XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2013, Beograd, 3. i 4. decembar 2013.

MULTIMEDIJALNA FORENZIKA – DESET GODINA RAZVOJA

Andreja Samčović
Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *Veliki broj novih publikacija iz oblasti multimedijalne forenzike zahteva razmišljanje o defnisanju pojmova u novom istraživačkom području, kao i relacije sa već postojećim disciplinama. U ovom radu će biti predstavljena struktura forenzičkih disciplina. Multimedijalna forenzika i računarska forenzika spadaju u širu oblast digitalne forenzike, ali se razlikuju po modelu korisnika koji definiše pogled na realnost forenzičkog istražitelja. Zbog ograničenja multimedijalnih senzorskih podataka, stroga pouzdanost dokaza koja se zahteva kod računarske forenzike nije moguća kod multimedijalne forenzike. U radu će biti navedeni konkretni primeri koji potkrepljuju navedene stavove.*

Ključne reči: *multimedija, forenzika, računari, fotografije, slike*

1. Uvod

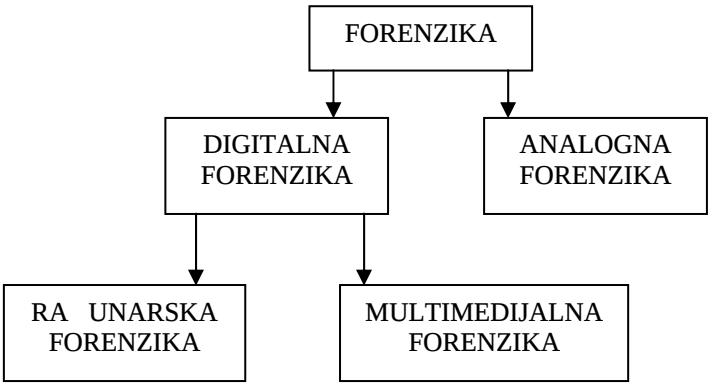
Napredak informaciono-komunikacionih tehnologija (IKT) u poslednjoj deceniji je doveo do digitalne revolucije koja je iz osnova promenila svet u kome živimo. Digitalne informacije koje se memorišu u računarskim sistemima postaju značajan deo naše svakodnevice. Štaviše, brojne fizičke ili društvene interakcije iz realnog sveta bivaju zamenjene računarskim komunikacijama. Kao posledica toga, pravni zakoni treba da budu prošireni i na digitalnu sferu, uključujući istraživanje i procesiranje kriminalnih radnji. S tim u vezi, javlja se potreba za naučno zasnovanom i pouzdanom rekonstrukcijom koja uključuje niz postupaka koji treba da se obave u digitalnoj sferi sa ciljem nalaženja pouzdanih dokaza. Navedeni postupak predstavlja preduslov u sprečavanju potencijalnih kriminalnih radnji u oblasti IKT [1].

Naučno zasnovani metodi koji imaju za cilj prikupljanje dokaza u kriminalnim istraživanjima se odnose na forenzičku nauku, ili forenziku (*forensics*). Termin forenzika ima etimološki koren u latinskoj reči *forum*, koja označava glavni trg, mesto na kome je sud imao javna zasedanja u antičkim vremenima. Pojam *računarska forenzika* se odnosi na slične tehnike kada su računari uključeni u kriminalne postupke. Računari mogu, sa jedne strane, da budu alat za izvršenje kriminala u realnom svetu, a sa druge strane, da predstavljaju medije preko kojih se obavlja kriminal u digitalnoj sferi. U oba slučaja,

forenzički istraživači pribavljaju dokaze iz računarskih sistema koji su involvirani u kriminalnim radnjama.

