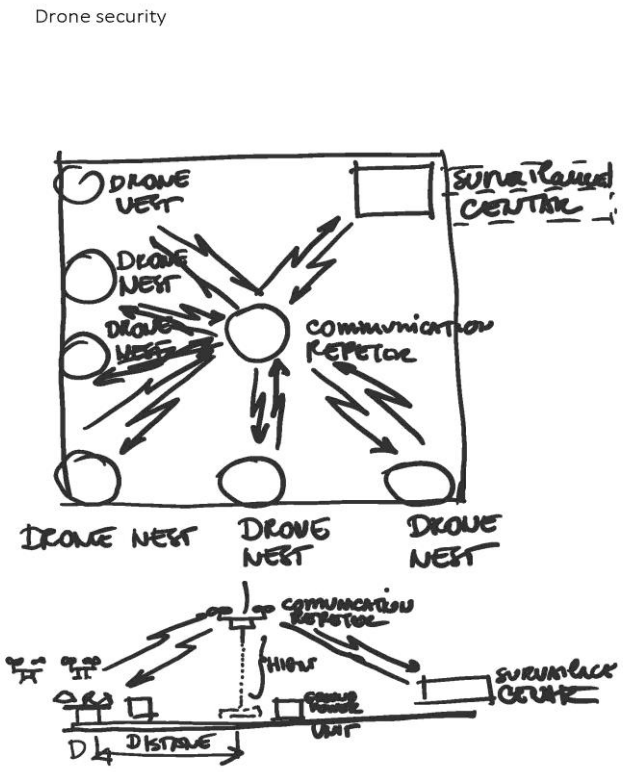
1. Sistem za video nadzor teško dostupnih ili nedostupnih velikih teritorija

Video nadzor velikih površina zahteva razvoj složene stacionarne infrastrukture koja ima za cilj snimanje i prenos signala preko repeticionih stanica do centralnog sitema koji vrši obradu podataka i prezentaciju istih operateru. Za razvoj i instalaciju takvih sistema potrebno je izgraditi potrebnu infrastrukturu uključujući dostupne saobraćajnice, dovesti potrebne izvore napajanja, postaviti odgovarajuće kamere na određena mesta i sl.

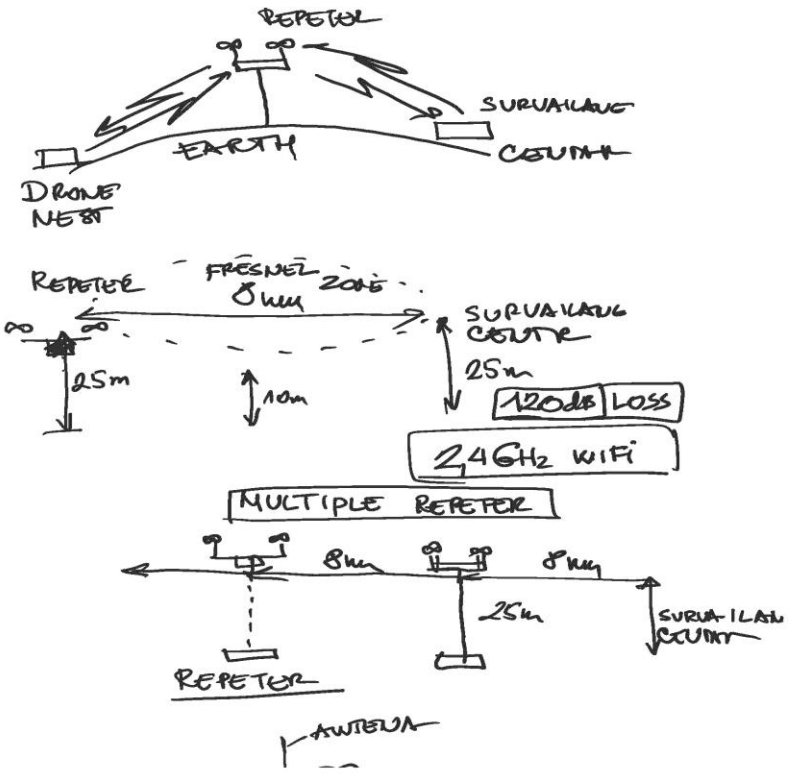
Predložen sistem je potpuno autonoman i mobilan, a baziran na "dron" tehnologiji. Koncipiran je tako da se samo skupljanje podataka i video slika vrši nezavisnim izviđačkim stanicama koje su opremljene dronovima. Isti su smesteni u odgovarajućim gnezdima koji imaju sopstvene izvore napajanja i bazne upravljačke stanice za skupljanje podataka kao i upravljanje samom izviđačkom stanicom(Slika 1.1).



Slika 1.1

Za prenos podataka na velike razdaljine koristili bi se stacionarno postavljeni dronovi koji su pozicionirani na potreboj visini (od 25m do 50 m), u određenim razmacima (9 do 15 km) i povezani su zičanom vezom sa zemaljskom stanicom iznad koje lebde, a koja služi za obezbeđivenje napajanja prenosne stanice kao i za backup podataka u slučaju privremenog prekida linka kao i za napajanje

zamenskih dronova koji se šalju u izviđačke stanice (Slika 1.2).



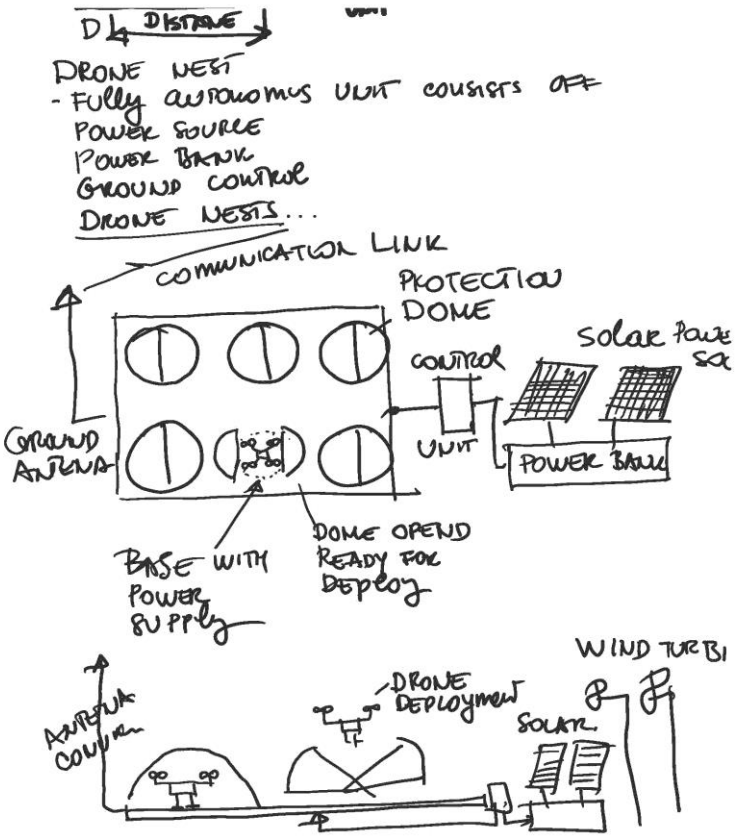
Slika 1.2

Sama kontrolna jedinica ima sve elemente stanice za video nadzor sa mestom za operatera koji upravlja i daje naloge samostalinim nezavisnim stanicama i prikuplja podatke koji one šalju.

<u>Nezavisna istraživačka stanica</u>

Komponente nezavisne istraživačke stanice su(Slika 1.3):

- Gnezdo dronova
- 12 dronova za dnevno izviđanje
- 12 dronova za noćno izviđanje
- 4 drona za onesposabljanje objekata
- Individualna platforma za napajanje dronova se odgovarajućim kupolama za čuvanje dronova dok su u gnezdu
- Kontrolna bazna stanica koja kontroliše rad, vrši monitoring statusa dronova u gnezdu i vrši skupljanje i čuvanje podataka u slučaju privremenog prekida veze sa stanicom za video nadzor.
- Power bank, solarni izvor napajanja, vetrogenerator, kao i rezervni generator sa 24-satnom rezervom goriva u slučaju loših meteo uslova.

