UDK 343.983:004
Izvorni naučni rad
Prihvaćen: 8.3.2017.

*Ranko Petrović**
Vlatacom institut visokih tehnologija, Beograd

*Irini Reljin***
Elektrotehnički fakultet u Beogradu

ULOGA FORENZIKE U OTKRIVANJU ZLOUPOTREBE DIGITALNE SLIKE

Apstrakt: S obzirom da je razvoj informacione tehnologije u potpunosti promenio način pristupa, obrade i deljenja informacija i da je danas, zahvaljujući Internetu, ogromna količina podataka doslovno na dohvat ruke, sve više do izražaja dolaze i negativne posledice ove pojave, naročito kada su u pitanju multimedijalni podaci. Rad se bavi aktuelnim problemom manipulacije nad digitalnom slikom čija uloga može biti da prikrije, naglasi ili u potpunosti izmeni određenu informaciju u slici sa posledicama u rasponu od trivijalnih do katastrofalnih, kao i ulogom digitalne forenzike u otkrivanju i dokazivanju izvršene manipulacije. Sa tim u vezi u radu su u najkraćim crtama opisane jedne od najčešćih manipulacija koje se izvršavaju nad slikom, copy-move ili kloniranje i splicing ili fotomontaža. Takođe su prikazani konkretni primeri copy-move manipulacije urađeni u Corel Photo Paint X5 programu, kao i promene u histogramu slike do kojih u tom slučaju dolazi, a koje dokazuju da je slika pretrpela određene promene. Na kraju je opisan i postupak forenzičke tehnike koja se zasniva na formatu slike, tzv. dvostruki JPEG. Pokazano je kako dvostruko komprimovanje koje je gotovo neizostavno u procesu manipulacije uvodi specifične efekte koji ne postoje u jednostruko komprimovanim slikama. Cilj rada je da ukaže na potrebu i važnost da se sačuva identitet i autentičnost digitalne slike, zatim da ukaže na mogućnosti manipulacije nad slikom, kao i da se ukoliko su manipulacije izvršene, one otkriju i neporecivo dokažu, u čemu svakako glavnu ulogu ima digitalna forenzika.

Ključne reči: digitalna slika, zloupotreba, dvostruka kompresija, digitalna forenzika

* *ranko.petrovic@vlatacom.com; ranko.petrovic@mts.rs*

** Redovni profesor, *irinitms@gmail.com*

1. UVOD

U borbi protiv kriminala najsnažnije društveno oružje je zakon kojim svaka društvena zajednica na osnovu sopstvene kulture i procenjenih potreba definiše koja su dela zabranjena i koje su i kolike sankcije predviđene za činjenje takvih dela. U sprovođenju krivičnog zakona ključna faza je otkrivanje i dokazivanje učinjenog krivičnog dela. Sa razvojem civilizacije umnožavale su se vrste, forme i šeme kriminala, ali su paralelno sa tim nastajali, razvijali se i usavršavali pravni sistemi društvenih zajednica. Kako su se pravni sistemi usavršavali i postajali demokratičniji, razvijala su se i zaoštravala pravila o postupanju i dokazivanju učinjenih kriminalnih dela. Iz tih razloga, a uz porast raznovrsnosti i složenosti kriminalnih dela, javila se potreba, koja se vremenom samo uvećavala, da se u proces dokazivanja uključi i nauka. Upravo ta potreba je dovela do nastanka jedne nove naučne discipline poznate pod nazivom forenzika.

2. FORENZIKA – ISTORIJSKI OSVRT

Razvojem društva razvijali su se svest i znanje, što je nagoveštavalo velike promene i na planu borbe protiv kriminala, odnosno na planu otkrivanja i dokazivanja kriminalnih dela. Ne postoji konsenzus o tome kada je tačno nauka prvi put ušla u domen sprovođenja zakona, mada je sigurno bila u nekim delovima sveta u upotrebi mnogo pre nego što je postala priznato polje izučavanja.[1]

Mnogi veruju da je ser *Artur Konan Dojl* prvi popularizovao primenu savremene forenzičke analize kroz svoje novinske serijale prvobitno objavljene 1887. godine, predstavljajući izmišljeni lik *Šerloka Holmsa*. Smatra se da je ovaj rad inspirisao mnoge od prvih forenzičkih naučnika. Jedan od njih bio je Francuz *Edmond Lokard*, koji je izneo tvrdnju da se, kada dva objekta dođu u kontakt jedan sa drugim, dešava unakrsni transfer dokaza. Ovo je osnova *Lokardovog načela razmene*, koje je temelj onoga kako često mogu da se koriste fizički dokazi da povežu ili barem dovedu u vezu osumnjičenog sa licem mesta ili žrtvom.[2]

Inače, izraz *forenzika* potiče od latinske reči *forensis* u značenju *forum* (opisno: „*pred forumom*“, odnosno „*pred sudom*“). U rimsko doba, suđenje okrivljenom značilo je javno predstavljanje slučaja grupi javnih ličnosti u forumu. I osoba okrivljena za kriminal i tužilac bi pred forumom izlagali svoju stranu priče. Osoba sa boljom argumentacijom i prezentacijom (boljim forenzičkim veštinama) bi određivala ishod slučaja.[3]

Forenzika (*forenzičke nauke, ređe sudske nauke*) je primena naučnih metoda i tehnika iz širokog spektra naučnih disciplina, kao što su hemija, biologija, fizika,

1 E. Bergslien /2012/: *Chapter 1, A Brief History of Forensic Science and Crime Scene Basics*, from *An Introduction to Forensic Geoscience*, 1st ed, Blackwell Publishing Ltd, p. 1.http://media.wiley.com/product_data/excerpt/56/11182279/1118227956–16.pdf.

