Biometrijska autorizacija korisnika Internet usluga – Online demo

Online demo projekta IT 'Sustav za biometrijsku autorizaciju Internet korisnika temeljen na fuziji značajki lica i otiska dlana' je mrežna aplikacija koja omogućuje ispitivanje biometrijskog sustava za verifikaciju u stvarnim uvjetima.
Sklopovski zahtjevi za pokretanje demonstracijskog programa su

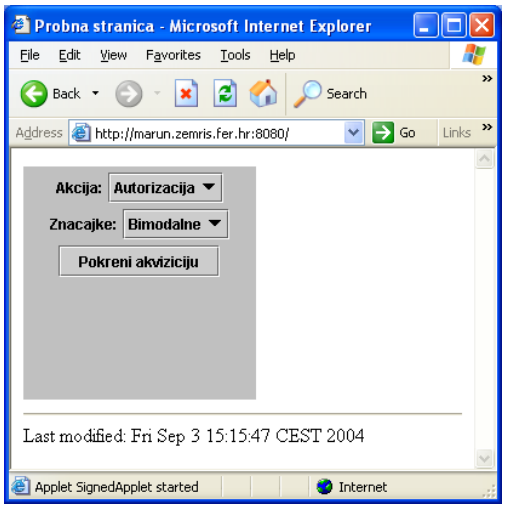
- Internet veza
- Kamera u boji s TWAIN kompatibilnim driverom
- Skener s TWAIN kompatibilnim driverom i podržanom rezolucijom od 180dpi

1. Instalacija

Za pokretanje demonstracijskog programa potrebno je prvo instalirati klijentsku aplikaciju. Instalacija klijentske aplikacije zahtjeva da na računalu bude instaliran .NET framework, a ukoliko nije, automatski će uputiti korisnika na Internet stranice odakle se može uzeti. Potrebno je da se klijentska aplikacija smjesti u direktorij u koji će svi njeni korisnici imati pravo pisanja.
Osim klijentske aplikacije, također je potreban Java Virtual Machine, koji se može instalirati s
http://java.com/en/download/windows_automatic.jsp

2. Pokretanje

Postupak autorizacije ili prijave pokreće se iz Web preglednika, tako da se unese adresa našega servera
http://balbo.zemris.fer.hr:8080
Prilikom otvaranja ove adrese pojaviti će se prozor u kojemu će se od korisnika tražiti dozvola za pokretanje mrežne aplikacije. Na ovom prozoru potrebno je dati dozvolu klikom na 'Yes'.
Nakon toga, otvara se stranica prikazana na slici 1.



Slika 1: Web stranica za pokretanje klijentske aplikacije

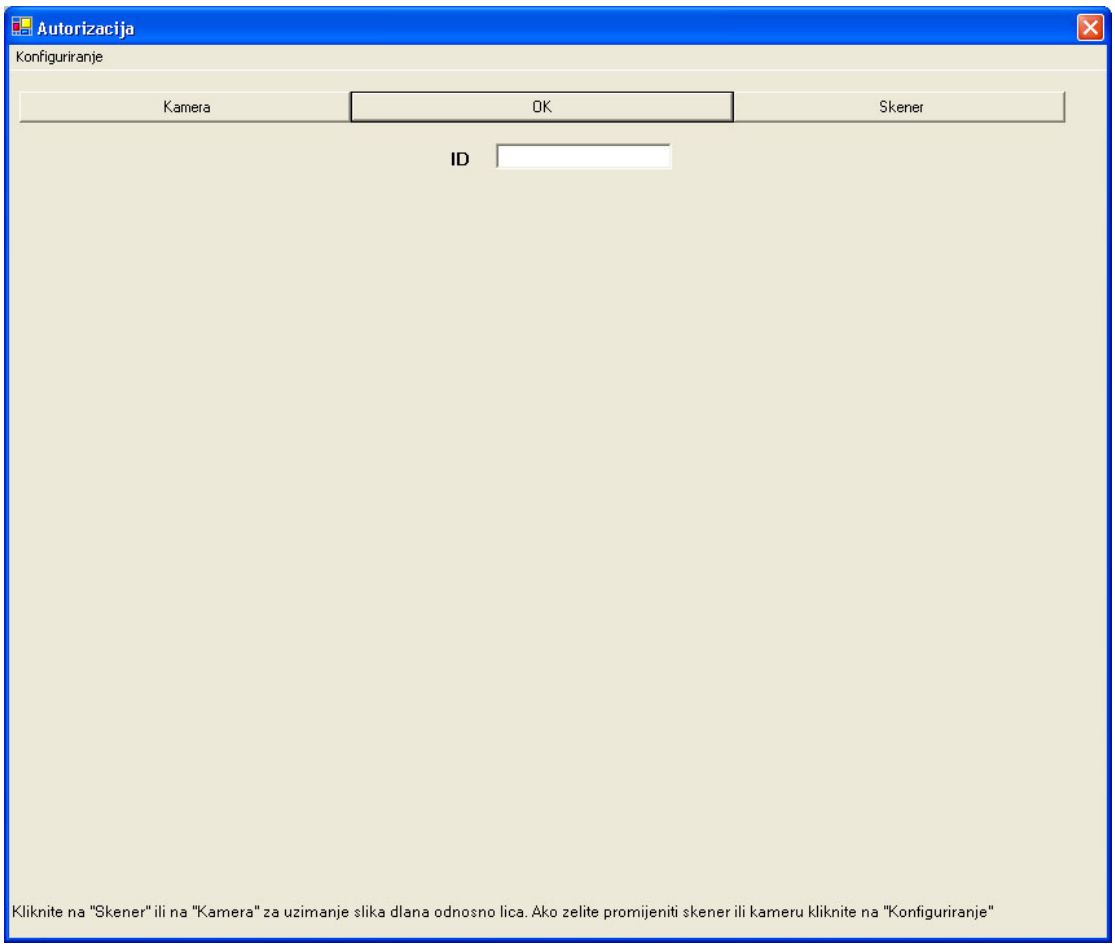
Na ovoj stranici moguće je iz liste 'Akcija' izabrati dvije osnovne akcije:

- **prijava** uključuje uzimanje nekoliko uzoraka (slike dlana, slike lice ili obje) od korisnika, čije će se značajke zatim sigurnim putem prenijeti na server i trajno pohraniti u bazu značajki registriranih korisnika. Korisnik će pri tome također odabrati ID s kojim će se kod autorizacije, odnosno verifikacije, predstavljati sustavu. Ukoliko se korisnik želi pokušati (uspješno) autorizirati kao registrirani korisnik prvo se treba registrirati ovim putem.
- **Autorizacija**, odnosno verifikacija, uključuje uzimanje jednog uzorka od korisnika, čije će se značajke zajedno s njegovim ID-om tada sigurnim putem prenijeti na server i usporediti sa značajkama u bazi registriranih korisnika. Dio sustava, smješten na serveru, utvrđuje radi li se o značajkama iste osobe i svoj odgovor sigurnim putem šalje klijentu.

Obje akcije moguće je izvesti koristeći značajke uzoraka i to:

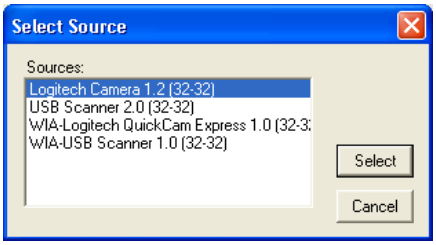
a) samo lica
b) samo dlana
c) i lica i dlana (bimodalne značajke)

Gornje se značajke mogu odabrati iz liste 'Znacajke' na početnoj Web stranici demonstracijskog programa.
Nakon odabira akcije i značajki, te klika na dugme 'Pokreni akviziciju' pokreće se, na klijentskom računalu, jedna od aplikacija za akviziciju slike (opcije a), b) ili c)), ovisno o odabranoj akciji i značajkama. Svrha ove aplikacije unos je slike lica kamerom, slike dlana skenerom, te ID-a korisnika koji želi autorizaciju ili prijavu. Primjer prozora aplikacije za akviziciju slike dlana i lica (ako je korisnik izabrao bimodalne značajke) nalazi se na slici 2.



Slika 2: Primjer sučelja za akviziciju slike

Prilikom prvoga pokretanja svake od aplikacija za akviziciju, pojaviti će se prozor u kojemu će korisnik, između ponuđene sklopovske opreme, odabrati kameru i/ili skener (Slika 3). U svakoj se od aplikacija za akviziciju pri dnu glavnoga prozora nalazi tekst koji upućuje korisnika na ono što je potrebno napraviti sljedeće. Detaljan opis aplikacija za akviziciju može se naći u seminarskome radu Želimira Končara, dostupnome preko web sitea projekta.



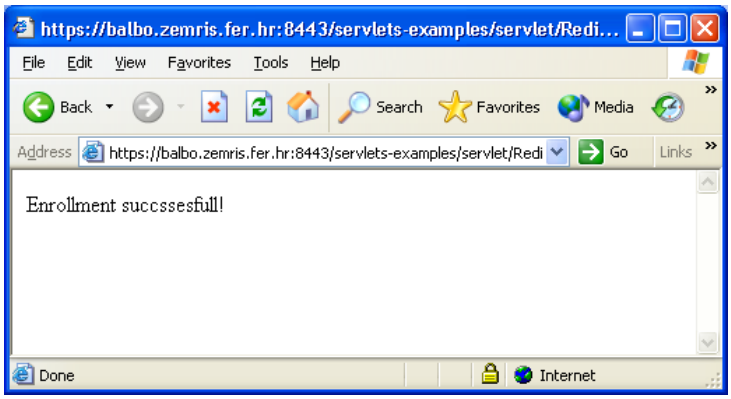
Slika 3: Prozor za odabir kamere ili skenera