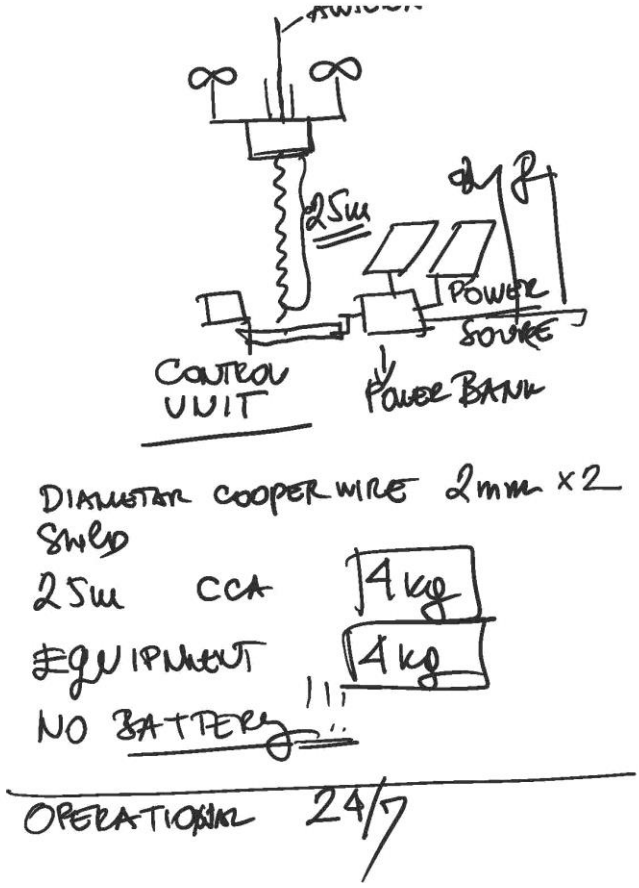


Slika 1.3

Stanica za prenos podataka

Stanica za prenos podataka se sastoji od (Slika1.4):

- Drona sa minimalnim sopstvenim izvorom napajanja i žičanom vezom sa zemaljskim modulom
- Zemaljski modul koji ima namotaj zice sa kontrolisanom motalicom iste
- Kontrolni modul koji vrši monitoring rada stanice ima mogućnost snimanja podataka u slučaju privremenog prekida prenosa istih
- Dve platforme sa kupolama za opsluživanje zamenskih dronova
- Power bank, solarnog izvora napajanja, vetrogeneratora, kao i rezervnog generatorasa 24-satnom rezervom goriva u slučaju loših meteo uslova.



Slika 1.4

Princip rada :

Nezavisna izviđačka stanica prema statusu i prema potrebama operatera vrši odabir izviđačkog drona za patrolu i upućuje isti prema ruti koja je tražena.Ruta može da se koriguje i tokom misije. Dron vrši video nadzor leteći na većoj visini i u realnom vremenu vrši raspoznavanje događaja na prostoru koji izviđa. U slučaju da je detektovano pomeranje ili IC promena, dron se spusta na nižu visinu i locira se iznad predmeta koji je izazvao poremećaj. Baza automatski šalje jos jedan dron koji ostaje na vecoj visni u stacionarnom položaju i služi za rezervnu upotrebu u slučaju nužde.

Signal se prenosi u realnom vremenu preko Stanica za prenos podataka do operatera u kontolnoj jdinici za video nadzor.

Nadogradnja sistema može da se razvija u smeru osposobljavanja sistema da nakon raspoznavanje vrši i neutrlizaciju odnosno onesposobljavnje uočenog objekta. Bazna stanica lansira dron za onesposobljenje

koji kad se nađe u blizini pozicije označene od strane izviđačkog drona pušta *micro drone swarm* koji neutrališe objekat.

U slučaju da se odluka ne može doneti brzo, bazna stanica odlučuje i šalje zamenu patrole, vraća predhodnu u gnezdo gde se vrši napajanje izviđačkih donova i priprema za sledeću misiju …

U slučaju da je doslo do privremenog prekida signala bazna stanica preuzima podatke sa drona prispelog u gnezdo i distribuira isto odmah po ponovnom uspostavljanju veze.

Baza sve vreme vrši monitoring stanja dronova na patroli I vraća iste u gnezdo i šalje sledeće na misiju.

U slučaju da je uočena potreba za zamenom drona zbog kvara ili nezadovoljavajućeg tehničkog stanja, bazna stanica šalje zahtev operateru koji šalje zamenu po ruti gde se nalaze Stanice za prenos podataka. Na tim mestim zamenski dron sleće radi napajanja. Posle napajanja baterija, nastavlja prema Nezavisnoj baznoj stanici.

Razvoj sistema i integracija istog zahteva multidisciplinarni pristup jer konačan tehnički zadatak koji proistekne iz konkretnih potreba sa terena može da se reši bez intervencije na hardveru. Bazna stanica može da se opremi novim tipovima dronova.Takodje, može u slučaju potrebe da se izvrši vrlo lako i zamena Stanica za prenos podataka.Sistem bi se nadograđivao softverski razvojem novih algoritama.

Sistem zahteva razvoj sledećih algoritama:

- Algoritam za detekciju, raspoznavanje i prepoznavanje (potprojekat 2).
- Algoritam za samostalno delovanje i donošenje odluka u slučaju prekida sa operaterom (AI).
- Algoritam za prepoznavanje pretnje ometanja i prelazak na samostalno delovanje (AI).
- Algoritam prilagođavanja prekidu komunikacije.

2. Softver za prepoznavanje lica i objekata

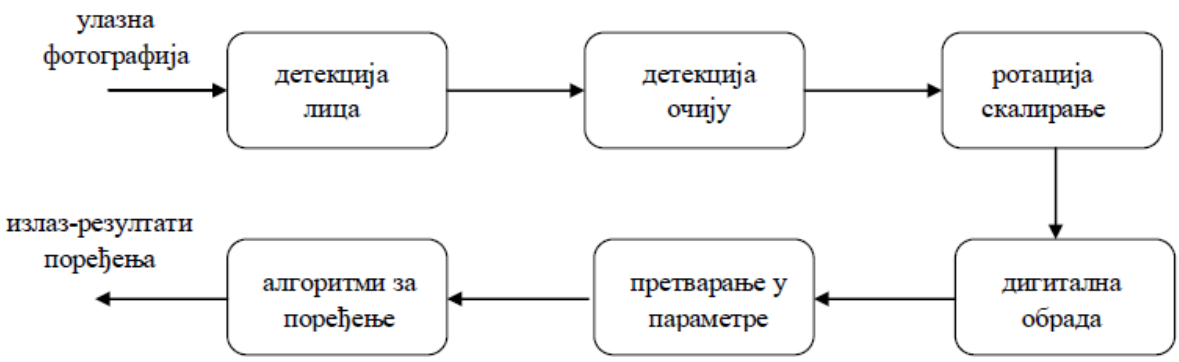
2.1 Softver za prepoznavanje lica

Prepoznavanje lica je vrlo zahtevan zadatak, koji je tradicionalno podrazumevao određen stepen inteligencije, koji čovek sa relativnom lakoćom ispunjava, ali nije jednostavno preneti tu logiku na računar, odnosno implementirati je tako da se može izvršavati automatski sa velikim stepenom preciznosti. Među najpreciznijim biometrijskim metodama su DNK analiza, otisak prsta i zenica oka, ali zbog različitih ograničenja nisu uvek primenljivi. Osnovna prednost metode prepoznavanja lica je lakoća dolaženja do informacija. Da bi nekoga prepoznali uz pomoć DNK koda, otiska prsta ili skeniranja zenice oka, najpre moramo imati u bazi takve informacije. Dalje, svaki put kada hoćemo da identifikujemo neku osobu, neophodno je da ta osoba sarađuje, tako što joj uzimamo otisak prsta, uzorak DNK ili skeniramo zenicu oka i tako dobijeni podatak upoređujemo sa podacima u bazi.

Sa druge strane, fotografije su postale vrlo uobičajen materijal koji se sa lakoćom nabavlja i pronalazi, s obzirom na sve veću pokrivenost javnih površina kamerama, a i rasprostranjenost fotografija na društvenim mrežama i uopšte internetu. Priroda zadatka računarske identifikacije osoba nam omogućuje da, uglavnom, najlakše dođemo do fotografija lica neke osobe koja nam je od interesa, mnogo jednostavnije nego do neke druge biometrijske karakteristike. Pecimo, prilikom obezbeđivanja državne granice, banke, sportske dvorane ili drugog objekta od važnosti, može se na odgovarajuće mesto na ulazu postaviti kamera i tako automatski pribaviti više kvalitetnih fotografija svake osobe koja ulazi u objekat bez njenog aktivnog učešća, i bez zastoja.