Situacija postaje složenija kada se uključe *senzori* u priču. Senzori prikupljaju delove realnosti i transformišu ih u digitalne signale, kao što su digitalne slike ili digitalni audio, koji se memorišu i obrađuju u računarskim sistemima. Digitalni signali koji predstavljaju delove realnosti mogu da budu objekat forenzičkih istraživanja, ali mogu da posluže i kao dokazi za pouzdanost i autentičnost podataka. Realizacija ovih ciljeva se odnosi na područje koje pokriva naučna disciplina *multimedijalna forenzika* [2].

Cilj ovog rada je da pojasni definicije novih pojmova iz forenzike i da ih uporedi sa klasičnom forenzičkom naukom poznatom iz analognog sveta, kao što je to pokazano na Slici 1.



Slika 1. Veza između forenzike, digitalne i multimedijalne forenzike

Na Slici 1 se može videti podela forenzičkih disciplina prema *domenu dokaza*. Domen dokaza predstavlja domen iz koga se izdvajaju dokazi. *Klasična (analogna) forenzika* se bavi prikupljanjem *fizičkih dokaza*, dok je *digitalna forenzika* usmerena ka istraživanju *digitalnih dokaza* [3]. Dok većina ljudi ima intuiciju šta su to fizički dokazi digitalni dokaz je nedodirljiv i stoga je više apstraktan. Kada se govori o digitalnim dokazima misli se na konačne sekvence diskretnih simbola, tipično uzetih iz binarnog alfabeta, kao što su nizovi bita izdvojenih iz računarske memorije i uređaja za memorisanje. Imajući to u vidu, računarska forenzika i multimedijalna forenzika koriste digitalne dokaze i stoga spadaju u širu oblast digitalne forenzike. Međutim, postoje i značajne razlike koje čine opravdanim postojanje ovih disciplina kao zasebnih oblasti. U praksi postoji često i preklapanje ove dve discipline.

Nakon uvodnog dela, u drugom poglavlju je predstavljena pasivna digitalna forenzika, koja pretpostavlja da nisu primenjeni mehanizmi za zaštitu multimedijalnih sadžaja. S tim u vezi, dato je nekoliko primera krivotvorenja fotografija kroz menjanje realnosti. Zatim su dati osnovni koncepti računarske forenzike. Naredna sekcija se bavi osnovama multimedijalne forenzike. Odnos između računarske forenzike i multimedijalne forenzike je objašnjen u sledećem poglavlju, pre zaključnih razmatranja.

2. Pasivna digitalna forenzika

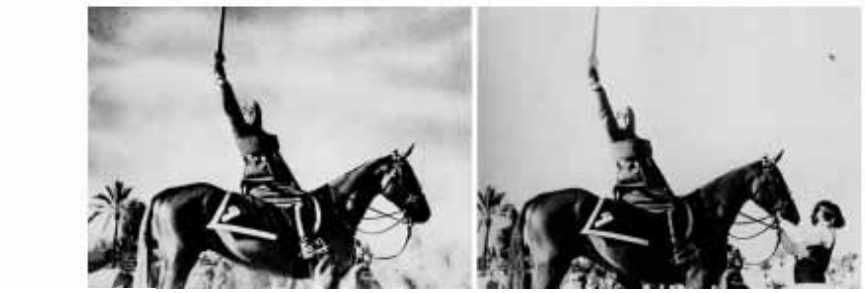
Zahvaljujući širokoj zastupljenosti interneta kao sredstva za masovnu komunikaciju, kao i dostupnosti relativno jeftinih kamera i fotoaparata visoke rezolucije, danas je naša realnost nezamisliva bez digitalnog multimedijalnog sadržaja, kao što su slike i video. Multimedijalni sadržaji se veoma lako distribuiraju preko web zasnovanih alata za razmenu sadržaja, kao što su društvene mreže, *Youtube, Picasa, Flickr*. Osim toga, veoma su zastupljeni u oblastima kao što su: novinarstvo, sport, naučne publikacije, političke kampanje i forenzička istraživanja.

