Konferencija o bezbednosti informacija BISEC 2015
Fakultet informacionih tehnologija

BIOMETRIJA I FORENZIKA U DIGITALNOM DOBU

BIOMETRICS AND FORENSICS IN DIGITAL AGE

ANDREJA SAMČOVIĆ
Saobraćajni fakultet, Beograd, andrej@sf.bg.ac.rs

Rezime: *U ovom radu je najpre uvedena biometrija i naznačeno je njeno istorijsko poreklo u forenzičkoj i pravnoj oblasti. Zatim su diskutovane sličnosti i razlike između biometrije i forenzike. Predstavljene su neke primene gde se principi biometrije uspešno primenjuju u forenzici kako bi se rešili kritični problemi u domenu prava. Posebno su istaknuti prepoznavanje lica na osnovu skice, tetovaža, kao i video nadzor. Na kraju su razmotrene neke mogućnosti za istraživače na polju biometrije i forenzike kako bi mogli da sarađuju na nerešenim pitanjima od kojih bi moglo da ima koristi društvo u celini.*

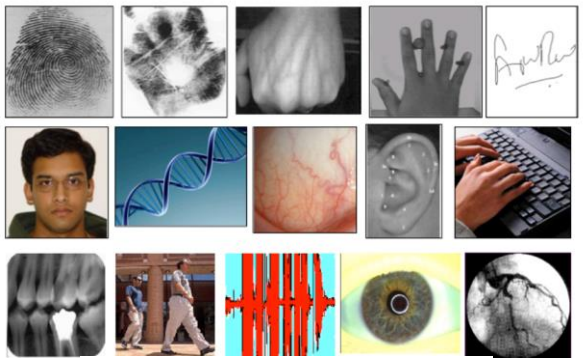
Ključne reči: *Digitalna forenzika, biometrija, slika, otisak prsta, autentifikacija*

Abstract: *In this paper, we first introduced biometrics and noted its historical origins in the forensics and law enforcement domain. Next, we discussed the similarities and differences between biometrics and forensics. Some applications where the principles of biometrics are being successfully leveraged into forensics in order to solve critical problems in the law enforcement domain, are then presented. Face recognition based on sketch, tattoo, as well as video surveillance, are pointed out. Finally, we discussed new opportunities for researchers in biometrics and forensics to cooperate, in order to address unsolved problems that can benefit society as a whole.*

Keywords: *Digital forensics, biometrics, image, fingerprint, authentication*

1. UVOD

Biometrija, ili biometrijsko prepoznavanje, se odnosi na automatsko prepoznavanje pojedinaca i zasnovana je na biološkim karakteristikama ili ponašanju. [1] Primeri biometrijskih osobina koje se uspešno koriste u praktičnim aplikacijama uključuju lice, otiske prstiju, dlan, iris, govor, kao i raspored vena na dlanu ili prstima, što je pokazano na Slici 1. Postoji jaka veza između neke osobe i njenih biometrijskih osobina, imajući u vidu nepromenljivost biometrije kroz životno doba. Tipični biometrijski sistem može da se sagleda kao sistem za automatsko prepoznavanje oblika u realnom vremenu, koji zahteva biološke podatke od neke osobe (npr. otisak prsta), koristeći senzore. Zatim se izdvaja niz oblika iz tih podataka (npr. minucije), i obavlja se poređenje dobijenog niza sa onima iz baze podataka kako bi se prepoznala osoba. Pretpostavlja se da je svaki niz oblika u bazi podataka (šablon) povezan sa nekom osobom preko identifikacije, koja može da bude ime, ili ID broj. Poređenje izdvojenog niza oblika i rezultata iz šablona ukazuje na sličnost između dva niza oblika. Procena sličnosti nizova oblika može zatim da se koristi kako bi se prepoznala neka osoba.