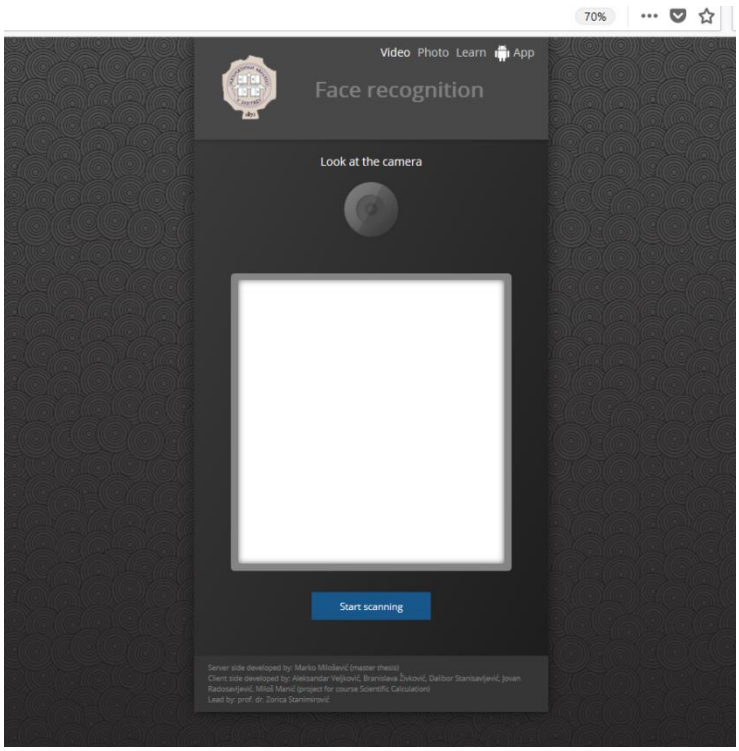
Prepoznavanje lica je biometrijska metoda koja doživljava ekspanziju zahvaljujući mogućnostima savremenog hardvera, a služi za automatsko prepoznavanje i identifikaciju osoba na osnovu digitalnih fotografija njihovih lica. To se postiže na taj način što se uneta fotografija upoređuje sa digitalnim opisima fotografija u bazi podataka. Napomenimo da se prepoznavanje lica, kao biometrijska metoda, ne može smatrati apsolutno pouzdanom, ali predstavlja veoma korisno pomoćno sredstvo koje se koristi u kombinaciji sa drugim informacijama i bazama podataka koje bezbednosne službe poseduju, u cilju prevencije bezbednosnih pretnji i otkrivanja počinilaca krivičnih dela.

Polazna tačka za istraživanje je postojeći softver za prepoznavanje lica, koji uspešno kombinuje postojeće algoritme u ovoj oblasti, koristeći prednosti svakog od njih u cilju postizanja što preciznijih rezultata. Softver je razvijen u okviru zajedničkog projekta Matematičkog fakulteta i Fakulteta bezbednosti Univerziteta u Beogradu. Na Slici 2.1. prikazana je uprošćena šema korišćenog algoritma za prepoznavanje lica.

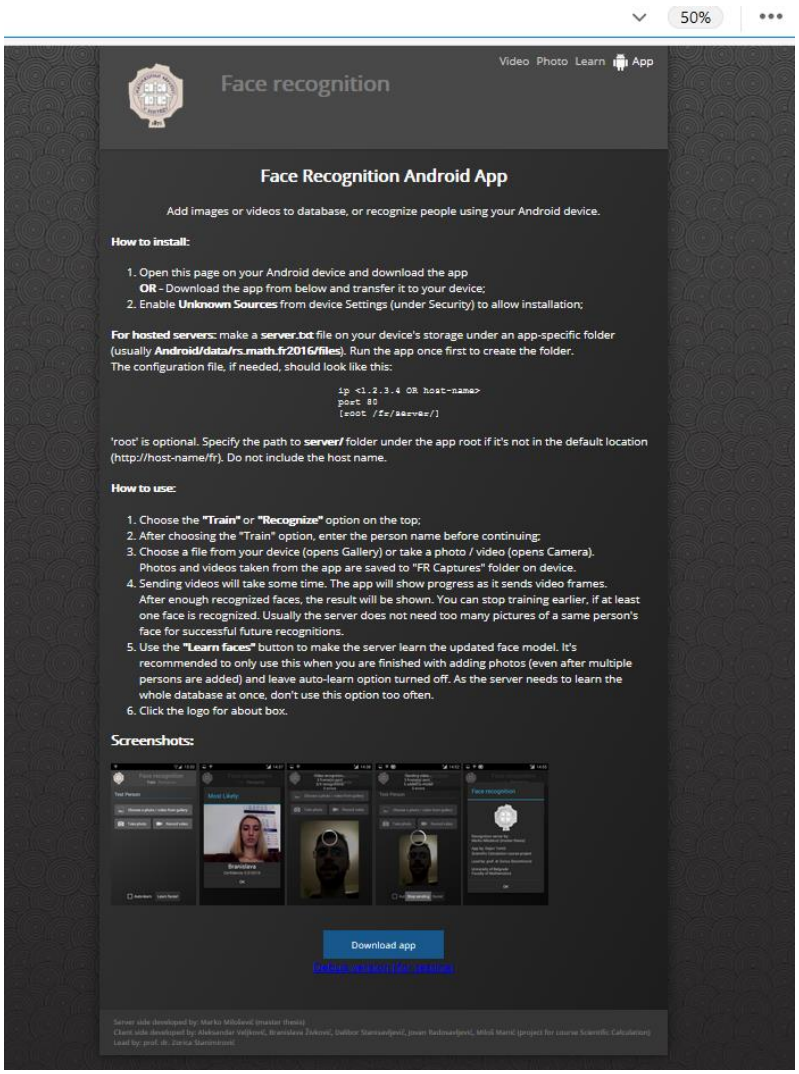


Slika 2.1. Osnovni dijagram softvera za prepoznavanje lica

Web aplikacija softvera (Slika 2.2) je dostupna na strani http://tocsearch.com/fr/. Razvijena je i android aplikacija (Slika 2.3), koja je dostupna na strani http://tocsearch.com/fr/app.html.



Slika 2.2 Web aplikacija softvera za prepoznavanje lica



Slika 2.3. Android aplikacija softvera za prepoznavanje lica

Razvijeni softver je testiran na četiri baze fotografija različitih težina (faces94, faces95, faces96 i grimace), koje predstavljaju baze predstavljaju standardne baze za testiranje softvera za prepoznavanje lica. Kako je razvijeni softver dao izuzetne rezultate na ovim bazama (99% pouzdanosti za bazu faces94, 97% pouzdanosti za bazu faces95, 95% pouzdanosti za bazu faces96, 100% pouzdanosti za bazu grimaces), to nam daje dobru osnovu za nastavak istraživanja u cilju daljeg unapređenja. Uz adekvatne modifikacije i prilgođavanja, softver se može koristiti kao alat za asistenciju u odlučivanju u različitim oblastima, među kojima je najznačajnija oblast bezbednosti.

Plan razvoja:

1. Unapređenja i modifikacije postojećeg softvera za prepoznavanje lica u više pravaca, pre svega u pogledu ubrzanja vremena izvršavanja. S obzirom da softver koristi veći broj modela i algoritama, očekivano mu je potrebno više prostora na disku i u memoriji računara, i algoritam se nešto duže izvršava. Dalje, neophodno je obezbediti veću konfigurabilnost sistema. Konkretno, za različite primene trebalo bi obezbediti različito vreme izvršavanja; ukoliko pouzdanost nije najznačajnija, treba obezbediti korisniku mogućnost da balansira između kvaliteta i performansi.Optimizacija rezultata, implementacija dodatnih algoritmi za svaki od koraka u prepoznavanju lica i oblika i testira njihov učinak na različitim bazama.
2. Kreiranje baze fotografija za potrebe korisnika, kako bi softver odgovorio konkretnim potrebama, i taj set se koristi kao najbitniji u preostalom testiranju rešenja. Formira se baza objekata (oblika) koja je od interesa za korisnika, i testira dobijeno rešenje.
3. Razvoj i testiranje(u saradnji sa korisnikom) grafičkog interfejsa i preciziranje skupa komandi dostupnih iz spoljašnjih servisa. Obučavanje korisnika na konkretnim primerima za formiranje i testiranje baza fotografija lica.

Planirane primene softvera za prepoznavanje lica:

1. Integracija u sistem za video nadzor teško dostupnih ili nedostupnih velikih teritorija (potprojekat 1) u cilju detekcije, raspoznavanja i prepoznavanja lica snimljenih iz drona.

2. Integracija predloženog softvera sa bazom TOC-search (potprojekat 3), ali i sa nekim drugim, profesionalnim bazama podataka. Iako informacije koje daje predloženi softver imaju visok stepen pouzdanosti, tek kombinacijom sa drugim metodama i unakrsnom proverom sa podacima iz profesionalnih baza možemo dobiti kompletan, pouzdan sistem bezbednosti.