Tradicionalno stanovište posmatra fotografije i video zapise kao verno i blisko predstavljanje stvarnosti. Međutim, u današnjem digitalnom dobu ova pretpostavka se više ne može uzimati u obzir, zbog mogućih manipulacija digitalnim multimedijalnim sadržajima. Manipulacije postaju moguće zahvaljujući širokoj dostupnosti računara visokih performansi, digitalnih kamera visoke rezolucije, kao i sofisticiranih softverskih alata za foto-editovanje i računarsku grafiku, kao što je to *Photoshop*. I korisnici koji nisu eksperti mogu lako da manipulišu i menjaju multimedijalne sadržaje, bez ostavljanja očiglednih tragova manipulacije. Kao posledica toga više se ne može pretpostavljati vernost i autentičnost slika i video zapisa, posebno kada se uzimaju u obzir forenzička i kriminalna istraživanja, sistemi za nadzor, medicinske slike i žurnalizam. Štaviše, promenjeni multimedijalni podaci mogu da utiču na mišljenje ljudi i čak da menjaju njihove stavove u odnosu na predstavljene događaje.

Lažni multimedijalni sadžaji imaju dugu istoriju, verovatno od nastanka fotografije u prvoj polovini XIX veka. Neki od ranih primera menjanja realnosti se odnose na generale i političare. Na Slici 2 je pokazana fotografija iz 1864. godine koja pokazuje generala Granta ispred svojih trupa u Siti Pointu, u Virdžiniji, za vreme Američkog građanskog rata. Istraživači iz Kongresne biblioteke u Vašingtonu su ustanovili da je fotografija zapravo sastavljena iz tri odvojene fotografije: glava je preuzeta sa drugog portreta generala Granta, konj i telo pripadaju generalu Mekkuku, dok je pozadina preuzeta sa fotografije zatvorenika koji su pripadali Konfederaciji.

Slika 2. Fotografija generala Granta iz 1864. godine koja je nastala kompozicijom tri druge fotografije snimljenih u različitim trenucima i uslovima [4]

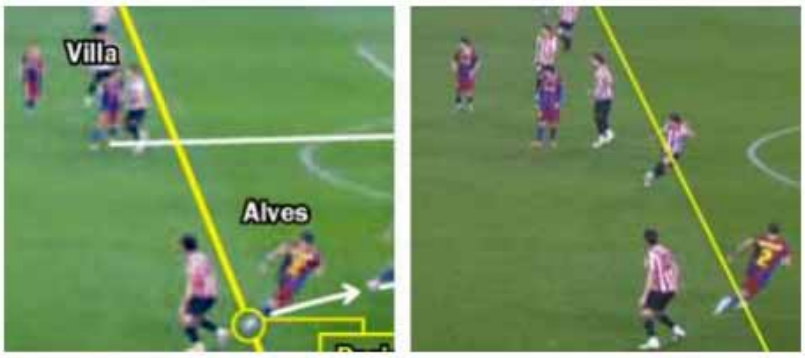
Drugi primer potiče iz II svetskog rata, kada je 1942. godine izmenjen portret italijanskog vođe Musolinija uklanjanjem lika koji je držao konja, kako bi vođa na fotografiji izgledao monumentalnije, što se vidi na primeru sa Slike 3.



Slika 3. Fotografija iz 1942. godine koja pokazuje kako je promenjena originalna slika brisanjem lika koji drži konja [4]

U to vreme bio je potreban visoki stepen tehničke ekspertize i specijalizovana oprema kako bi fotografija bila izmenjena. Danas postoji moderni softver koji veoma lako može da menja sadržaj fotografija, a od skoro i video zapisa, jednostavnije nego ikada i teže za otkrivanje.

Primer lažne slike je registrovan 2011. godine kada su španske sportske novine objavile izmenjenu fotografiju meča između Atletika Bilbao i Barcelone, sa namerom da se prikaže ofsajd. Međutim, originalni frejm pokazuje da je odbrambeni igrač digitalno izbrisan sa fotografije i prema tome nije bilo incidenta, što je pokazano na Slici 4. Novine su objavile javno izvinjenje, tvrdeći da je to doga došlo zbog greške u štampi.