Slika 1: Primeri biometrijskih osobina

U savremenom društvu, mogućnost da se pouzdano identifikuju pojedinci u realnom vremenu predstavlja osnovni zahtev u mnogim primenama, uključujući prelazak međunarodnih granica, transakcije preko automata za podizanje novca, elektronsko poslovanje, kao i logovanje na računarima. Budući da postoji povećana mobilnost ljudi u visoko umreženom svetu, proces pouzdane identifikacije postaje sve izazovniji i kritičniji. Korektna identifikacija ima reperkusije u odbrani društva od terorističkih napada, kao i krađi identiteta prilikom pristupa bankovnim računima, ili drugim ličnim informacijama. Može se reći da dva najznačajnija faktora koji ukazuju na neophodnost biometrije jesu bezbednost društva i finansijske zloupotrebe.

U poslednje dve decenije je zabeleženo ubrzano uvođenje biometrijskih sistema u raznim oblastima. Bez sumnje, biometrijska tehnologija je formirala značajan upliv u naše društvo. Na primer, biometrija nastavlja da igra kritičnu ulogu u pravnom sistemu, i to kako u procesu istrage da bi se suzila lista osumnjičenih osoba, tako i u izvođenju forenzičkih dokaza na sudu. Biometrijsko prepozavanje je takođe postalo integralni deo sistema za upravljanje identitetom širom sveta, posebno u zemljama u razvoju gde veliki broj ljudi i ne poseduje formalne dokumente za identifikaciju kako bi se proverio njihov identitet.

U Indiji je u toku najveći projekat uvođenja biometrije u istoriji čovečanstva. Naime, indijske vlasti ulažu napore u obezbeđivanju jedinstvenog identifikacionog broja od 12 bita za oko 1,2 milijardu stanovnika. U okviru ovog projekta koriste se otisci deset prstiju, kao i irisi oba oka, kako ne bi došlo do dupliranja identiteta. Očekuje se da će program za biometrijsku identifikaciju poslužiti u efikasnijoj zdravstvenoj zaštiti, izbegavanju prevara u ostvarivanju socijalnih prava, kao i bezbednijim finansijskim transakcijama.

Biometrijski sistemi su takođe promenili način kako putujemo, imajući u vidu poboljšanu bezbednost, efikasnost i pouzdanost sistema za prelazak granica. U Sjedinjenim Državama, sistemi za biometrijsku autentifikaciju su implementirani na graničnim kontrolama, kao i transportnim sistemima, nakon terorisatičkih napada 11. septembra 2001. U potrošačkoj elektronici, svaki veći proizvođač mobilnih uređaja je već uključio ili je u procesu uvođenja autentifikacije korisnika na osnovu biometrije, imajući u vidu bezbednost mobilnih uređaja i mobilno plaćanje.

Prvo poznato istraživanje na temu automatskog biometrijskog prepoznavanja je objavljeno 1963. na temu prepoznavanja otisaka prstiju. [2] Sistemi za automatsku biometriju su uvođeni 60-ih godina XX veka i zasnivaju se na ljudskim karakteristikama kao što su govor [3], lice [4], i potpis [5]. Nakon toga su postepeno razvijani i biometrijski sistemi koji se baziraju na obliku ruke [6] i irisa [7]. Nije iznenađujuće da se razvoj biometrijskih sistema odvija uporedo sa razvojem u bliskim oblastima, kao što su veštačka inteligencija, prepoznavanje oblika, kao i obrada slike, koje su pomogle u analizi i prepoznavanju biometrijskih oblika.

Događaj koji je uticao na sistematsko korišćenje biometrijskih osobina u prepoznavanju pojedinaca dogodio se 1869. u Velikoj Britaniji. Tada je uvedena obaveza da se registruju sve osobe osumnjičene za kriminal sa odgovarajućim dokazima njihovog identiteta. U međuvremenu je uveden sistem za prepoznavanje na osnovu antropometrijskih merenja. Sistem je koristio i opise ljudskih osobina kao što su boja očiju, ili ožiljci, što se danas u literaturi označava kao soft biometrija. Međutim, taj sistem nije bio automatski, bila je komplikovana administracija, i nije uzimao u obzir promene tokom životnog veka. Imajući sve to u vidu, sistem je brzo napušten u korist relativno jednostavnijeg i pouzdanijeg pristupa, koji je uzimao u obzir ručno poređenje otisaka prstiju.

