Revija za kriminalistiko in kriminologijo / Ljubljana 66 / 2015 / 3, 259–266

Slikovna biometrija v forenziki

Borut Batagelj,[1] Franc Solina[2]

Članek opisuje težave, s katerimi se je predvsem prvi avtor srečal pri svojem delu kot sodni izvedenec za področje biometričnih prepoznav obrazov in interpretacije slik. Preden lahko na sliki iz nadzorne kamere uporabimo sistem za samodejno prepoznavo obrazov, jo moramo z različnimi metodami za obdelavo slik izboljšati in popraviti. Z metodo računalniškega vida iz slik rekonstruiramo 3D informacije. Včasih je treba potrditi tudi pristnost videomateriala, za kar lahko uporabimo različne tehnike na podlagi poznavanja formata zapisa in delovanja algoritmov za obdelavo slike in videa. Če identifikacija na osnovi obraza ni mogoča ali je neuspešna, lahko uporabimo tudi druge biometrične karakteristike osebe – mehke biometrike. Sodni izvedenec za slikovno biometrijo mora razumeti in znati uporabiti različne metode za obdelavo slik in različna orodja računalniškega vida. Sposoben mora biti tudi razložiti svoje ugotovitve in koliko verjetni so končni rezultati.

Ključne besede: sodni izvedenci, slikovna biometrija, forenzika, prepoznava obrazov, identifikacija, videonadzor, računalniški vid

UDK: 343.983

1 Uvod

Množica snemalnih naprav, od pametnih telefonov do vedno večje mreže videonadzornih kamer, proizvede ogromno količino slikovnih in videoposnetkov. Videonadzora je vse več v javnih in tudi zasebnih prostorih. Zato strmo narašča število primerov, pri katerih so prisotni slikovni dokazi. Ko takšen primer pride pozneje na sodišče, je treba vključiti izvedenca z dobrim poznavanjem področja računalniške obdelave slik in računalniškega vida. Interpretacija različnih kaznivih dejanj, posnetih na video ali na fotografijah, ima poleg različnih drugih sledi (prstni odtisi, krvni madeži itd.) na sodišču vedno večjo vlogo. Za pravilno in neodvisno interpretacijo slikovnega gradiva je potreben sodni izvedenec, ki lahko neodvisno oceni in interpretira slikovno gradivo. Najpogostejša naloga pri takšni interpretaciji je potrditev ali identifikacija osebe na posnetku. Raziskovalci Laboratorija za računalniški vid na Fakulteti za računalništvo in informatiko Univerze v Ljubljani na slovenskih sodiščih že več kot 15 let sodelujemo kot sodni izvedenci za interpretacijo slikovnega in videomateriala.

V tem prispevku bi radi predstavili nekaj koristnih izkušenj iz naše prakse sodnega izvedenstva. Omejili se bomo na videoposnetke, na katerih so bile prisotne osebe, tako da so bile naloge izvedenca povezane z biometrijo. Naloge sodnega izvedenca za področje slikovne biometrične prepoznave so obsežnejše, kot je le uporaba sistemov za prepoznavo obrazov (Jain, Klare in Park, 2012). Tudi če se na koncu uporabi kateri od sistemov za prepoznavo obrazov, je treba pred tem izvesti več drugih slikovnih obdelav. Slike so navadno zajete pod najrazličnejšimi pogoji, ki niso najboljši. Zaradi tega je treba pred interpretacijo s slikami izvesti številne postopke za njihovo izboljšavo (popravek osvetlitve in kontrasta, odprava šuma, stabilizacija videa itd.). Ker obrazi na slikah pogosto niso zajeti od spredaj, ampak od strani in od zgoraj, standardnih sistemov za prepoznavo frontalnih obrazov ne moremo neposredno uporabiti. V primeru, da imamo na voljo več slik istega obraza z različnih zornih kotov, lahko iz teh zgradimo model obraza 3D in na podlagi tega določimo frontalni obraz (Hassner, Harel, Paz in Enbar, 2014; Park in Jain, 2007). Naslednja težava je lahko velika razlika v starosti med osebami, ki jih obravnavamo, in slikami oseb v kartoteki. V takih primerih je treba uporabiti metode za kompenzacijo sprememb zaradi staranja. Pri primerjavi osumljenca moramo upoštevati tudi spremembe na obrazu, ki so lahko posledica poškodb, ličil ali tetovaž. Če ni možno izvesti prepoznave na osnovi obraza, lahko preverimo še mehke biometrične značilnosti osebe na posnetku. Na primer, če je na sliki dovolj ravnih in pravokotnih linij, lahko ocenimo višino osebe na podlagi zgolj ene fotografije po pravilih perspektivne geometrije (Criminisi, Reid in Zisserman, 2000). Včasih se srečamo tudi z vprašanjem verodostojnosti slikovnega materiala,