3. Implementacija u sistem za identifikaciju osoba, odnosno sigurnosni sistem koji služi automatskom obezbeđenju prolaska lica kroz ciljane tačke (prolaz, vrata, kapija) na osnovu biometrijskih karakteristika.Krajnji rezultat podrazumeva softversko rešenje koje u kombinaciji sa adekvatnim vratima ili kapijom računarski kontroliše prolaz i potpuno autonomno, a istovremeno pouzdano, kontroliše prolazak osoba bez potrebe da nose dodatne kartice ili ključeve koje su podložne gubljenju ili krađi. Osoba čiju identifikaciju želimo da sprovedemo bi na tački prolaska prolazila pored kamere koja šalje fotografije softveru za prepoznavanje lica. i, Ukoliko je osoba identifikovana, automatski se odobrava prolaz, odnosno otvara elektronska brava. Ukoliko osoba ne bude pronađena u bazi (u relativno malom broju slučajeva) mogla bi da se autentifikuje osnovnim metodom, otiskom prsta ili unosom šifre. Postiglao bi se brži protok, bez usporenja, s obzirom da bi bez korisničke interakcije bilo moguće autentifikovati osobu u visokom broju slučajev.Svaki kako uspešan tako i neuspešan pokušaj prolaska osoba bi se detaljno beležio sa video zapisom i bio dostupan administratorima sistema za analizu.

2.2 Softver za prepoznavanje objekata

Softversko rešenje planirano ovim projektom podrazumeva sistem koji uz adekvatne trening podatke može da klasifikuje tipove objekata (recimo, vozila, stambeni ili drugi objekti, oružja) ili oblika sa visokom preciznošću, zavisno od kvaliteta ulaznih informacija.

Dobijeni produkt bi bio servis pogodan za integraciju sa različitim sistemima zaštite i bazama podataka, lako dostupan i napravljen tako da ga je lako prilagoditi različitim novim zahtevima koji ti spoljašnji sistemi donose.

Osnovni korisnički interfejs podrazumeva vizuelni pristup opcijama pravljenja trening seta podataka (recimo baza fotografija oblika čije prepoznavanje želimo da postignemo, ili objekata), kao i opciju klasifikovanja sledeće fotografije sa snimka kamere, ili iz već ranije dostupne datoteke sa diska ili globalne računarske mreže.

Korisnik dobija i precizno dokumentovan skup komandi koje servis pruža, što kao rezultat ima laku implementaciju sprege sa bilo kojim drugim uže specijalizovanim softverom.

U planu je da ovo rešenje omogućuje lako integrisanje dodatnih algoritama (ako donose osetne prednosti) koji se u međuvremenu pojave u okviru svetskih istraživanja ovog problema, što je vrlo čest slučaj, s obzirom na aktuelnost teme u naučnim okvirima.

Plan razvoja:

1. Implementacija osnovnog algoritma sa jednostavnom optimizacijom ulaznih podataka (obradom i popravljanjem kvaliteta podataka – fotografija). Nakon te faze se vrši testiranje dobijenog rešenja, i upoređivanje rezultata dobijenih različitim algoritmima i procedurom optimizacije.
2. Optimizacija rezultata dobijenih u prvim fazama projekta. Implementiraju se dodatni algoritmi za svaki od koraka u prepoznavanju objekata ili oblika i testira njihov učinak na različitim bazama. Istoremeno, razvija se baza za potrebe korisnika, kako bi softver bio što bolje prilagođen konkretnim potrebama, i taj set se koristi kao najbitniji u preostalom testiranju rešenja. Započinje se sa implementacijom modifikacije korišćenih algoritama u cilju prepoznavanja objekata i vrše se prva testiranja.
3. Optimizacija performansi i preciznosti algoritama za prepoznavanje objekata ili oblika. Formira se baza objekata (oblika) koja je od interesa za korisnika, i testira dobijeno rešenje. Paralelno se razvija, u saradnji sa korisnikom, grafički interfejs i precizira skup komandi dostupnih iz spoljašnjih servisa. Obučavaju se korisnici sa konkretnim primerima i daju pomoć i smernice za formiranje i testiranje baza fotografija objekata (oblika).

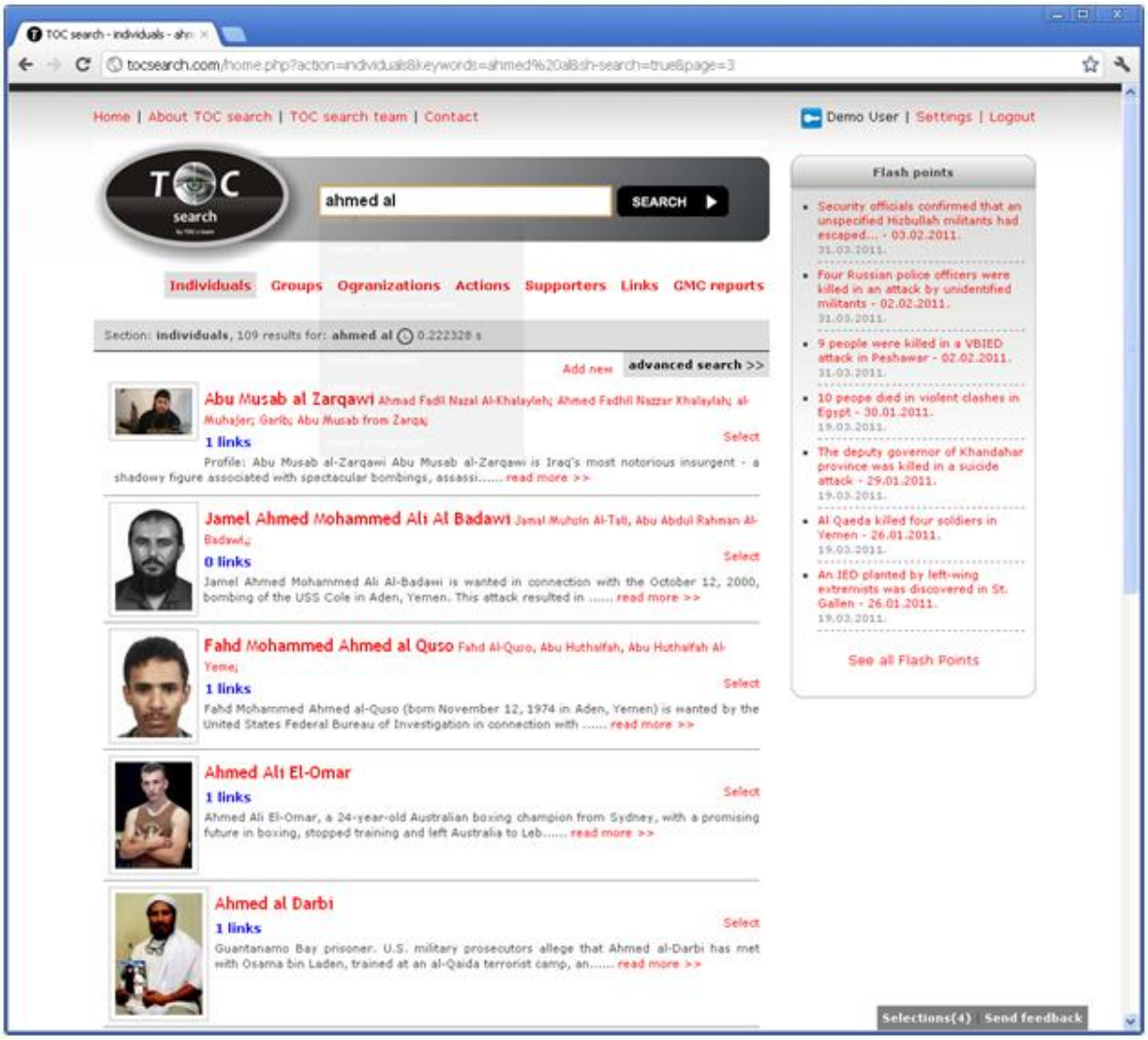
Planirane primene softvera za prepoznavanje lica:

1. Integracija u sistem za video nadzor teško dostupnih ili nedostupnih velikih teritorija (potprojekat 1) u cilju detekcije, raspoznavanja i prepoznavanja objekata i oblika snimljenih iz drona

4. **Baza podataka o terorizmu i organizovanom kriminalu**

TOCsearch (Terrorist and Organized Crime Search) je računarska baza koja sadrži veliku količinu podataka iz javno dostupnih sredstava informisanja obrađenih od strane profesionalnog kadra iz evropskog centra za obučavanje u oblastima bezbednosti George C. Marshall.Fakultet bezbednosti i Evropski centar za studije bezbednosti - George C. Marshal su 2007. godine potpisali ugovor o saradnji. U okviru ove saradnje, razvojni tim baze je dobio pristup izveštajima o terorizmu i organizovanom kriminalu na globalnom nivou koje sastavljaju postdiplomci George C. Marshal centra na osnovu različitih otvorenih izvora, na nedeljnom nivou. Ti izveštaji predstaljaju jedan od glavnih izvora podataka otvorenog tipa u bazi.