1891. godine su argentinske policijske vlasti inicirale uzimanje otisaka prstiju kao dokaz u ubistvima ljudi. Veruje se da je to prvo korišćenje otisaka prstiju u kriminalnim radnjama u istoriji. Počev od 1900, u Velikoj Britaniji se koriste otisci prstiju u pravnim postupcima. Otisci prstiju su prvi put prihvaćeni kao dokaz 1905. u britanskoj pravnoj praksi. 1924. godine je Kongres Sjedinjenih Država naložio prikupljanje otisaka prstiju, zajedno sa drugim informacijama o osumnjičenim osobama za kriminal. Ta činjenica je utabala staze za uvođenje sistema za automatsku identifikaciju otisaka prstiju, u kasnim 1970-im godinama. Iako se ovaj sistem smatra za automatski, mora biti napomenuto da automatizam nije bio potpun u prvim godinama primene sistema. Prisustvo eksperata je bilo neophodno za obradu otisaka prstiju, kao i identifikaciju tačaka na minucijama, koje su kasnije određivane automatski za pristup listi kandidata u okviru baze podataka. Odluka o konačnom poklapanju morala je da bude doneta od strane eksperata. Treba reći da je i u brojnim savremenim inteligentnim aplikacijama proces poređenja još uvek polu-automatski.

Prethodna diskusija ukazuje na to da poreklo biometrijskog prepoznavanja ima korene u pravnom sistemu i domenu forenzičke nauke, gde je prepoznavanje bilo usmereno na izvršitelje kriminalnih radnji. Međutim, biometrija se u savremenom društvu sve više koristi u sistemima za upravljanje identitetom, gde je glavni cilj da se omogući pojedincima pristup određenim resursima, npr. mobilnim telefonima, ili ostvarivanje nekih privilegija, kao što je ulazak u neku zemlju. Primeri biometrijske autentifikacije su prikazani na Slici 2.

Slika 2: Primeri za biometrijske aplikacije

Posle uvodnog razmatranja, u ovom radu razmotrene su veze koje postoje između biometrije i forenzike. Zatim su navedene i analizirane mogućnosti primene biometrijskih metoda u forenzičkoj naučnoj disciplini. Opisani su postupci analize otisaka prstiju, slike tetovaže na ljudskim telima, kao i analiza snimaka dobijenih video nadzorom. Na kraju rada su data zaključna razmatranja.

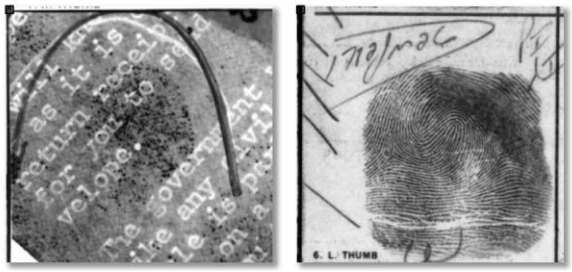
2. SLIČNOSTI I RAZLIKE IZMEĐU BIOMETRIJE I FORENZIKE

Forenzička nauka obuhvata naučne principe pri analizi dokaza neke kriminalne radnje kako bi se rekonstruisali i opisali događaji koji su tome prethodili, poštujući pri tome pravne procedure. Postoje brojni izvori dokaza koji se koriste u forenzičkim istraživanjima, uključujući otiske prstiju, tragove guma, obuće, ili rukopis. [8] Govor i lice se takođe koriste kao dokazni materijal. Jedan od glavnih zadataka forenzičkog istraživanja je povezivanje dokaza, kao što je otisak prstiju, sa izvorom dokaza tj. određenim pojedincem.

Razmotrimo otisak prsta, pokazan na Slici 3, koji je nađen na mestu neke kriminalne radnje. U kontekstu forenzičkog istraživanja, ukoliko je otkriveno da se taj otisak odnosi na kriminalnu aktivnost, sledeće pitanje koje se može postaviti je: koji je izvor tog dokaza, tj. ko ili šta je generisalo taj otisak? U tradicionalnoj forenzičkoj evaluaciji postojala su tri moguća odgovora zasnovana na razmatranju dokaza:

- individualizacija – ne postoji nijedna druga osoba koja bi mogla biti izvor otiska;
- nije moguće pouzdano zaključiti da li može ili ne može da se otisak pridruži nekoj poznatoj osobi;
- ekskluzivnost – otisak definitivno ne može da se pridruži nekoj poznatoj osobi.