[1] Dr. Borut Batagelj je višji predavatelj za računalništvo in informatiko ter član Laboratorija za računalniški vid na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. E-pošta: borut.batagelj@fri.uni-lj.si

[2] Dr. Franc Solina je redni profesor računalništva in informatike ter predstojnik Laboratorija za računalniški vid na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. E-pošta: franc.solina@fri.uni-lj.si

ali je kdo ponaredil posnetek, tako da je spremenil vsebino. Zaznavanje pristnosti slikovnega materiala obsega celo paleto metod, od analize na ravni slikovnega elementa, formata zapisa, do analize snemalne naprave in končno analize fizikalnih in geometrijskih lastnosti na zajeti sceni posnetka (Farid, 2009).

Z obdelavo oziroma izboljšavo slik, tako da je to, kar je prikazano na sliki lažje razberljivo, se ukvarja znanstveno področje obdelave slik (angl. *image processing*) (Petrou in Petrou, 2010). Z analizo oziroma interpretacijo slik v smislu, kaj je na sliki, pa se ukvarja znanstveno področje računalniški vid (angl. *computer vision*) (Prince, 2012). Pojem obdelava slik razumemo kot vsako opravilo na vhodni sliki ali seznamu slik, ki izboljša posnetek. Izhod obdelave je bodisi izboljšana slika bodisi njene karakteristike ali parametri slike. Večina metod za obdelavo slik obravnava sliko kot dvodimenzionalni signal in izvaja osnovne tehnike obdelave signala. S pomočjo teh tehnik lahko iz slike odstranimo šum, povečamo ostrino, popravimo barve itd. Bolj napredne analize slik obsegajo iskanje enotnih pomenljivih slikovnih regij – segmentacijo, registracijo in ujemanje slik. Najnaprednejše metode obdelave slik vsebujejo metode računalniškega vida, ki poskušajo na primer na slikah prepoznati določene objekte in jim slediti. Te metode poskušajo posnemati v grobem človeški zaznavni sistem, tako da iz dvodimenzionalnih slik razpoznajo posamezne objekte in rekonstruirajo okolje 3D, prikazano na sliki. Pri tem uporabljamo različne metode strojnega učenja in umetne inteligence.

Na trgu že lahko najdemo programsko opremo za pomoč pri forenzičnih nalogah na področju slikovnega in videomateriala (npr. Amped Software, 2014). Celotno področje slikovne biometrije se razvija tako hitro, da so največkrat zaradi boljše prilagodljivosti in večje fleksibilnosti za posamezno specifično nalogo uporabnejša samostojna, pogosto odprtokodna orodja.

V vsakem primeru mora izvedenec slikovne biometrije razumeti, kdaj in zakaj mora uporabiti nek korak ali metodo. Od sodišča imenovani izvedenec mora tudi znati razložiti celoten proces, kako je dobil rezultate in kako jih je preveril. V prispevku bomo predstavili nekaj težav pri identifikaciji oseb s pomočjo različnih biometričnih karakteristik, na katere smo v dolgoletni praksi naleteli pri svojem delu kot sodni izvedenci. Z opisom teh primerov bi radi ponazorili raznolikost biometričnih problemov v praksi in na potrebo po uporabi metod iz široke palete raziskovalnih dosežkov s področja računalniškega prepoznavanja vzorcev na slikah.

2 Prepoznava obrazov

Izvedencu sodišče najpogosteje postavi vprašanje: »Ali je na posnetku res obdolžena oseba?« To je vprašanje verifikacije. Navadno ima izvedenec na voljo tropozno fotografijo iz policijske kartoteke in videoposnetek iz nadzorne kamere. Najprej se pri identifikaciji osebe na videoposnetku omejimo le na obraz osebe. Tudi pričakovanja sodišča so, da bi na podlagi priloženega videoposnetka naredili natančno analizo obraznih značilnic. To vključuje velikost posameznih obraznih značilnic ter njihove medsebojne razdalje. V nadaljevanju bomo opisali najpogostejše težave pri prepoznavi obrazov v praksi.