Slika 4. Fotografija iz 2011. objavljena u španskom sportskom časopisu [4]

Kao što pokazuju navedeni primeri porast krivotvorenja slika je u značajnom porastu u svakodnevici i ima uticaj u našim životima i društvu. Pouzdanost digitalnih sadržaja ne može biti verno uzeta i može se postaviti pitanje da li multimedijalni sadržaji zaista predstavljaju verni prikaz realnosti. Odakle zaista potiče neka slika? Kakva je, zapravo, njena predistorija? Da bi se odgovorilo na ova pitanja, pasivna digitalna forenzika je privukla pažnju naučne zajednice u poslednjoj deceniji, imajući u vidu porast broja publikacija iz ove oblasti [5]. Za ovaj pristup digitalne forenzike kaže se da je pasivan ili

slep, jer ne uzima u obzir a priori informacije o dostupnom sadržaju, a sa druge strane nisu primenjivani mehanizmi zaštite integriteta, kao što je digitalni votermarking.

Pasivna digitalna forenzika je tesno povezana sa brojnim različitim naučnim disciplinama kao što su: računarska nauka, obrada signala i procesiranje kriminala. Imajući u vidu literaturu iz ove oblasti, mogu da se definišu sledeća istraživačka polja u okviru nje:

- Identifikacija izvora: cilj je da se identifikuje uređaj koji je prikupio sadržaj, istraživanjem tragova ostavljenih pri različitim koracima u procesu akvizicije slike. Osnovna ideja potiče iz klasične forenzičke nauke, gde se analiza metaka sprovodi na osnovu oznaka koje su jedinstvene za svako posebno oružje i prema tome može da se uspostavi veza između metka i oružja iz kojeg je ispaljen. Slično tome, kada se snimi slika postoji jedinstveni otisak koji se uvodi u sadržaj i koji ukazuje na uređaj pomoću koga je slika snimljena. Kada se slika prikupi ustanovi se šum u vidu artefakata na slici, distorzije ili statističkih osobina podataka. Takav šum je nevidljiv za ljudsko oko, ali može da se analizira uspešno doprinoseći procesu autentifikacije [6].
- Diskriminacija između sintetičkih i realnih slika: svrha je da se obavi diferencijacija između realnih i računarski generisanih slika, imajući u vidu povećani fotorealizam slika formiranih pomoću sofisticiranih trodimenzionalnih (3D) grafičkih alata čineći dati zadatak izazovnim kada je u pitanju samo vizuelna inspekcija. Zadati cilj se postiže preko algoritama za mašinsko učenje koji su modifikovani tako da klasifikuju prirodne i veštačke slike.
- Detekcija krivotvorenja: cilj je autentifikacija digitalnih sadržaja, uključujući slike i video zapise, što se zasniva na pretpostavci da krivotvorenje može da ne ostavi nikakvu indiciju o tome da se dogodilo, ali može da promeni statistiku sadržaja.

3. Računarska forenzika

Računari predstavljaju fizičke mašine koje čine deo naše svakodnevice. Kada se govori o računarskoj forenzici često se podrazumeva da je forenzička analiza ograničena na digitalne dokaze memorisane u statusu konačnih automata koje predstavlja svaki računar. To podrazumeva posmatrački model sa drastično redukovanim pogledom na realnost a to je da biti po sebi ne nose informacije o svojoj istoriji. Uobičajena je praksa da se napravi kopija digitalnog dokaza memorisanog na računaru i zatim da se istraživanja obavljaju isključivo na toj *read-only* kopiji, što uključuje navedeni posmatrački model [7].