Savremeni forenzički postupci, međutim, fokusiraju se na jačini dokaza pod uslovima da ili otisak koji se istražuje potiče od osobe koja je osumnjičena u slučaju, ili da potiče od neke druge osobe. [9]



Slika 3: Otisak prsta sa leve strane je dokaz uzet sa mesta neke kriminalne radnje; otisak sa desne strane potiče od poznatog izvora.

Imajući sve to u vidu, može se zaključiti da forenzika i biometrija zahtevaju povezivanje sa biološkim podacima određene osobe. Međutim, postoje i brojne razlike između ove dve naučne discipline.

Forenzika igra ulogu nakon što se desio neki događaj i uobičajeno se koristi kako bi se rekonstruisali kriminalni događaji koji su se desili u prošlosti putem hipotetičko-deduktivnog pristupa. Biometrijsko prepoznavanje se, sa druge strane, koristi tipično pre nego što se neki događaj desio, npr. provera biometrijskih osobina prilikom ulaza u neku zemlju.

U forenzičkoj istrazi nije moguće odrediti unapred tip dokaza koji će biti korišćen prilikom istraživanja osumnjičenih. Kriminalna radnja treba da bude pažljivo istražena kako bi se prikupili dokazi koji bi se koristili u svrhu prepoznavanja. Ta činjenica predstavlja kontrast u odnosu na biometrijske sisteme, gde su biološke karakteristike koje se koriste za prepoznavanje neke osobe poznate unapred.

Forenzika prevashodno uključuje ručno prikupljanje i proučavanje dokaza u poređenju sa biometrijskim prepoznavanjem, koje je po definiciji potpuno automatizovano. U stvari, sistemi za kvalitativnu procenu se veoma koriste u forenzičkom kontekstu kako bi se uspostavila sličnost između dokaza i određenog izvora.

Odlučivanje o prepoznavanju kod biometrijskih sistema treba da se donese u realnom vremenu, i zbog toga je računarska efikasnost važan faktor u biometrijskim primenama. U forenzici, međutim, ne zahteva se prepoznavanje u realnom vremenu.

Slučaj pogrešnog nepoklapanja u forenzici se smatra neželjenim, jer može da rezultira u isključivanju osumnjičenog za kriminal od dalje obrade. U slučaju biometrije, zavisno od primene, posledice pogrešnog poklapanja ili nepoklapanja mogu da budu različite. Na primer, kod video nadzora pogrešno nepoklapanje mora da bude minimizirano zbog povećanog rizika od pogrešnog poklapanja. Međutim, kod sistema za biometrijski pristup nekim osetljivim podacima, pogrešno poklapanje mora da se minimizira, čak i ako bi imalo za posledicu povećan broj pogrešnih nepoklapanja.

Za razliku od forenzike, biometrijski sistemi mogu da zahtevaju dodatne uzorke biometrijskih osobina, ili dodatne osobine od neke osobe kako bi se ispravno donela odluka o poklapanju ili nepoklapanju.

Kvalitet podataka o dokazima dobijenih u slučaju forenzike je uobičajeno niži nego u slučaju biometrije. Tragovi dokaza koji se koriste u forenzičkoj istrazi treba da se izdvoje od kriminalne scene gde, za razliku od biometrije, neka osoba ne ostavlja smišljeno svoje biološke dokaze. To je, ujedno, i jedan od razloga zašto potpuno automatski sistem ne može uvek da se uspostavi u forenzičkim slučajevima.

Izlaz procesa forenzičke istrage obično treba da bude obrazložen na sudu. Prema tome, verbalno objašnjenje je od vitalnog značaja kod forenzike. Na primer, kada se objašnjava stepen sličnosti nekog otiska prsta, sudski veštak mora verbalno da opravda kako je koristio kvalitativnu i kvantitativnu metriku. Izlaz biometrijskog prepoznavanja, sa druge strane, je numerički rezultat koji se koristi od strane automatskog sistema. Sistem se izjašnjava o poklapanju, tako da nije neophodno verbalno rezonovanje u automatskim sistemima za upravljanje identitetom.