2.1 Problemi iz prakse

2.1.1 Slaba kakovost posnetka

Videoposnetek iz nadzornih kamer je velikokrat preslabe kakovosti bodisi zaradi premajhne ločljivosti bodisi zaradi premočnega stiskanja podatkov. Navadno je to posledica nepremišljene nastavitve snemalnih naprav, da bi videomaterial zasedel manj spominskega prostora, in le redko posledica preslabega video signala snemalne naprave. Nekateri varnostni sistemi zaradi manjše porabe spomina shranjujejo samo omejeno število slik na sekundo oziroma samo takrat, ko sistem zazna premikanje na sceni. Zaradi teh naštetih okoliščin je pogosto takšen videomaterial preslab, da bi lahko uporabili napredne algoritme za prepoznavo obrazov, ki temeljijo na obraznih značilnicah ali pa na videzu obraza (Batagelj in Solina, 2006).

2.1.2 Majhna obrazna regija

Druga težava, s katero se strokovnjaki za prepoznavo obrazov pogosto srečujemo, so premajhni obrazi na slikah. Da bi z metodo za prepoznavo obrazov lahko dobili verodostojne rezultate, mora biti medočesna razdalja vsaj 32 slikovnih elementov. Idealno pa je, da je medočesna razdalja 70 slikovnih elementov. V praksi pogosto obdelujemo posnetke z majhno ločljivostjo, velikosti 320 × 240 elementov ali 640 × 480 elementov, na katerih je obraz zajet z velike razdalje. Na takšnem posnetku meri regija obraza 15 × 15 slikovnih elementov z medočesno razdaljo 8 slikovnih elementov. V takšnih primerih se uspešnost sistemov za prepoznavo močno zmanjša, tudi če so na posnetku dobro osvetljeni frontalni obrazi.

2.1.3 Nefrontalni pogledi

Obrazi na posnetkih nadzorne kamere so navadno zajeti od zgoraj in od strani, tako da največkrat niso posneti frontalno. Osebe, ki izvajajo kaznivo dejanje, pa se še dodatno izogibajo kameram in zato navadno nikoli ne pogledajo v kamero. Vse te

okoliščine pripeljejo do dejstva, da v celotnem videoposnetku nimamo niti ene frontalne slike obraza. Osebe na posnetkih imajo tudi pogosto delno prekrit obraz s sončnimi očali, kapuco ali kapo in tako še otežijo primerjavo osnovnih obraznih značilnic.

2.2 Možne rešitve

Zaradi vseh naštetih težav s kakovostjo slik in orientacijo obraza si velikokrat pomagamo z drugimi bolj vidnimi obraznimi značilnostmi, ki izstopajo tudi pri slikah slabše kakovosti. Takšne značilnosti so oblika glave, brade, ličnic, lasišča, pleše, barve las, ušesa, nosu, oblika ust in ustnic. Največkrat pripomorejo k boljši prepoznavi tudi katere nepravilnosti oziroma poškodbe iz preteklosti, ki jih ima osumljeni. Tu gre za poškodovan nos ali za izrazito obliko nosu, poudarjeno Adamovo jabolko pri moških, posebna plešavost. Vse to nam lahko olajša prepoznavo. Če ima obtoženi na obrazu ali vidnem delu telesa tetovažo, koristno uporabimo tudi to značilnost. Pri zelo slabem videoposnetku ali slabi ločljivosti lahko razpoznamo spremembo barve, saj gre pri tetovaži največkrat za velik kontrast s kožnim ozadjem.

2.2.1 Uporaba profila

Ko poskušamo analizirati obrazne značilnice osebe na posnetku, se izkaže, da je med vsemi orientacijami zelo uporaben obrazni profil, kjer so poudarjene določene obrazne značilnosti, na primer nos. Kot smo že omenili, je oseba na posnetku nadzornih kamer zajeta pod različnimi, večinoma netipičnimi zornimi koti. Te okoliščine moramo upoštevati tudi pri pogledu od strani. Če je osumljenec na voljo, lahko zaprosimo sodišče za dodatne obrazne posnetke pod različnimi zornimi koti, ki se najbolj ujemajo z zornimi koti na posnetku iz nadzorne kamere.