TOC searchbaza je aktivna i dostupna na adresi www.tocsearch.com, a razvijena je i njena android aplikacija. Bazasadrži sveobuhvatne podatke o teroristima i kriminalcima, terorističkim i kriminalnim grupama i organizacijama, njihovim pomagačima, napadima, lokacijama terorističkih i kriminalnih aktivnosti, kao i o vezama između svih pomenutih kategorija (Slika 4.1). Servis www.tocsearch.com pokazao se kao veoma jednostavan i efikasan dodatni alat za poboljšanje mera bezbednosti na raznim događajima i situacijama od visokog rizika kao i tokom edukacije studenata, istraživačkog i praktičnog rada.Ovaj jedinstven i javno dostupan internet servis omogućava korisnicima da u samo nekoliko koraka provere da li je određena osoba pod sumnjom da je povezana s terorističkim aktivnostima ili organizovanim kriminalom. Baza je do sada uspešno primenjena tokom organizacije Olimpijskih igara u Pekingu, Kina 2008, Svetske izložbe u Kini 2010 i Svetskog prvenstva u fudbalu 2011. Svakodnevno je koriste studenti i istraživači fakulteta, univerziteta i instituta, kao i stručnjaci u oblasti bezbednosti iz zemnje i inostranstva.

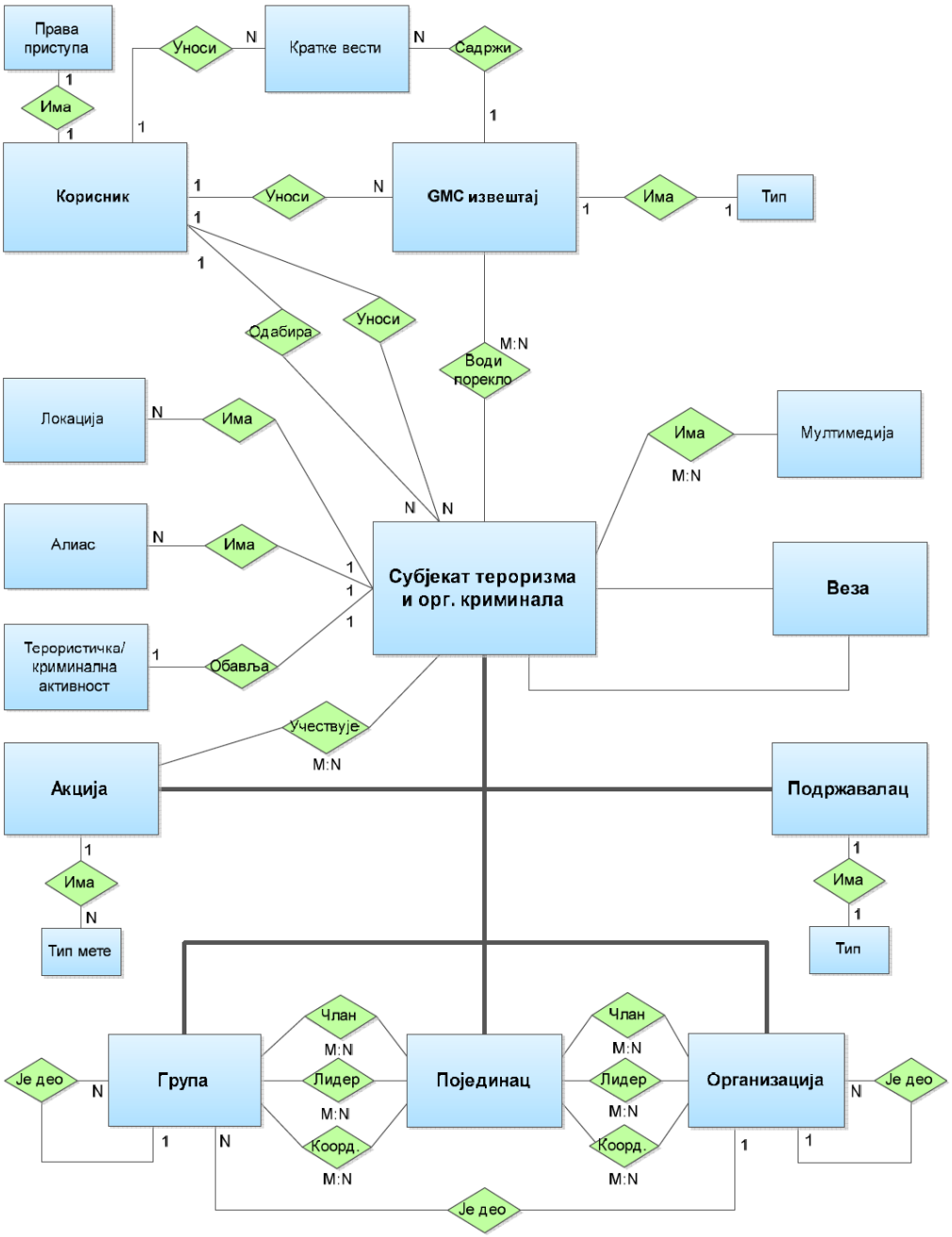


Slika 4.1 : Prikaz korisničkog interfejsa za pretraživanje podataka

Pored osnovnih informacija o osobama koje su na neki način učestvovale u nekom terorističkom/kriminalnom činu baza sadrži detaljne informacije o različitim aktivnostima u kojima se individualac pominjao, kao što su bombaški napad, nuklearni napad, sajber napad i tome slično. Takođe, TOCSearch sadrži i informacije o grupama i organizacijama koje se bave nekim od aktivnosti od interesa, kao i različitim organizacijama ili osobama koje nisu direktno učestvovale u terorističkim akcijama ili organizovanom kriminalu, ali su im pružale neku vrstu podrške (finansijsku, medijsku, itd.).

Korišćen je relacioni model podataka koga karakteriše mogućnost čivanja različitih tipova podataka kao što su tekst, slike, audio i video sadržaji (Slika 4.2). Osnovni entiteti koje baza obuhvata su pojedinci, grupe, organizacije, akcije i podržavaoci terorizma i organizovanog kriminala. Posebnu vrednost ove baze podataka sadrže informacije o međusobnim povezanostima subjekata u bazi, takozvanim linkovima. Tu se beleže sve eventualne informacije o srodstvu, poznanstvu, zajedničkim akcijama i tome slično.Tokom

razvoja aplikacije korišćen je inkrementalni pristup. Veći poslovi su podeljeni u manje i postavljani su prioriteti za određene funkcije. Na taj način je postignuta veća efikasnost rada.