U prethodnim godinama istraživanja biometrijske i forenzičke zajednice su tekla nezavisno jedna od drugih. Međutim, od skoro je došlo do povećanog interesovanja

za automatske pristupe koji su razvijeni u biometriji kako bi se rešili problemi uočeni od strane forenzičara. [10]

3. BIOMETRIJA U FORENZIČKIM PRIMENAMA

Prepoznavanje lica na osnovu skice

Postoji nekoliko primera kada se biometrija može uspešno primenjivati u forenzičkim istraživanjima. Jedan takav primer se odnosi na skice lica u okviru pravnog sistema, kako bi se pomoglo u identifikaciji osumnjičenih za kriminalno delo, gde nije moguće doći do slike lica tog osumnjičenog, npr. kada nema kamera za video nadzor. Kada se napravi kompozicija lica osumnjičenog, odgovarajući autoriteti proslede skice nadležnima u okviru pravnog sistema, kao i medijima, sa nadom da će neko da prepozna tu osobu i obezbedi valjane informacije koje bi dovele do hapšenja. Primeri kompozicija nekih lica su prikazani na Slici 4. Kompozicije lica su posebno značajne kada su opisi svedoka jedina forma dostupnih dokaza. [11] Nažalost, ovaj postupak nije efikasan i ne upotrebljava sve raspoložive resurse, pogotove ne baze podataka u okviru policijskih službi. Uspešne tehnike za automatsko poklapanje kompozicija lica bi ubrzale nalaženje osumnjičenih za kriminalno delo.

Slika 4: Primeri kompozicija lica od strane forenzičkih umetnika korišćenih u slučajevima kada su osumnjičeni uhvaćeni na osnovu dojava

Kompozicije (skice) lica koje se koriste u pravnim postupcima mogu da se podele u tri kategorije:

- rukom crtane skice lica – kompozicije lica nacrtane od strane forenzičkih umetnika, na osnovu opisa od strane svedoka, koriste se dugo u kriminalnim istragama;
- softverski generisane kompozicije – kompozicije lica formirane od strane softvera koji omogućava operateru da odabere razne komponente lica, kao što su oči ili nos, iz odgovarajućeg menija. Softverski generisane kompozicije su postale popularne kao alternativa rukom crtanim skicama; [12]
- kompozicije iz video nadzora – skice lica nacrtane od strane forenzičkih umetnika na osnovu snimaka iz video nadzora koji su lošeg kvaliteta. Koriste se u slučajevima kada komercijalni sistemi za prepoznavanje lica ne daju rezultate, zbog lošeg osvetljenja ili položaja lica.

Nezavisno od toga koji metod se koristi, kvalitet kompozicije uglavnom zavisi od pouzdanosti opisa od strane svedoka, kao i veštine umetnika ili operatera. Može se reći da bi poboljšanje prepoznavanja forenzičke skice značajno poboljšalo javnu bezbednost. Pod široki kišobran biometrijskog prepoznavanja bi mogla da se podvede identifikacija osumnjičenih koristeći forenzičke skice. Skica može da se konvertuje u digitalnu sliku i zatim da se obavi automatsko poklapanje sa drugim slikama lica iz baze podataka, na primer sa fotografijama iz vozačkih dozvola. Automatski postupak, omogućen razvojem računarske vizije i algoritama za mašinsko učenje, može da pruži značajne resurse autoritetima odgovornim za pouzdano i brzo hapšenje opasnih kriminalaca.

Tetovaža

Drugi primer za primenu biometrije u forenzičkoj praksi jeste ispitivanje tetovaža na telu. Tetovaže naslikane na ljudskom telu mogu uspešno da se upotrebljavaju pri asistenciji za identifikaciju u forenzičkim primenama, što je ilustrovano na Slici 5. Tetovaže mogu da sadrže i skrivena značenja koja se odnose na kriminalnu predistoriju osumnjičenog, kao što je pripadanje određenoj bandi, prethodni događaji iz života, godine provedene u zatvoru, i drugo.