Slika 1: Silhueta osebe pred bankomatom

Obrazni profil je še posebej uporaben pri analizi slik iz nadzornih kamer bankomatov, saj je na teh slikah obraz osebe velikokrat podosvetljen, ker je v ozadju močna svetloba. Z dodatno spremembo osvetlitve lahko posnetek sicer malo izboljšamo, toda še vedno premalo, da bi bile vidne posamezne obrazne značilnice. Oseba pred bankomatom med nezakonitim dejanjem zaradi sumničenja pogosto pogleduje naokrog in tako lahko kamera zajame tudi obrazni profil, ki je zaradi bližine kamere in osvetlitve iz ozadja zelo jasen. Takšna silhueta nam pozneje služi kot referenčna slika pri prepoznavi osebe od strani (slika 1).

2.2.2 Uporaba sistemov za prepoznavo obrazov

Kljub vsem naštetim težavam z različnimi zornimi koti in slabo kakovostjo posnetkov lahko vseeno uporabimo klasične sisteme za prepoznavo obrazov iz frontalne slike obraza ali skice obraza. Pred uporabo takšnih metod ali sistemov moramo vhodno sliko obraza ustrezno prilagoditi. Poleg tega moramo rezultate iz takšnih sistemov znati pravilno interpretirati. Pred uporabo sistema za frontalno prepoznavo obrazov moramo iz posameznih pogledov najprej zgraditi tridimenzionalni model. Ta model nam nato omogoči generiranje frontalnega pogleda obraza, ki nam pozneje služi kot vhodna slika za sistem za prepoznavo (Hassner et al., 2014; Park in Jain, 2007). Sistem za primerjavo lahko uporabimo tudi na delno obrnjenih obrazih, vendar moramo takšen sistem z metodo strojnega učenja tudi učiti na tako obrnjenih obrazih. Drugi način uporabe obstoječih sistemov pa je, da na podlagi obraza na posnetku izdela strokovnjak za izdelavo fotorobotov skico osebe. Pri izdelavi skice mora zajeti čim več značilnosti obraza. Tako pripravljena skica služi nato kot vhodni podatek sistema za prepoznavo oseb na podlagi skic (Klare, Li in Jain, 2011).

Velikokrat se zgodi, da nepridiprava zalotijo pri dejanju. Nato pa sodišče zanima, ali je omenjena oseba zakrivila tudi kakšno drugo podobno, še nepojasnjeno kaznivo dejanje. V teh primerih moramo ugotoviti, koliko je obravnavana oseba podobna osebam na posnetkih nerazrešenih primerov. Obstoječi sistemi za verifikacijo nam pomagajo, da določimo stopnjo ujemanja med dvema osebama.

3 Identifikacija na osnovi drugih biometričnih značilnosti

Ker je identifikacija na podlagi obraza največkrat nemogoča oziroma ni dovolj natančna, moramo pogledati, ali lahko s posnetka varnostne kamere ugotovimo še kakšne druge telesne značilnosti osebe, ki bi pripomogle k identifikaciji osebe. Pri tem se lahko omejimo na fizične lastnosti osebe ali na značilnosti obnašanja. V nadaljevanju bomo predstavili nekaj najpogostejših lastnosti, na katere moramo biti pozorni in nam

lahko močno omejijo krog osumljencev. Najpogosteje poskušamo tako oceniti velikost osebe na posnetku (Criminisi et al., 2000). Naslednje lastnosti, ki so opazne pri daljšem spremljanju osebe, pa so način hoje (Kovač in Peer, 2013), rokovanje s predmeti in postava osebe.

3.1 Ocena višine osebe

Da bi ocenili višino osebe na sliki, lahko uporabimo metodo meritve iz enega pogleda (angl. *single view metrology – SVM*) (Criminisi et al., 2000). S pomočjo te metode lahko ocenimo višino osebe na osnovi le ene slike. Pred uporabo metode moramo sliko najprej izboljšati, tako da povečamo kontrast, osvetlitev in poudarimo robove. Če imamo na voljo video posnetek, se pravi, da imamo na razpolago več slik istega prostora pod različnimi svetlobnimi pogoji, lahko sliko izboljšamo tudi tako, da v določenem časovnem obdobju povprečimo isto ležeče slikovne elemente. Tako lahko še dodatno izostrimo in poudarimo robove statičnih predmetov na sliki.