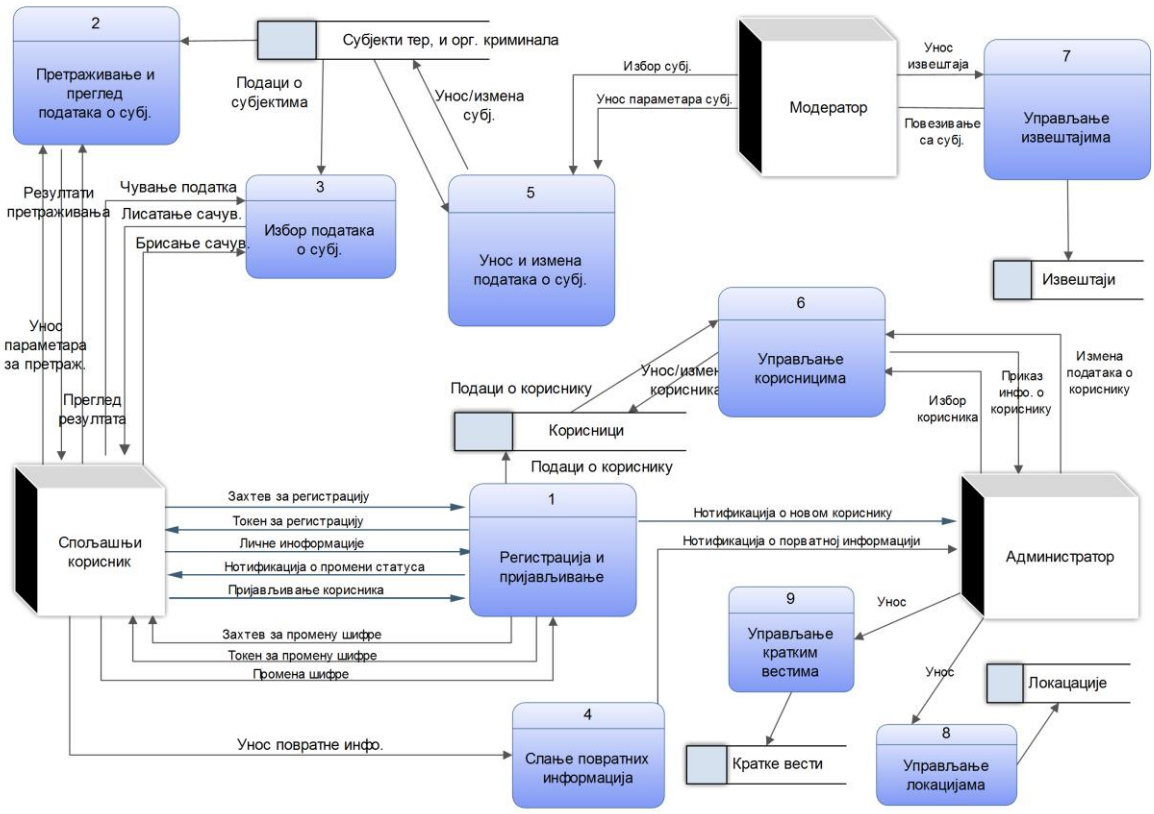


Slika 4.2 : Relacioni model baze podataka koji obuhvata sve entitete i podentitete u bazi, i njihov međusobni odnos.

Na Slici 4.3 prikazan je dijagram nultog nivoa koji prikazuje sve glavne unutrašnje procese koji se u bazi odvijaju, kako su procesi međusobno povezani, spoljašnje entitete i interakciju procesa sa bazom podataka

Osnovne karakteristike po kojima se baza TOCsearch razlikuje od postojećih baza sa sličnim sadržajem su:

- Podrška za sve kategorije subjekata terorizma i organizovanog kriminala;
- Čuvanje veza (linkova) između subjekata, kao i osobina tih veza;
- Evolucija i unapređenje unetih podataka - podaci se ažuriraju tokom vremena;
- Čuvanje i klasifikovanje podataka iz otvorenih i poverljivih izvora;
- Podrška za sve tipove podataka: tekst, slike, zvučni i video zapisi;
- Različite uloge korisnika u bazi za pregled i upravljanje podacima;
- Različiti nivoi pristupa podacima.



Slika 4.3: Dijagram nultog nivoa za bazu TOC search

Plan daljeg razvoja:

- Unapređenje tehničkih karakakteristika postojeće baze u cilju poboljšanja efikasnosti pretraživanja, brzine pristupa, prezentacije rezultata pretrage itd.
- Nadogradnja novim funkcijama koje su prepoznate kao korisne tokom samog korišćenja
- Unapređenje postojeće android aplikacije
- Integracija sa softverom za prepoznavanje lica
- Integracija sa softverom za 3D rekonstrukciju lica na osnovu 2D fotografija
- Mogućnost otvaranja jedne ili većeg broja instanci sistema slične vrste, za specifične potrebe, sa podacima koji su njemu od interesa. Bilo bi moguće takav sistem instalirati na serverima korisnika, u cilju očuvanja potpune privatnosti podataka.
- U skladu sa potrebama korisnika, biće razvijen poseban sistem enkriptovanja podataka u cilju bezbednosti, poštujući najmodernije i najrigoroznije standardi bezbednosti podataka. Imajući u vidu osetljivost podataka,sve kritične informacije unutar baze se enkriptuju, tj. obezbeđuje se sistem takav da njihova eventualna krađa usled nekog npr. računarskog napada ne pruža počiniocu nikakvu korist, jer nema načina da ih pročita (dekriptuje).

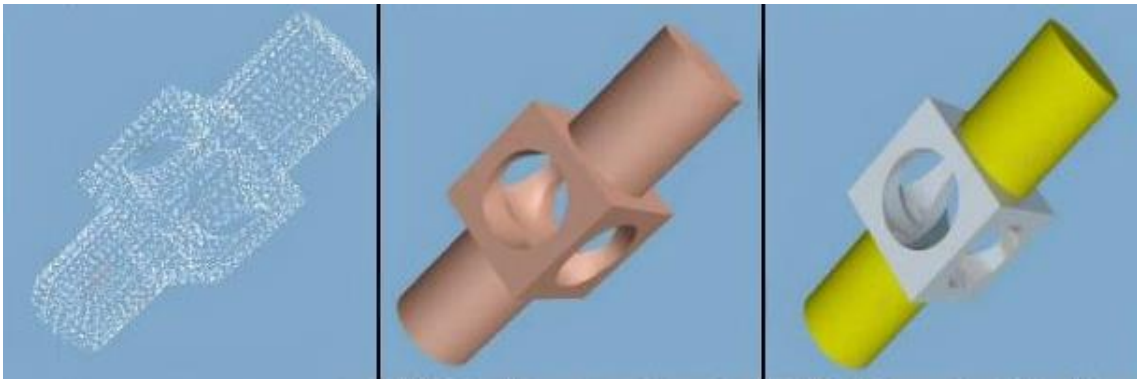
- Primena matematičkih metoda kao što su modeliranje događaja i statistički testovi prilagođeni problematici
- Razvoj alata za predikciju trendova u terorizmu i organozovanom kriminalu na lokalnom i globalnom nivou.

5. **Softver za 3D rekonstrukciju objekata i lica korišćenjem 2D fotografija**

Automatska 3D rekonstrukcija predstavlja važnu oblast kompjuterske vizuelizacije, koja u poslednje dve decenije ima važnu primenu u kompjuterskoj grafici, virtuelnoj realnosti, medicini, komunikacijama, i slično.Proces rekonstrukcije je inverzan procesu dobijanja 2D slike na osnovu 3D modela ili scene.Za ulazni skup slika, koje predstavljaju 2D projekcije delova nekog trodimenzionalnog modela ili delova scene, moguće je izvršiti automatsku rekonstrukciju tog modela, odnosno scene. U skupu mora biti najmanje dve slike, budući da se na osnovu jedne slike ne može dobiti informacija o dubini bilo kog piksela. Međutim, u praksi je broj slika obično veći, od nekoliko desetina do nekoliko stotina, što zavisi od veličine modela, terena ili scene koja se rekonstruiše.Ključna stvar za ovaj proces čini način na koji su povezane slike od kojih je potrebno generisati model.U praksi se zbog raznih spoljašnjih faktora ne može uvek verodostojno rekonstruisati model. Na primer, slike mogu imati različitu ekspoziciju ili ne moraju svi delovi modela biti vidljivi. Proces automatske rekonstrukcije se sastoji od sledeće četiri faze:

1. određivanje položaja kamera – u ovoj fazi se na osnovu početnog skupa slika vrši procena položaja kamera u prostoru;
2. određivanje dubine tačaka – na osnovu početnih slika i određenih položaja kamera se za sve značajne tačke određuju njihove dubine, čime se približno može odrediti njihova pozicija u prostoru;
3. rekonstrukcija modela – na osnovu dubina tačaka i položaja kamera vrši se precizna ili aproksimativna rekonstrukcija modela;
4. teksturisanje – u ovoj fazi se vrši bojenje generisanog neteksturisanog modela.

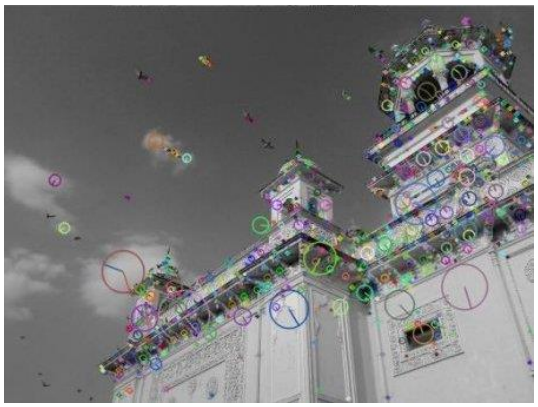
Na Slici 5.1 su prikazane tri faze generisanja 3D modela, pod pretpostavkom da je na osnovu ulaznih slika određen položaj kamera. Na levom delu slike se nalazi skup značajnih tačaka sa svojim dubinama. U ovom slučaju je on jednobojan, ali je u praksi pored dubine, nekad poznata informacija i o boji tačke. Naredna faza predstavlja rekonstrukciju modela, koji predstavlja neobojenu površ u 3D prostoru (deo slike u sredini). Konačno, na desnom delu slike je prikazan finalni teksturisan model.