Slika 5: Slike tetovaže na telima osumnjičenih

Postoji, takođe, i povećana učestalost tetovaže u populaciji u celini. Pigmenti tetovaže utiskuju se u kožu na takvu dubinu, da čak i ozbiljne opekotine na koži ne mogu da unište tetovažu. Iz ovog razloga, recimo, tetovaže su korišćene pri identifikaciji žrtava terorističkih napada 11.09.2001. u SAD, kao i žrtava cunamija u Aziji, 2004. godine. Slike tetovaže mogu da se koriste, ako je to moguće, kako za identifikaciju žrtava, tako i osumnjičenih.

Pravne agencije obično rutinski fotografišu razne oblike tetovaže i arhiviraju ih u katalozima, u svrhu identifikacije žrtava i osumnjičenih. Postoji standard koji definiše osam glavnih kategorija tetovaže, kao što su: ljudi, životinje, biljke, zastave, objekti, apstraktni oblici, simboli, i drugo. Pretraživanje slika tetovaže obuhvata poređenje standardnih kategorija tetovaže sa onima iz baza podataka. Međutim, u praksi se pokazalo da standardne kategorije ne mogu da obuhvate semantičke informacije, ili značenje simbola, u slikama tetovaže. Tetovaže često sadrže višestruke simbole i ne mogu da se klasifikuju na odgovarajući način. Slike tetovaže koje pripadaju istoj kategoriji često pokazuju velika odstupanja u sadržaju i pojavi. Postojeće kategorije nisu adekvatne za

opis novih dizajna tetovaže. Osim toga, proces pridruživanja slike tetovaže nekoj kategoriji je subjektivne prirode.

Navedeni nedostaci su doveli do razvoja tehnika obrade slike kako bi se poboljšale performanse prepoznavanja slika tetovaže. Pri tome se kao izazov javlja predstavljanje vizuelnog sadržaja tetovaže u smislu raznih oblika, kao što je tekstura. Ti oblici mogu da se koriste za predstavljanje i poređenje slika tetovaže, bez korišćenja standardnih kategorija tetovaže. Automatski sistemi za poklapanje tetovaže su predstavljeni u biometrijskoj literaturi. [13] Primer takvog sistema koji demonstrira kako biometrija može da se uveze u forenzičke primene tj. u istragu nakon događaja, je pokazan na Slici 6.

Slika 6: Izlaz iz sistema za automatsko pretraživanje slika tetovaže [13]

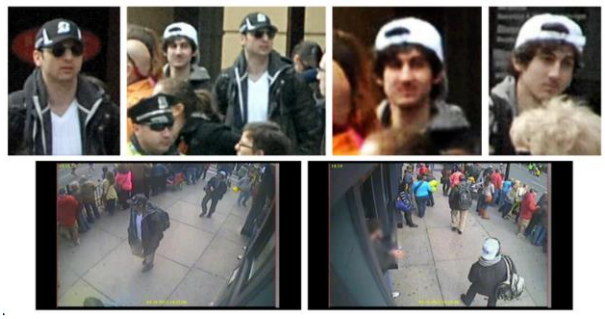
Davanje značaja brzom rešavanju kriminalnih dela, potreba za automatskim postupcima u okviru forenzičke istrage, kao i korišćenje biometrijskih algoritama u pravnom sistemu, bi dovelo do koristi za društvo. Može se reći da zaključci zasnovani na forenzičkim dokazima još uvek nisu dovoljno naučno validni. Naime, smatra se da su sa izuzetkom DNK analize, tvrđenja u okviru forenzike izvedena manje rigorozno nego što se to od njih očekuje. U mnogim slučajevima se smatra da iskustvo forenzičkog veštaka može da posluži kao zamena za naučno strogo zasnovani dokaz. Postoji tendencija ka tome da se u okviru forenzičke zajednice često ponavljane tvrdnje uzimaju kao naučno validne, u nedostatku podataka koji bi potkrepili te tvrdnje. Prema tome, postoji mogućnost za istraživače na polju biometrije da pomognu forenzičkim stručnjacima i statističarima u prikupljanju velikih forenzičkih baza podataka, npr. otisaka prstiju, kao i da analiziraju pouzdanost i validnost forenzičkih procedura primenom automatskih metoda.