Na tako izboljšani sliki lažje določimo geometrijske značilnice oziroma umerimo prostor v vseh treh dimenzijah (x, y, z) (slika 2). Če je slika na videoposnetku na robovih ukrivljena zaradi napake leč, moramo te nepravilnosti popraviti, da dobimo pravilno prikazane ravne predmete na sliki. Pri umerjanju prostora nam pomagajo predmeti, ki so poravnani s stenami prostora. Posebej koristni so v tem primeru s talnimi ploščicami tlakovani prostori, kjer stiki potekajo vzporedno z zidovi prostora in omogočajo, da enostavno umerimo ravnino $x – y$. Za določitev neznane višine moramo umeriti tudi navpično os z. V tem primeru se največkrat opremo na podboje vrat, oken ali popolnoma pokončno postavljene predmete v prostoru (slika 2).

Slika 2: Umeritev prostora moramo izvesti na izboljšani sliki. Oseba na posnetku ni v celoti vidna. Oceno višine osebe določimo na podlagi drugih izmerjenih višin predmetov na sceni.

Pri predmetih moramo paziti, da niso bili premaknjeni v času od zajema posnetka do umerjanja prostora. Pogosto se namreč zgodi, da je bil prostor v tem času preurejen. V takih primerih je lahko težavna določitev referenčnega predmeta. Tudi zato se največkrat omejimo na vrata in okna, ki se praviloma tudi v daljšem časovnem obdobju ne spreminjajo. V daljšem časovnem obdobju se lahko zamenja tudi videonadzorni sistem. Če želimo v takem primeru narediti rekonstrukcijo dejanja ali izmeriti višine, moramo sliko predhodno pravilno registrirati na sliko iz prejšnjega nadzornega sistema na osnovi znanih točk predmetov, ki se niso spremenili. Pred računanjem višine moramo vnesti referenčno višino znanega predmeta. Zato moramo tudi obiskati obravnavan kraj in izmeriti dimenzije čim več različnih predmetov na sceni, da bi nam pozneje pri ocenjevanju višine lahko služili tudi za kontrolo pravilne umeritve.

Zelo pomembno je, da vedno uporabljamo originalno sliko videoposnetka, na kateri izvajamo meritve. Na podlagi tega lahko pravilno ocenimo, kakšna je napaka meritve. Napaka pri določanju višine osebe na posnetku je odvisna od ločljivosti posnetka in od velikosti osebe na posnetku. S pomočjo metode SVM zato lahko podamo dobro oceno velikosti oseb na posnetkih. V posebnih primerih, ko oseba stoji pod podbojem vrat ali ko želimo izmeriti velikost predmeta (npr. odtis, copat), zadošča že umeritev le v dveh dimenzijah. Če leži predmet na umerjeni dimenziji prostora, zadošča že ena sama izmerjena dolžina.

3.1.1 Težave pri določanju višine osebe

Pri meritvah višine imamo največkrat težave, ker oseba na posnetku ni vidna v celoti. To pomeni, da se na primer ne vidijo stopala ali vrh glave. To se zgodi, če kamera ni postavljena dovolj visoko ali pa če oseba stoji preblizu kamere. V takšnih primerih si lahko pomagamo z rekonstrukcijo zakritih delov s pomočjo splošnega modela osebe ali opazovane osebe, če je zakriti del telesa viden na kakšni drugi sliki posnetka.

Druga zelo pogosta težava je ta, da je oseba na posnetku stalno v sključenem položaju zaradi teka ali hitre hoje. Če se oseba na posnetku ustavi in zravna, da jo kamera lahko zajame v pokončnem položaju, lahko to sliko uporabimo za meritev višine. Sicer pa moramo pri oceni višine upoštevati tudi dejavnik sključenosti. V takih primerih lahko z gotovostjo trdimo le to, da je oseba visoka vsaj toliko oziroma da ni manjša kot izmerjena višina. Koliko pa je oseba višja glede na ocenjeno višino, lahko dodatno ocenimo na podlagi razkoraka, v katerem je oseba (Ljungberg in Sönnerstam, 2008).

3.2 Druge telesne značilnosti – mehka biometrika

Če imamo na voljo daljši videoposnetek, lahko pozorno preučimo tudi obnašanje osebe. Iz hoje lahko prepoznamo določen vzorec ali značilnost, ki nam pomaga pri identifikaciji osebe (Kovač in Peer, 2013). Če gre za rokovanje z različnimi predmeti, smo pozorni na to, s katero roko oseba kaj opravlja. Pri nakupovanju opazujemo, s katero roko oseba jemlje izdelke s police, s katero plačuje, telefonira, dviga denar na bankomatu. Pomembno je tudi, na kakšen način nosi predmete, v kateri roki oziroma na kateri rami nosi torbo. Vse to pripomore k temu, da lažje določimo dominantno roko osebe ali vzorce obnašanja. Ugotovljene lastnosti nam pomagajo pri identifikaciji osebe.