Opisani pristup nije bez posledica na pouzdanost činjenica koje se izvode iz tako prikupljenih digitalnih dokaza. Broj stanja u zatvorenom sistemu je konačan, tako da uvek postoji mogućnost da sofisticirani kriminalac perfektno izbriše sve moguće tragove. Pretpostavljajući da je sve memorisano na hard disku brisanje može biti obavljeno korišćenjem računara podizanjem preko kompakt diska, ne menjajući pri tome ništa na hard disku.

Perfektno brisanje tragova u praksi nije uvek jednostavno. Broj mogućih stanja koja je neophodno proveriti raste eksponencijalnom progresijom. Na primer, personalni računari (PC) koji imaju prostor na disku od 100 GB, imaju $(2^{10})^{11}$ mogućih stanja. Radi

poređenja, procenjuje se da broj atoma u univerzumu ima red veličine $(2^{10})^3$. Pogotovo u složenim modernim umreženim sistemima sa brojnim softverskim komponentama i hardverskim interfejsom je teško nekome da kontroliše sve delove tako kompleksnog sistema. Međutim, kriminalac može da koristi drugi sistem koji simulira relevantni računar u kriminalnom scenariju na virtuelnoj mašini. Simulacija može da pomogne konstrukciji validnih stanja uz razumno vreme i napore, kao jedan mali deo broja svih mogućih stanja. U praksi, za istraživače je često teško da odrede granice sistema koji treba da se analizira, posebno ako se koriste bežične mreže.

Postavlja se pitanje da li može da se princip transfera primeni na računarsku forenziku. Brojni istraživači u praksi smatraju da može, jer iz iskustva znaju da kriminalci prave greške i ostavljaju tragove kriminalnih aktivnosti kao dokaze. Međutim, digitalna priroda dokaza čini mogućim perfektno prekrivanje tragova. Štaviše, za razliku od praktičnih ograničenja koja ima posmatrač u analognoj forenzici, kriminalac ovde zna unapred sve ili gotovo sve o "slepim tačkama" forenzičkih istražitelja i tako može da se prilagodi kroz plasiranje lažnih ili pogrešnih činjenica. Prednosti relativno jeftine računarske forenzike, zahvaljujući automatizaciji, leže u tome što većina istražnih radnji može da se obavi u radnim prostorijama forenzičkih istražitelja. Imajući u vidu da se danas dosta socijalnih interakcija pomera u digitalnu sferu, istraživači koje finansira država treba da donesu delikatnu odluku o alokaciji resursa između eksploatacije fizičkih i digitalnih dokaza.

Potpuno različita situacija nastaje ako se računarska forenzika posmatra u širem smislu da uključuje i fizičke i digitalne dokaze. Dodatni fizički dokazi, kao što su podaci o temperaturi, promeni frekvencije električne mreže, sve vrste analognih tragova na medijima za memorisanje, mogu da posluže u kriminalnoj istrazi, iako je ponekada skupo da se prikupe. Digitalni ili digitalizovani dokazi memorisani u drugim uređajima mogu da formiraju dodatnu informaciju ako je njihov identitet bezbedan.

3. Multimedijalna forenzika

Važna klasa digitalnih podataka koja se često nalazi i analizira na masovnim uređajima za memorisanje jesu digitalni multimedijalni podaci. Uprkos tome što su digitalni i digitalizovani mediji prisutni u našoj svakodnevici, nikada nije bilo jednostavnije manipulisati medijskim podacima. Sofisticirani softver omogućava i korisnicima sa malo ili nimalo iskustva da uz mali napor značajno menjaju sadržaj digitalnih medija. Kao rezultat toga javljaju se brojna pitanja u vezi autentičnosti medijskih sadržaja, što je od posebnog interesa za sud, gde odluke mogu da budu zasnovane na dokazima u formi digitalnih medija.

U prethodnoj deceniji relativno nova oblast kao što je multimedijalna forenzika je doživela nagli razvoj angažujući istraživače iz oblasti kao što su: multimedijalna bezbednost, računarska forenzika, obrada signala i slike. Uprkos tome što je multimedijalna forenzika, kao i računarska forenzika, zasnovana na digitalnim dokazima, činjenica da se simboli prikupljaju pomoću senzora je izdvaja, što ima uticaja i na poudanost dokaza.