Pri akviziciji slika potrebno je voditi računa o slijedećem:

- Pri akviziciji slike lica potrebno je da lice bude okrenuto prema kameri. Također je potrebno gledati u kameru u trenutku akvizicije. Cijelo lice treba biti vidljivo na slici, a poželjno je da lice na slici bude što veće.
- Pri akviziciji slike dlana, važno je da skener bude postavljen tako da je redoslijed skeniranja od vrha prstiju prema zapešću, tako da na skeniranoj slici vrhovi prstiju pokazuju budu okrenuti prema gore. Dlan desne ruke potrebno

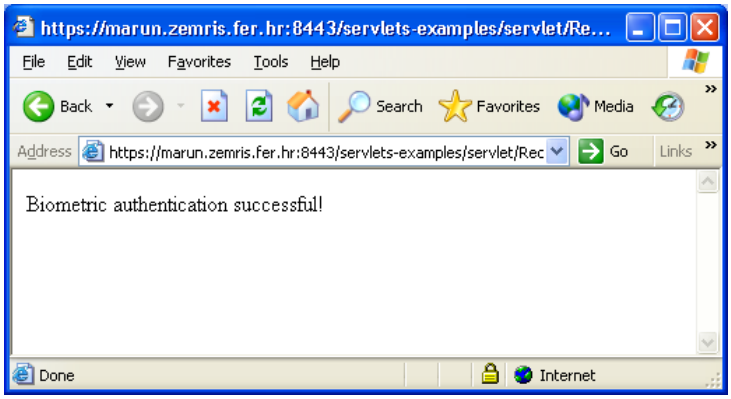
je lagano prisloniti na površinu skenera uz prirodno raširene prste. Za vrijeme skeniranja ruku je potrebno držati mirno.

Nakon završetka aplikacija za akviziciju, potrebno je **pričekati** dok se iz uzetih slika ne izluče biometrijske značajke, te sigurnim putem prebace na server gdje će se dogoditi odgovarajuća akcija. Ovaj postupak nešto duže traje za prijavu nego za autorizaciju, jer se kod prijave radi sa više uzoraka, dok se kod autorizacije radi samo s jednim. Na kraju postupka prijave, korisnik u Web pregledniku dobiva odgovor o uspješnoj prijavi, prikazan na slici 4.



Slika 4: Odgovor servera u slučaju prijave

Ukoliko se radi o postupku autorizacije, korisnik dobiva poruku o njenoj uspješnosti. Na slici 5 prikazan je odgovor servera u slučaju uspješne autorizacije.



Slika 5: Primjer odgovora sa servera (slučaj uspješne autorizacije)

Pomoću online aplikacije moguće je izvršiti dva osnovna eksperimenta, pri kojima korisnik igra ulogu klijenta ili uljeza.

- **klijent** je osoba prijavljena na sustav, čije značajke su spremljene u bazi registriranih korisnika na serveru. Da bi se proveo ovakav eksperiment, potrebno je prvo proći postupak prijave. Pri svakom pokušaju autorizacije klijent unosi (pomoću kamere i/ili skenera) biometrijske značajke u sustav uz svoj ID, dakle onaj isti koji je unio pri postupku prijave. U ovom slučaju autorizacija bi trebala biti uspješna.
- **uljez** je osoba koja nije registrirana na serveru kao korisnik, a pokušava se autorizirati pomoću nekog od ID-a registriranih korisnika, ili je registrirana, ali pokušava se autorizirati preko ID-a nekog drugog korisnika. Rezultat autorizacije u ovome slučaju trebao bi biti neuspješan. Da bi se omogućio ovakav eksperiment, u bazi registriranih korisnika već su unešene značajke

nekoliko osoba. Njihovi ID-jevi su 'ifratric', 'ssegvic', 'jkrapac', 'jsnajder', 'zkalafatic', 'thrkac', 'bdalbelo'.

PRIMJERI:

1. Slučaj: Osoba nije prijavljena, odnosno registrirana kao korisnik i njezine se značajke ne nalaze u bazi podataka na serveru. Osoba (uljez) unosi svoje biometrijske značajke (pomoću kamere i/ili skenera) i koristi 'ukradeni' ID, npr 'ifratric'.
   Očekivani rezultat: Odovor servera 'Biometric authentication failed'.
2. Slučaj: Osoba prolazi postupak registracije. Biometrijske značajke s odgovarajućim ID-jem se šalju serveru i pohranjuju u bazi podataka. Nakon toga, osoba se pokušava autorizirati. Osoba ponovno unosi svoje biometrijske značajke (skenerom i/ili kamerom) i koristi svoj ID (odabran u postupku registracije).
   Očekivani rezultat: Odovor servera 'Biometric authentication successful'.