Pri kraji predmetov moramo preveriti, ali oseba kaj skriva pod obleko ali se je mogoče zaradi tega spremenil način hoje. K identifikaciji osebe pripomorejo tudi različna znamenja, ki pri osebi izstopajo zaradi poškodb ali prirojenih napak. Zelo dobro so tudi na slikah slabše kakovosti prepoznavne tetovaže, ki na barvi kože velikokrat izstopajo.

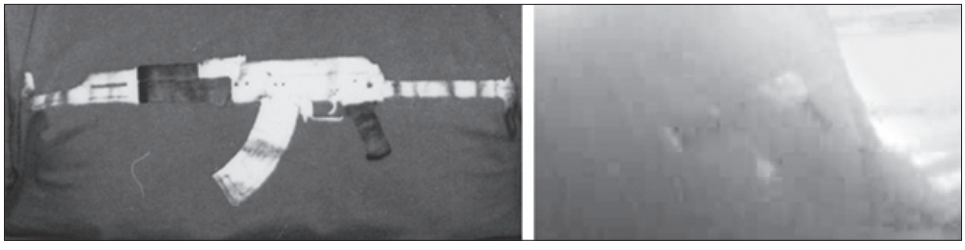
Pri identifikaciji oseb na posnetku, zato ne smemo gledati le na obrazne značilnice, ampak tudi na mehko biometriko, kar nam lahko omogoči, da zožimo preiskovalni seznam osumljencev ali da dobimo dokaz, ki izključuje obdolženo osebo. Zato je pomembno, da bi bila v policijski kartoteki fotografirana celotna postava osebe, da bi bile vidne vse telesne značilnosti in posebnosti.

Na sliki 3 levo lahko vidimo, da ima oseba nadpovprečno široke boke glede na svojo velikost. Takšno razmerje lahko preverimo tudi na slikah z videoposnetka (slika 3, na sredini in desno).

Če je oseba prijeta takoj po kaznivem dejanju, damo lahko večjo težo primerjavi značilnic, ki se sicer čez čas spremenijo, kot so dolžina, oblika in barva las, prisotnost brkov ali brade. V primerih, ko se oseba med časom od kaznivega dejanja do prijetja ne more preobleči, lahko preverimo tudi podobnosti oziroma posebnosti na oblačilih in obutvi.

Na sliki 4 vidimo, kako s tehniko izboljševanja slike z videoposnetka razpoznamo predmet, ki je viden na oblačilu obdolženega. Če gre za posebno oblačilo, je tudi pomembno, da to v poročilu opišemo, ker se lahko pozneje opravi hišna preiskava z namenom, da se poiščejo opisani predmeti.

Slika 3: Primer uporabe mehke biometrike (širina bokov) pri identifikaciji osebe.



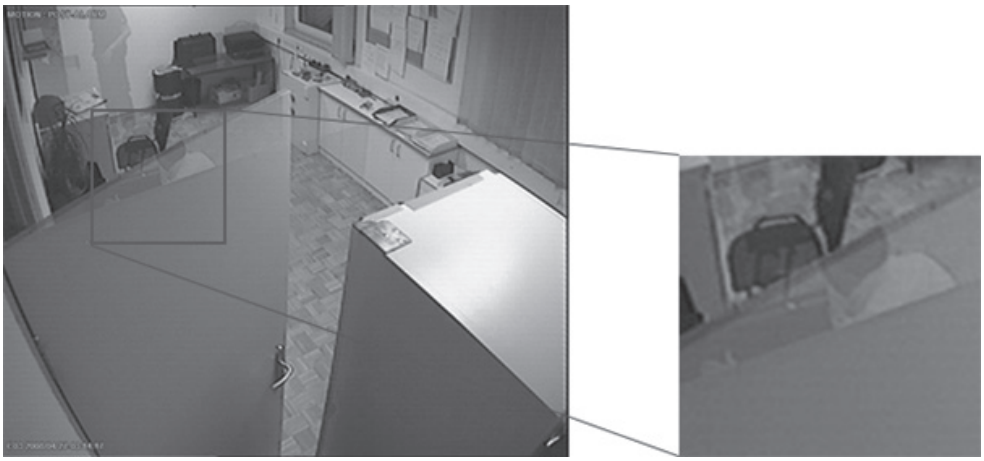
Slika 4: Levo: majica obdolženega, ki so ga prejeli takoj po dejanju, desno: izostrena majica na osebi iz posnetka nadzorne kamere.