Istraživači na polju multimedijalne forenzike imaju za cilj da razviju alate za prikupljanje tragova prethodnih manipulacija na polju medija, kao i da prikupe podatke vezane za izvorne uređaje. Ova dva postupka se nazivaju scenario detekcije manipulacije i scenario identifikacije, respektivno. Multimedijalna forenzika u ovom smislu nije samo

analiza semantike digitalnih ili digitalizovanih medijskih objekata. Tehnike u okviru multimedijalne forenzike obezbeđuju način za testiranje autentičnosti i izvora. Činjenice koje se izvode iz multimedijalnih sadržaja su od koristi jedino ako su podaci pouzdani i autentični npr. identifikacija osobe koja govori iz snimljenog govora sa mikrofona, ili registarska tablica automobila uzeta iz snimaka sa video nadzora.

Kod multimedijalne forenzike se generalno smatra da forenzički istražitelj nema prethodno znanje o originalu. Takvi metodi se nazivaju slepi ("*blind*") i uobičajeno koriste dva izvora digitalnih tragova:

- Karakteristike uređaja za prikupljanje podataka mogu da se provere u njihovom prisustvu (scenario identifikacije);
- Artefakti prethodno izvedenih radnji mogu da se detektuju u scenariju detekcije manipulacija.

Prva klasa tragova je povezana sa procesom prikupljanja digitalnih medija. Pošto se senzori razlikuju u načinu kako transformišu delove realnosti u diskretne signale, smatra se da svaki uređaj za prikupljanje ostavlja karakteristične oblike u izlaznim podacima. Nivo promena određuje da li će odgovarajući tragovi biti korišćeni za izdvajanje klase, modela, ili specifičnog uređaja za prikupljanje podataka. Savremene multimedijalne forenzičke tehnike su većinom usmerene ka analizi digitalnih slika. U literaturi su najviše proučene karakteristike CCD/CMOS (*Charged Coupled Device / Complementary Metal-Oxide Semiconductor)* senzorskih šumova, koji se pojavljuju praktično kod svih digitalnih kamera ili skenera [8]. Procene tkz. neuniformnosti foto odgovora (*Photo Response Non-Uniformity* – PRNU) služe kao digitalni otisak koji omogućava identifikaciju pojedinih uređaja za akviziciju podataka. PRNU predstavlja izvor šuma koji prouzrokuje male ali sistematske devijacije u osetljivosti svetla pojedinih senzorskih elemenata. Ovde može da se uspostavi analogija sa ogrebotinama kod metaka u klasičnoj forenzici.

Pored koristi tragova koji potiču od specifičnih uređaja u scenariju identifikacije, široku primenu nalaze i kod detekcije manipulacija. Posmatranjem karakteristika uređaja u celom digitalnom medijskom objektu mogu da se uoče devijacije na izlazu senzora. Na primer, analiza blok po blok može da ukaže na odustvo PRNU u nekim regionima slike, što vodi ka mogućem lokalnom postprocesiranju.

Postoji više načina kako da se otkriju manipulacije nad digitalnim medijima. Tragovi primenjenog postprocesiranja mogu da sami za sebe budu veoma indikativni. Forenzički metodi koji koriste ovaj pristup su suprotni metodama koje su zasnovane na karakteristikama uređaja. Prisustvo posebnih oblika ukazuje na moguće postprocesiranje. Tipični tragovi manipulacije uključuju periodične interpikselske korelacije posle geometrijskih transformacija, kao što su skaliranje ili rotacija digitalnih slika, ili identifikacija duplih regiona na slikama posle operacija tipa "*copy-paste*". Primer za manipulaciju nad slikama pokazan je na Slici 5, koji pokazuje sliku lansiranja rakete koja je analizirana detektorom tipa "*copy-paste*".