Video nadzor

Postoje i neke primene gde je veoma teško prevazići ograničenja vezana za to kako biometrijske osobine mogu da se preuzimaju. Klasični primer za takve primene jeste okruženje video nadzora, gde se koriste snimci sa kamera koje nadziru javne lokacije. Pokazalo se da je stalni video nadzor uspešno sredstvo protiv kriminala, tako da se kamere za nadzor postavljaju širom sveta, naročito u urbanim područjima. Na primer, procenjuje se da trenutno samo na području Londona ima instalirano više od milion kamera, dok na području Velike Britanije ima oko 4,9 kamera za video nadzor. [14] Skoro sve postojeće kamere su pasivne po prirodi, što znači da samo snimaju video zapise sa posmatrane lokacije. Arhivirani video materijal se analizira od strane ljudi jedino ako se dogodi neki kriminal i o tome se izveste odgovarajuće službe. Obrada video signala i prepoznavanje u realnom vremenu se retko kada obavlja kako bi se predvideo ili detektovao neki incident, ili kako bi se obavila identifikacija. Osnovni zadatak automatskog video nadzora u realnom vremenu je kako da se detektuje „osoba od interesa“ u video zapisu, i zatim kako da se identifikuje pomoću sistema za prepoznavanje lica. [9] Sličan problem je re-identifikacija osobe, gde je zadatak praćenje iste osobe kada prolazi kroz mrežu kamera za nadzor. Prepoznavanje lica u video nadzoru je veoma izazovan problem, imajući u vidu sledeća dva razloga:

- relativno loš kvalitet slika lica snimljenih pomoću kamera za video nadzor – faktori koji utiču na degradaciju kvaliteta uključuju lošu prostornu rezoluciju kamere, veliku udaljenost između subjekta i kamere, brzinu kojom se kreće subjekat, promene osvetljenja na posmatranoj lokaciji, kao i zaklanjanje od strane drugih objekata i ljudi u sceni;
- pošto se ne očekuje od subjekta da bude kooperativan, može biti prikrivanja lica, recimo pomoću kape ili naočara za sunce. U nekim slučajevima, može doći do namernog sakrivanja lica od kamere, kako bi se izbegla detekcija.

Uprkos ograničenjima, značajan napredak je postignut u postupcima prepoznavanja lica. Klonc i Džejn [15] su prikazali scenario korišćenja prepoznavanja lica za identifikaciju osumnjičenih u bombaškom napadu na maraton u Bostonu 2013, što je dato na Slici 7. Tri slike od oba osumnjičena brata su upoređena sa slikama iz baze podataka koja je sadržala oko milion različitih slika. Tih šest slika je pridodato bazi podataka, uključujući i slike lica osumnjičenih dobijenih iz društvenih mreža. Slike osumnjičenih izdvojenih iz kamera za nadzor su korišćene kao probne slike pri pretraživanju. Uočeno je da se jedna od slika mlađeg osumnjičenog brata ispravno poklapa sa fotografijom sa završetka srednje škole, koja je uključena u galeriju slika. [15] Međutim, zbog lošije rezolucije i smetnji u vidu kape i sunčanih naočara, stariji osumnjičeni brat nije mogao uspešno da bude identifikovan. To pokazuje da se zahtevaju značajna poboljšanja pouzdanosti u prepoznavanju lica, pre nego što se sistemi za prepoznavanje lica primene u većoj meri u forenzičkim aplikacijama koje bi uključile podatke iz video nadzora.