4 Ugotovitve in druge izkušnje iz prakse

Pri postavljanju videonadzornega sistema moramo zagotoviti, da kamera pokriva celoten prostor, ki ga hočemo nadzorovati, in da je kakovost slike posnetka v vseh svetlobnih pogojih zadovoljiva. Predvideti moramo različne okoliščine, kjer se lahko ta dva parametra spremenita. Včasih potrebuje sistem veliko časa, da se prilagodi nenadnim spremembam osvetlitve ali celo ne deluje ob slabi osvetlitvi. Druga težava, s katero se velikokrat srečamo, je, da nekateri predmeti zakrivajo vidno polje kamere. Če so nekateri deli telesa opazovane osebe prekriti, je veliko težje izmeriti višino osebe. Na sliki 2 lahko vidimo, da je spodnji del osebe zakrit in zaradi tega določitev njene višine ni več preprosta. Ko merimo višino osebe na posnetku, je zelo pomembno, da navedemo, ali smo upoštevali, ali je oseba obuta ali ne. Slika 5 prikazuje primer slabo postavljene nadzorne kamere, saj odprta vrata zakrijejo velik del vidnega polja kamere, vključno s prostorom, kjer stoji trezor.

jih ni bilo mogoče pridobiti. Zakonsko je omejeno samo maksimalno obdobje hranjenja videomateriala. Po tem obdobju se stari posnetki prepišejo z novimi in zaradi tega posnetka pozneje ni mogoče pridobiti. Priporočila informacijskega pooblaščenca zagovarjajo sicer čim krajše časovno obdobje hranjenja podatkov. Večina izvajalcev videonadzora jih po našem vedenju hrani od sedem dni do treh mesecev. Največ se smejo hraniti do enega leta. Industrijski standard priporoča vgradnjo diskovnih polj v snemalno napravo, ki omogočajo minimalno vsaj 48 ur arhiva, da bi omogočili funkcionalno rekonstrukcijo dogodkov.

Pri zasegu videomateriala običajno zaseže le material iz prostora kaznivega dejanja. Izkazalo se je, da bi bilo treba upoštevati in uporabiti tudi javni nadzorni sistem, ki nam v določenih primerih omogoča določitev smeri bežanja oziroma skrivanja dokaznega materiala.



Slika 5: Primer neprimerno postavljene nadzorne kamere, kjer vrata zakrijejo velik del prostora, vključno s trezorjem, ki je najpomembnejši predmet v prostoru s stališča varovanja.

Pri dvigu denarja je zelo pomembna časovna usklajenost med videonadzornim sistemom in bančnim sistemom za zapisovanje transakcij. Če sistema časovno nista usklajena, ju lahko uskladimo na osnovi časovnih razmikov med posameznimi dvigi. Za tako uskladitev je zato zelo pomembno, da zasežemo daljše časovno obdobje videoposnetka, ki nam služi za to, da lahko na osnovi več transakcij določimo časovno neujemanje med sistemoma.

V nekaterih primerih se je naknadno izkazalo, da bi bili zelo koristni posnetki drugih videonadzornih sistemov v bližini kaznivega dejanja. Ker pa niso bili pravočasno zaseženi,

Pogosto se kakovost posnetka izgubi tudi zaradi neustreznega presnemavanja videomateriala. Zgodi se tudi, da se videomaterial izgubi oziroma odtuji. V takih primerih imamo na voljo le slike, ki so bile predhodno natisnjene na papir, kar pa predstavlja veliko slabšo kakovost. V nekaterih primerih že v osnovi ne razpolagamo z digitalnim originalom, ampak le s tiskanimi slikami slabe kakovosti, kjer so še toliko bolj potrebne napredne tehnike izboljševanja posnetkov (Bourlai, Ross in Jain, 2011).