Slika 5. Primer manipulacije nad slikom i detekcije pomoću multimedijalne forenzike [2]

4. Odnos između računarske forenzike i multimedijalne forenzike

Iako se i računarska forenzika i multimedijalna forenzika bave istraživanjem digitalnih dokaza, smatra se da zbog svoje razvijenosti danas čine posebne grane digitalne forenzike. Domen dokaza je ograničen na niz diskretnih simbola pronađen na određenim uređajima. Kod multimedijalne forenzike se pretpostavlja da su digitalni dokazi prikupljeni nekim senzorom. Postojanje senzora koji transformišu prirodne fenomene u diskretne signale, koji su potom objekat istraživanja, ukazuje na to da multimedijalna forenzika može da se smatra empirijskom naukom. Forenzički istražitelji nikada ne mogu da dođu do saznanja da li deo digitalnog medija reflektuje realnost ili ne. Isto tako, počinilac kriminalne radnje ne može da bude nikada siguran da li je njegova manipulacija ostavila neki trag koji kasnije može da bude detektovan. Za razliku od računarske forenzike, digitalni dokazi kod multimedijalne forenzike su povezani sa spoljašnjim svetom i ne mogu da budu reprodukovani pomoću mašina. Imajući to u vidu, princip transfera ima svoje mesto u multimedijalnoj forenzici.

Multimedijalna forenzika koristi modele realnosti. Identifikacija kamere pomoću PRNU, na primer, pretpostavlja da šum senzora poseduje neku verovatnoću raspodele, koja se najčešće aproksimira Gausovom raspodelom. Na taj način, problem može da se formuliše kao problem testiranja hipoteze sa optimalnim detektorom za primenjeni model. Drugi modeli se primenjuju kod detekcije manipulacije tipa "*copy-paste*". Kod njih je pretpostavka da nije verovatno da se povezani regioni sa identičnim, ali ne i konstantnim, vrednostima piksela pojavljuju na originalnim slikama.

Kvalitet činjenica proističe iz kvaliteta modela koji koriste metode multimedijalne forenzike. Što bolje upotrebljeni metod može da objasni i predvidi detalje realnosti, to su pouzdanije odluke koje se donose zahvaljujući primenjenom modelu. Model PRNU koji uključuje različite orijentacije slike definitivno ima prednost u odnosu na modele koji to ne nude. To može da pomogne da se smanji verovatnoća pogrešne detekcije. Pogrešna upozorenja mogu da budu redukovana uklanjanjem artefakata kao što su tragovi od procena PRNU.

Važno je da se naglasi da nesigurnost u pogledu uopštenja realnosti nije jedina fundamentalna razlika između multimedijalne forenzike i računarske forenzike. Transformacija iz analognog sveta u diskretne simbole po sebi unosi dodatne stepene slobode na senzorskom nivou. Posebno je kvantovanje važno kod svih multimedijalnih forenzičkih tehnika, ali takođe i sve vrste postprocesiranja unutar senzora treba da budu uzete u obzir pri analizi podataka sa digitalnih medija. Po definiciji kvantovanje prouzrokuje gubitak informacije i stoga uvodi nesigurnost u forenzičku analizu.

Kvantovanje se ovde ne odnosi samo na tehnike kompresije sa gubicima kao što je JPEG (*Joint Photographic Expert Group*), već takođe i na rezoluciju izlaznih podataka. Ovde treba naglasiti da JPEG kompresija predstavlja najvažniji izvor nesigurnosti u praktičnim aplikacijama, budući da su skoro svi forenzički metodi manje ili više osetljivi na jaku JPEG kompresiju. Kada se razmatra šta čini senzor u širem smislu npr. uključivanje tehnika za kompresiju podataka, pre ili kasnije se dolazi do pitanja koji postupci predstavljaju legalno postprocesiranje. Na primer, skeniranje štampanih slika može da rezultuje vrlo grubim digitalnim predstavljanjem realnosti, ali tragovi nekonzistentnog osvetljavanja mogu da budu vidljivi. Uopšteno posmatrajući, kvalitet senzorskog izlaza neophodnog za kvalitetnu forenzičku analizu veoma zavisi od primenjene tehnike, što je još jedan aspekat koji ne važi u računarskoj forenzici, gde digitalni simboli nisu povezani sa spoljnim svetom već čine zatvoren sistem.