Slika 5.1. Skup tačaka sa dubinama, neteksturisan i teksturisan model

Određivanje položaja kamera

Prvi deo u procesu automatske rekonstrukcije 3D modela jeste računanje parametara senzora kamere, kao i računanje pozicija kamera u prostoru. Parametri senzora kamere se sastoje od žižne daljine, koeficijenata distorzije, kao i tačke projekcije centra perspektive na ravan slike. Parametri senzora služe računanju pozicije tačke u 3D prostoru kamere. Pozicija kamere u prostoru se sastoji od rotacije i translacije. Ovi parametri služe za računanje pozicija tačaka u 3D prostoru sveta.Proces pozicioniranja kamera počinje određivanjem ključnih tačaka na slikama. Detekcija ključnih tačaka se vrši pomoću SIFT algoritma (Slika 5.2).



Slika 5.2. Skup ključnih tačaka detektovanih uz pomoć SIFT algoritma

Nakon detekcije ključnih tačaka, potrebno je upariti ključne tačke sa različitih slika. Tačke za koje se pronađe odgovarajući par na dve ili više slika služe u rekonstrukciji scene i pozicije kamera. Uparivanje tačaka može da se poboljša davanjem inicijalnih pretpostavki o pozicijama kamera. Ukoliko se slika telefonom, kao što je ovde slučaj, moguće je odrediti rotaciju telefona na osnovu senzora. Time se može smanjiti obim pretrage parova ključnih tačaka u ostalim slikama, a time i pojava da će neadekvatne tačke biti uparene. Postoji nekoliko bitnih testova prilikom uparivanja. Jedan od njih je test ogledala. Ukoliko se za neku tačku nađe par na istoj slici koji je bliže po parametrima nego tačka sa druge slike, taj potencijalni par se proglašava nevažećim. Ovo je važno u situacijama gde postoji dosta ponavljajućih tekstura. Pored ovog testa, implementiran je test ugla i test veličine ključne tačke. Svi ovi testovi smanjuju verovatnoću uparivanja neadekvatnih tačaka.

Nakon uparivanja, generisan je skup kamera i uparenih tačaka čije tačne pozicije u prostoru nisu poznate. Potrebno je optimizovati te pozicije na osnovu trenutnog znanja o samoj sceni. Ovde je izvršena optimizacija grafa gde se u svakoj iteraciji pomeraju tačke i kamere.Za svaku tačku poznat je skup kamera iz kojih je ona vidljiva. Na osnovu toga se takva tačka može projektovati na ravan slike na osnovu trenutnih pozicija i izračunati distanca od njene potencijalne pozicije. Generisani skup tačaka u prostoru je redak, ali sa preciznim dubinama. U sledećoj fazi se izračunavaju dubine većeg broja tačaka, na osnovu koga se može rekonstruisati model.

Određivanje dubine tačaka

Za rekonstrukciju modela potreban je znatno veći skup tačaka u odnosu na skup generisan nakon faze pozicioniranja kamera. U ovoj fazi su poznate pozicije kamera, koje ostaju fiksirane.Za određivanje dubine svake tačke, potrebne su dve kamere. Jedna služi kao kamera za čije tačke se traži dubina, a uz pomoć druge se određuje dubina pojedinačnih tačaka. Najpre je potrebno odrediti skup parova kamera. Za svaku kameru se pronalazi najbolji par iz skupa dobijenog nakon faze pozicioniranja. Ovaj skup parova se može odrediti na osnovu pozicija kamera, ili broja ključnih tačaka koje vide obe kamere. Nakon toga, za svaki par je potrebno odrediti što veći broj tačaka za koje se može pretpostaviti određena vrednost dubine sa dovoljno velikom verovatnoćom.

Postoji više načina za određivanje dubine tačaka sa prve slike. Većina se zasniva na pretpostavci minimalne i maksimalne dubine koju prva slika vidi. Ovaj podatak se izvlači iz skupa tačaka koje su rekonstruisane u prvoj fazi. Za svaku tačku sa prve slike pronalazi se reprojekcija na drugoj slici iz para za odgovarajuću minimalnu i maksimalnu dubinu. Time se na drugoj slici formira duž. Sve tačke na toj duži predstavljaju potencijalni par odgovarajućoj tački sa prve slike. Definisanje funkcije koja određuje sličnost piksela je od izuzetne važnosti i predstavlja ključni deo pronalaženja dubine.

Implementacija određivanja dubine tačaka u prostoru je izvršena na grafičkoj kartici, jer je za veliki broj tačaka potrebno uraditi iste kalkulacije. Zbog mogućnosti paralelizacije na grafičkoj kartici, algoritam je ubrzan do nekoliko desetina puta.

Rekonstrukcija modela

Rekonstrukcija modela predstavlja problem dobijanja 3D modela na osnovu određenog skupa tačaka koji ga opisuju. Ukoliko je skup tačaka precizan i dovoljno gust, radi se o tačnoj rekonstrukciji. Međutim, u praksi je često skup tačaka nepotpun ili neravnomerno raspoređen, zbog čega se model aproksimira na osnovu postojećeg skupa tačaka.

Početni skup tačaka može biti redak ili gust. Jasno je da je sama aproksimacija modela preciznija za veći skup tačaka. Takođe, u praksi tačke mogu biti neravnomerno raspoređene. Tako na određenim mestima ima dovoljno tačaka na osnovu kojih se može uverljivo izvršiti rekonstrukcija, dok u drugim delovima tačke mogu nedostajati. Na taj način se mogu stvorati manje ili veće rupe, pa je samim tim zbog nedostatka informacija i aproksimacija modela znatno teža. Rupa se u skupu tačaka može pojaviti i u slučaju kada se određeni deo 3D modela nije nalazio ni na jednoj slici iz početnog skupa. U praktičnim situacijama položaj tačaka ne može uvek biti precizno izmeren, zbog čega dolazi do pojave šuma. Metod koji uspešno vrši proces rekonstrukcije mora biti robustan na pojavu šuma, u smislu da takve tačke prilikom rekonstrukcije modela ingoriše. Najzad, česta je i pojava izdvojenih tačaka, koje se nalaze daleko od većine drugih tačaka. Za ove tačke se pretpostavlja da ne pripadaju modelu, tako da se one obično ignorišu.Druga opcija je da se nakon generisanja modela delovi koji sadrže takve tačke jednostavno eliminišu.

Metode koje vrše rekonstrukciju uzimaju u obzir način na koji je skup početnih tačaka predstavljen. Obično, bez dodatnih pretpostavki o tačkama, problem nije dobro određen, budući da se dosta modela

može generisati na osnovu takvog skupa tačaka. Najčešće je uz svaku tačku jedinstveno definisana njena normala, prava koja je normalna na tangentni prostor. Tagnentni prostor predstavlja lokalizovanu aproksimaciju modela u datoj tački.Normale koje ne poseduju informaciju o smeru se nazivaju neorijentisane. Takve vrste normala se često mogu dobiti i na osnovu samog skupa tačaka. Sa druge strane, orijentisane normale nose informaciju o smeru pružanja, što je u najvećem broju slučajeva ka unutrašnjosti ili ka spoljašnjosti modela. Najzad, pored skupa tačaka, nekad su poznate informacije o položaju kamera sa svojim tačnim koordinatama ili koordinatama dobijenih u prvoj fazi automatske 3D rekonstrukcije. U ovom radu su za generisanje modela iskorišćene 3D pozicije kamera određene u prvoj fazi.

U ovom softveru je korišćena metoda za rekonstrukciju modela koja predstavlja kombinaciju primene Delunijeve triangulacije i sečenja grafa. Korišćena metoda podrazumeva da su poznate informacije o položaju kamera. Delunijeva triangulacija skupa trodimenzionalnih tačaka predstavlja konveksnu konturu koja je podeljena na tetraedre, tako da nijedan tetraedar ne sadrži nijednu dodatnu tačku sem svoja četiri temena. Čitava kontura se sastoji od skupa trouglova koji predstavljaju stranice tetraedara, a konačni model će biti podskup tog skupa trouglova. Metoda sečenja grafa nosi istovetan naziv kao i poznata metoda u teoriji grafova, budući da se na njoj bazira. Ovde tetraedri predstavljaju čvorove, a trouglovi ivice između dva tetraedra.Graf je usmeren, budući da su svi trouglovi u triangulaciji usmereni. Kao rezultat algoritma, potrebno je odrediti koji od tetraedara predstavlja vidljiv prostor, a koji prostor koji se ne vidi nijednom kamerom. Ivicima grafa se dodeljuju početne vrednosti parametara koje označavaju meru vidljivosti, glatkosti, površine, i sl. U tom smislu se najčešće nalaze preseci tetraedara sa zracima koji spajaju položaje kamera i tačaka iz skupa. Za takve tetraedre se očekuje da će u rezultujućem modelu biti vidljivi. Na tako kontruisani graf se primenjuje metod maksimalnog protoka, na osnovu koje se odrede vidljivi i zaklonjeni tetraedri. Konačan model predstavlja skup trouglova (tzv. interfejsa) koji se nalaze između dva tetraedra, od kojih je jedan vidljiv, a drugi zaklonjen