5 Zaključek

Slikovni material iz videonadzornih sistemov, na katerem želimo identificirati osebe, pogosto ni primeren za neposredno uporabo v sistemih za samodejno prepoznavo oseb na podlagi obraza. Slike moramo predhodno izboljšati s pomočjo različnih tehnik za obdelavo slik in metod računalniškega vida. Včasih je treba tudi ročno opraviti katero nalogo, pri kateri spodleti sistemu za prepoznavo. Ekspert za izdelavo fotorobotov lahko na primer na podlagi videoposnetka nariše skico obraza, ki se nato uporabi kot vhod v sistem za prepoznavo obrazov iz skic obrazov. V primerih, ko sistema za prepoznavo obrazov ne moremo uporabiti, nam lahko pomaga pri identifikaciji tudi mehka biometrika, kot je višina osebe ali vzorci obnašanja.

Sodni izvedenec za področje biometrične identifikacije na osnovi slik mora zaradi tega pri svojem delu razumeti in znati uporabljati različne metode in orodja računalniškega vida in obdelave slik.

Literatura

1. Amped Software. (2014). *Amped FIVE: Product information guide*. Pridobljeno na http://dl.ampedsoftware.com/amped-five-en.pdf
2. Batagelj, B. in Solina, F. (2006). Face recognition in different subspaces: A comparative study. V A. L. N. Fred in A. Lourenço (ur.), *Pattern recognition in information systems: Proceedings of the 6th International Workshop on Pattern Recognition in Information Systems, PRIS 2006 in conjunction with ICEIS 2006* (str. 71–80). Insticc Press.
3. Bourlai, T., Ross, A. in Jain, A. K. (2011). Restoring degraded face images: A case study in matching faxed, printed, and scanned photos. *IEEE Transactions on Information Forensics and Security, 6*(2), 371–384.
4. Criminisi, A., Reid, I. in Zisserman, A. (2000). Single view metrology. *International Journal of Computer Vision, 40*(2), 123–148.
5. Farid, H. (2009). A survey of image forgery detection. *IEEE Signal Processing Magazine, 26*(2), 16–25.
6. Hassner, T., Harel, S., Paz, E. in Enbar, R. (2014). *Effective face frontalization in unconstrained images*. Pridobljeno na arXiv:1411.7964.
7. Jain, A. K., Klare, B. in Park, U. (2012). Face matching and retrieval in forensics applications. *IEEE MultiMedia, 19*(1), 2–10.
8. Klare, B. F., Li, Z. in Jain, A. K. (2011). Matching forensic sketches to mug shot photos. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 33*(3), 639–646.
9. Kovač, J. in Peer, P. (2013). Transformation based walking speed normalization for gait recognition. *Transactions on Internet and Information Systems, 11*(7), 2690–2701.
10. Ljungberg, J. in Sönnerstam, J. (2008). *Estimation of human height from surveillance camera footage – a reliability study* (Diplomsko delo). Jönköping: Jönköping University.
11. Park, U. in Jain, A. K. (2007). 3D model-based face recognition in video. V S. W. Lee in S. Z. Li (ur.), *Advances in biometrics, lecture notes in computer science, 4642* (str. 1085–1094). Berlin; Heidelberg: Springer.
12. Petrou, M. in Petrou, C. (2010). *Image processing: The fundamentals*. Chichester: Wiley.
13. Prince, S. J. D. (2012). *Computer vision: Models, learning, and inference*. Cambridge: Cambridge University Press.

Revija za kriminalistiko in kriminologijo / Ljubljana 66 / 2015 / 3, 259–266

Image-Based Biometrics in Forensic Science

Borut Batagelj, Ph.D., Senior Lecturer of Computer and Information Science, Faculty of Computer and Information Science, University of Ljubljana, Slovenia. E-mail: borut.batagelj@fri.uni-lj.si

Franc Solina, Ph.D., Professor of Computer and Information Science and Head of Computer Vision Laboratory at the Faculty of Computer and Information Science, University of Ljubljana, Slovenia. E-mail: franc.solina@fri.uni-lj.si

The paper recounts various problems that the authors encountered in biometric face recognition and biometric image interpretation in their experience as court appointed expert witnesses. Before an automated face recognition system can be applied on a typical surveillance video, images must be enhanced using various image-processing methods or enriched by using computer vision 3D reconstruction methods. Authenticity of video material must also sometimes be verified. If face recognition is not possible or successful then other soft biometric characteristics can be checked. A legal expert witness for image biometry must be able to employ a large array of image processing and computer vision tools and methods. The expert witness must be able to explain how the biometric results were obtained, what the necessary processing steps were, and how confident the final results are.

Keywords: expert witnesses, image biometrics, forensics, face recognition, identification, surveillance video, computer vision

UDK: 343.983