5. Zaključak

U ovom radu je razmotrena struktura različitih forenzičkih disciplina imajući u vidu primarni domen dokaza. Postalo je poslednjih godina evidentno da činjenica da li je digitalni dokaz prikupljen iz realnog sveta pomoću senzora ili predstavlja zatečeno stanje jednog zatvorenog računarskog sistema predstavlja razliku između forenzičkih disciplina uvažavajući pouzdanost izdvojenih činjenica. Teže je krivotvoriti medijske podatke neopaženo nego manipulisati drugim digitalnim dokazima. Uvođenje modela posmatrača pomaže da se odvojeno posmatraju računarska forenzika i klasična analogna forenzika.

U praksi se može dodgoditi preplitanje ovih disciplina. Forenzički istražitelji mogu da istražuju hard disk nekog računara, na kome digitalne fotografije mogu da budu pronađene metodama računarske forenzike. Multimedijalna forenzika se zatim primenjuje kako bi se povezale fotografije sa odgovarajućim digitalnim fotoaparatima ili kamerama. Otisci na aparatima mogu da ukazuju na identitet kriminalca koristeći policijsku bazu podataka. Imajući to u vidu, sve discipline forenzike mogu da budu zastupljene povezujući digitalne i analogne dokaze, formirajući kompletni lanac dokaza.

Literatura

[1] B. Carrier, E.H. Spafford: 'Getting physical with the digital investigation process', *International Journal of Digital Evidence*, Vol. 2, No. 2, 2003.

[2] R. Boehme, F.C. Freilling, T. Gloe, M. Kirchner: 'Multimedia forensics is not computer forensics', *3rd International Workshop on Computational Forensics*, The Hague, Netherlands, 13-14. August 2009.

[3] E. Casey: '*Digital evidence and computer crime*', 2nd edition, Academic Press, 2004.

[4] V. Conotter: *Active and passive multimedia forensics*, PhD dissertation, University of Trento, Italy, 2011.

[5] T.T. Ng, S.F. Chang, C.Y. Lin, Q. Sun: 'Passive-blind image forensics', in *Multimedia security technologies for digital rights*, pp 383-412, Academic Press, 2006.

[6] N. Khanna, G.T.C. Chiu, J.P. Allebach, E.J. Delp: 'Forensic techniques for classifying scanner, computer generated and digital camera images', *2008 International Conference on Acoustics, Speech and Signal Processing* ICASSP 2008, pp 1653-1656, 2008.

[7] M. Milosavljević, G. Grubor: *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, 2009.

[8] M. Chen, J. Fridrich, M. Goljan, J. Lukaš: 'Determining image origin and integrity using sensor noise', *IEEE Transactions on Information Forensics and Security,* Vol. 3, No. 3, pp 539-552, 2008.

Abstract: *An increasing number of new publications in the field of multimedia forensics requires thinking about definition of terms in this new research area, as well as relationships with existing disciplines. The structure of forensic disciplines is presented in this paper. Multimedia forensics and computer forensics belong to the broader field of digital forensics, but they differ in the observer model that defines the user's view on the reality of forensic investigators. Due to the limitations of multimedia sensor data, strict reliability of the evidence that is required in computer forensics is not possible in multimedia forensics. The paper gave specific examples that support these points.*

Keywords: *multimedia, forensics, computers, photographies, images*

MULTIMEDIA FORENSICS – TEN YEARS OF DEVELOPMENT

Andreja Samčović