Slika 7: Slike lica i video zapisi dva osumnjičena brata za bombaški napad na maratonu u Bostonu [15]

4. ZAKLJUČNA RAZMATRANJA

Automatsko prepoznavanje ljudi na dnevnoj osnovi danas čini integralni aspekt našeg društva. Brojne aplikacije, počev od pristupa smart telefonima, preko prelazaka

međunarodnih granica, zavisi od korišćenja mehanizama autentifikacije kako bi se pouzdano identifikovala neka osoba. Tradicionalno, lične karte i pasoši se koriste za potvrdu identiteta. Međutim, dobro poznati nedostaci pristupa koji se zasnivaju na tome šta nosimo sa sobom, ili onome šta znamo, doveli su do korišćenja bioloških karakteristika u automatskom i pouzdanom prepoznavanju.

Uprkos tome što je forenzika jedna od najranijih oblasti biometrijskog prepoznavanja, biometrijski sistemi su pokazali puni potencijal u rešavanju problema sa kojima se suočavaju eksperti na polju forenzike. Biometrijsko prepoznavanje može da se koristi u forenzici na dva načina:

- kao alat za pomoć pri forenzičkoj istrazi;
- za podršku dokazima koji treba da budu predstavljeni na sudu.

Ne treba posebno naglašavati da ova dva slučaja imaju različite zahteve. U prvom slučaju, ključni su brzina i pouzdanost biometrijskog sistema pod izazovnim uslovima. Međutim, niski nivoi grešaka od strane sistema se tolerišu u u ovom scenariju, jer istražitelji mogu da koriste druge informacije tipa pol ili starost, kako bi se eliminisale neke greške.

U drugom slučaju, osnovni zahtev je naučno predstavljanje biometrijskog dokaza sudu, sa jakom statističkom bazom. To, sa jedne strane, uključuje dobijanje pouzdane procene jedinstvenosti biološke karakteristike, a to je problem koji tek treba da bude rešen u kontekstu bioloških tragova. Drugi sličan problem je stalnost pouzdanog biometrijskog prepoznavanja.

LITERATURA

[1] A. K. Jain, A. Ross, K. Nandakumar: „*Introduction to biometrics: a textbook*“, Springer Publishers, 2011.

[2] M. Trauring: „On the automatic comparison of finger ridge patterns“, *Nature*, Vol. 197, pp 938-940, 1963.

[3] S. Pruzansky: „Pattern-matching procedure for automatic talker recognition“, *Journal of the Acoustic Society of America*, Vol. 35, pp 354-358, 1963.

[4] W. W. Bledsoe: „*Man-machine facial recognition*“, Technical report PRI 22, Panoramic Research, Inc, 1966.

[5] A. J. Mauceri: „*Feasibility study of personal identification by signature verification*“, Technical report SID 65-24, North American Aviation, 1965.

[6] R. H. Ernst: „*Hand ID system*“, United States patent number US 3576537

[7] J. G. Daugman: „The importance of being random: statistical principles of iris recognition“, *Pattern Recognition*, Vol. 36, No. 2, pp 279-291, 2003.

[8] F. Taroni, C. Champod, P. Margot: „Foreunners of Bayesianism in early forensic science“, *Jurimetrics*, pp 183-200, 1998.

[9] D. Meuwly, R. Veldhuis: „Forensic biometrics: from two communities to one discipline“, *Proceedings of the International conference of the biometrics special interest group* BIOSIG 2012.

[10] A. Samčović: „Multimedijalna forenzika – deset godina ravoja“, *XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel 2013*, Beograd, str. 407-416, 3-4. decembar 2013.

[11] A. K. Jain, B. Klare, U. Park: „Face matching and retrieval in forensic applications“, *IEEE Multimedia*, Vol. 19, No. 1, pp 20-28, 2012.

[12] D. McQuiston-Surrett, L. Topp, R. Malpass: „Use of facial composite systems in US law enforcement agencies“, *Psychology, Crime and Law*, Vol. 12, No. 5, pp 505-517, 2006.

[13] J-E. Lee, W. Tong, R. Jin, A. K. Jain: „Image retreival in forensics: tattoo image database application“, *IEEE Multimedia*, Vol. 19, No. 1, pp 40-49, 2012.

[14] D. Barrett: „One surveillance camera for every 11 people in Britain“, *The Telegraph*, July 2013.

[15] J. C. Klontz, A. K. Jain: „A case study of automated face recognition: The Boston Marathon bombing suspects“, *IEEE Computer*, November 2013.