Teksturisanje

Teksturisanje predstavlja poslednju fazu automatske rekonstrukcije 3D modela. Ono je veoma značajno za mnoge praktične situacije, gde je pored oblika samog modela bitna i odgovarajuća tekstura. U nekim situacijama teksturisanje nije potrebno izvršiti, jer je samo od značaja oblik 3D modela (na primer, sâm model se može konstruisati za određivanje panorame). Pri teksturisanju se nekad dodele unapred definisane teksture ili se teksture mogu generisati na osnovu slika. Ako se, na primer, radi o teksturisanju modela glave, mogu se automatski prepoznati oblici kao što su nos, usta, oči ili obrve i shodno tome obojiti model. U slučaju triangulisanog modela koji je u ovom radu korišćen, svaki trougao je obojen jedinstvenom teksturom. Jedan od načina dobijanja specifične teksture trougla je projektovanje sa slike na model, pri čemu se najčešće uzima tekstura sa one slike iz koje je taj deo modela najviše vidljiv

Plan razvoja:

1. Implementacija osnovnog algoritma. Testiranje dobijenog rešenja, i upoređivanje rezultata dobijenih različitim algoritmima.

2. Optimizacija rezultata dobijenih u prvim fazama projekta. Implementacija dodatnih algoritama za svaki od koraka i testiranje njihvog učinka na različitim setovima fotografija
3. Optimizacija performansi i preciznosti algoritama. Formira se baza objekata (oblika) koja je od interesa za korisnika, i testira dobijeno rešenje.
4. Kreiranje grafičkog korisničkog interfejsasaadekvatnim skupom komandi.

Planirane primene softvera:

1. Integracija u sistem za video nadzor teško dostupnih ili nedostupnih velikih teritorija (potprojekat 1)
2. Integracija sa bazom podataka o terorizmu i organizovanom kriminalu (potprojekat 3)
3. Generisanje panorama enterijera objekata od interesa na osnovu fotografija

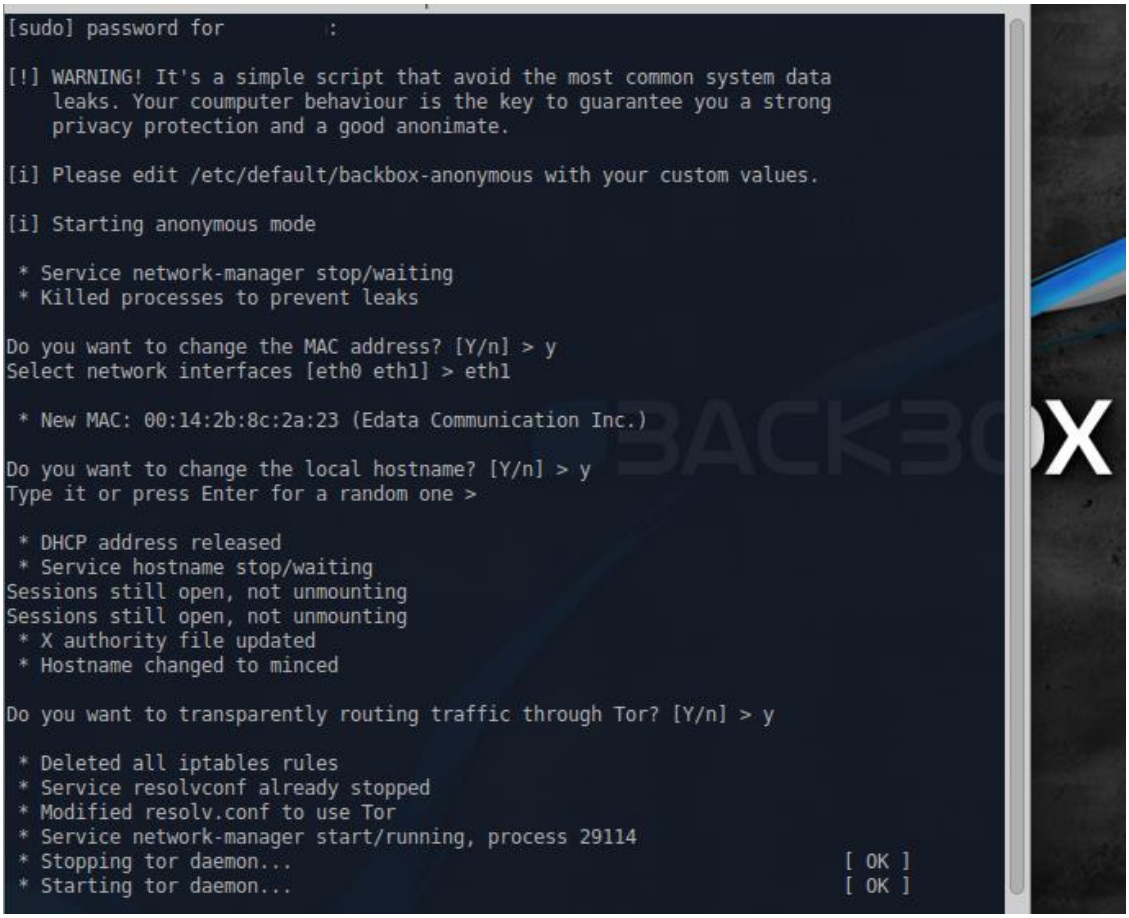
6.Sistem za sigurnu komunikaciju preko USB-a

Predlog projekta sigurne komunikacije preko USB-a je plod višegodišnjeg istraživanja zaštite lične privatnosti i komunikacije preko interneta. Cilj projekta je potpuna zaštita komunikacije korisnika, izmenom njegovog identiteta, sakrivanjem (kriptovanjem) svih njegovih aktivnosti na internetu, kao I onemogućavanje bilo koga da stekne uvid u sadržaj istog. Drugim rečima, korisnik na USB-u ima sve što mu je potrebno za sigurnu komunikaciju, a ukoliko ovaj uređaj padne u pogrešne ruke, ne postoji mogućnost neovlašćenog pristupa.

Naime, radi se o kompletnoj instalaciji Backbox Linux distribucije na USB memoriju unutar LUKS kriptovanog kontejnera. Operativni sistem koji se nalazi na USB-u, može se podići sa skorog svakog desktop ili laptop računara. Iako se u ovo svrhu može koristiti bilo koja Linux distribucija, Backbox se pokazao najboljim izborom jer već poseduje skoro sve neophodne sigurnosne skripte I programe.

Backbox je specijalizovana distribucija za pentesting (penetration testing) ili jednostavno rečeno, za proveru sigurnosti kompjuterskih sistema, tj. hakovanje (Slika 6.1). Sadrži neophodne alatke za sve moguće vrste hakovanja i ima ugrađen Anonymous mode, kao i opciju čišćenja RAM (RAM wiping) memorije prilikom gašenja sistema.Preciznije, ključivanjem Anonymous mode-a, korisnik ima mogućnost promene MAC adrese (fizička adresa mrežne kartice), javne IP adrese i hostname-a, tako da prilikom svakog novog pokretanja ovog moda dolazi do potpune promene identiteta korisnika. Anonymous skripta kompletan internet saobraćaj operativnog sistema preusmerava na popularnu Tor mrežu I tako menja IP adresu korisnika i kriptuje sve njegove aktivnosti na internetu. Isključivanjem Anonymous moda, pored vraćanja podataka u prethodno stanje, dolazi do potpunog brisanja svih podataka iz sistema koji bi mogli da kompromituju korisnika kasnijom analizom.

Slika 6.1. Backbox



Slika 6.2. RAM wiping skripta

RAM wiping skripta (Slika 6.2) u potpunosti čisti RAM memoriju tako da ne postoji mogućnost da se digitalnom forenzikom dođe do bilo kakvih podataka. Backbox (kao I većina Linux distribucija) prilikom instalacije nudi mogućnost potpune enkripcije operativnog sistema što je veoma korisno jer onemogućava neovlašćeni pristup I uvid šta se nalazi na hard disku ili particiji na kojoj je sistem instaliran. U našem slučaju radi se o USB memoriji.Enkripcija je dovoljno jaka da je skoro nemoguće otključati particiju i podići operativni sistem bez šifre.

U slučaju opasnosti, dovoljno je nekoliko sekundi da se USB izvuče iz kompjutera, negde sakrije ili izbaci kroz prozor. Instalacija na USB, korisniku omogućava da promeni fizičku lokaciju I podigne svoj operativni sistem sa bilo kog kompjutera koji mu je dostupan.