2 E. Bergslien, *ibid*, p. 8; *Forensic Analysis*, Encyclopedia of Polymer Science and Technology, http://docs4.chomikuj.pl/333787021,PL,0,1,Forensic-Analysis.pdf, 15.12.2016.

3 *Forensic /2012/*, http://en.wikipedia.org/wiki/Forensic, 15.12.2016.

medicina, matematika, elektrotehnika i informatika, za istragu kriminalnih radnji s ciljem pružanja odgovora na pitanja od interesa za pravni sistem, tj. za utvrđivanje činjenica u sudskim ili upravnim postupcima. Obuhvata širok spektar nastojanja, od prikupljanja i analiziranja dokaza do svedočenja eksperata, odnosno veštačenja na sudu.

Međutim, za razliku od ranijih vremena, pojava informacione tehnologije i rapidno širenje njene primene uslovili su nastajanje novog ambijenta u kojem su kriminalci dobili nove prilike i mogućnosti, sa brojnim specifičnim karakteristikama koje su uvećale njihovu moć. Jedna od vrlo značajnih vrsta zloupotrebe informacionih tehnologija novijeg datuma je i zloupotreba multimedijalnog sadržaja. Najčešći oblik ove vrste zloupotrebe je usmeren na krađu ili obmanu, a najčešći način je krivotvorenje (falsifikovanje) multimedijalnih podataka. Krađa je usmerena, pre svega, na intelektualnu svojinu u koju spadaju naučni rezultati, književna dela, umetnički radovi i muzika.

Prevare digitalnim multimedijalnim sadržajima obavljaju se na „bezbroj" načina, a toliki je i broj mogućih razloga, odnosno motiva za takve prevare. Pri tome treba reći da se pod prevarom podrazumeva namerno veštački proizvedena (fabrikovana) laž da bi se maskirala istina.

Zloupotreba digitalnih multimedija se javlja kada se sadržina slike, ilustracije, animacije, audio ili video zapisa falsifikovanjem menja da bi se izvršila obmana. S tim u vezi konstatovano je da je ključni problem u suzbijanju novih i usavršenih klasičnih formi kriminala prisutnost sve veće suptilnosti u njegovom izvršavanju, što značajno otežava njegovo otkrivanje i dokazivanje.

3. DIGITALNA FORENZIKA

Nastanak informacione tehnologije sredinom XX veka i rapidno širenje njene primene u svim oblastima čovekovog života značajno je uticalo da se skoro sve ljudske aktivnosti u oblastima rada, stvaranja, učenja i zabave odvijaju lakše, brže, obimnije i kvalitetnije. Zahvaljujući tome društvena zajednica ostvaruje snažan napredak u sopstvenom razvoju.[4]

Nažalost, kao i u svim prethodnim istorijskim epohama, uvek su se javljali pojedinci i organizovane grupe koje su želele da u ličnom interesu zloupotrebe mogućnosti novonastalih tehnologija. Ono što posebno zabrinjava u ovoj situaciji jeste činjenica da informaciona tehnologija kriminalcima obezbeđuje brojne prilike i mogućnosti i moćne alate za izvršavanje vrlo složenih i obimnih kriminalnih dela, često na načine koje prošlost nije poznavala, a koje je, isto tako često, teško i predvideti, a još teže dokazati.

Upravo zbog toga, otkrivanje i dokazivanje zloupotreba informacionih tehnologija postalo je jedno od krucijalnih pitanja današnjice, kako zbog posledica koje izaziva društvenoj zajednici, tako i zbog činjenice da su tradicionalne forenzičke metode i alati postali primitivni i neefikasni za upotrebu u informacionom ambijentu.

4 *Forensic*, *ibid*.

Izneto jasno ukazuje, a već prvi slučajevi su potvrdili, da je otkrivanje i dokazivanje učinjenih dela zloupotrebe informacionih tehnologija izuzetno složen i zahtevan zadatak, koji je uz to i prepun specifičnosti. Upravo ove specifičnosti i njihovo uspešno razrešavanje nametnuli su imperativnu potrebu razvoja nove grane forenzičkih nauka koja bi, u novim uslovima, doprinela i omogućila lakše i uspešnije otkrivanje, dokazivanje i sankcionisanje kriminalnih dela zloupotrebe informacione tehnologije.

Novo-rođena naučna disciplina poznata pod nazivom *računarska forenzika*, definiše se kao *metodička serija tehnika, procedura i alata koji se koriste za pronalaženje dokaza u računaru, računarskoj opremi, raznim skladišnim uređajima i digitalnim medijima, koji mogu biti predstavljeni u sudu u koherentnoj i sadržajnoj formi.*[5] U širem smislu računarska forenzika podrazumeva naučno sticanje, očuvanje (konzerviranje), identifikovanje, ekstrakciju, analiziranje, interpretaciju (tumačenje) i dokumentovanje računarskih dokaza koji se mogu koristiti kao dokazi na sudu.[6]

Uvećavanje broja i raznovrsnosti zloupotrebe informacione tehnologije i radijusa njenog dejstva uslovili su uvođenje novog termina – *digitalna forenzika*. Ovaj termin je izveden kao sinonim za računarsku forenziku, čija je definicija proširena tako da obuhvati forenziku svih digitalnih tehnologija:[7]

> *„Upotreba naučno izvedenih i dokazanih metoda u svrhu očuvanja, prikupljanja, validacije, identifikacije, analize, tumačenja, dokumentovanja i prezentacije digitalnih dokaza izvedenih iz digitalnih izvora u cilju olakšavanja ili unapređenja rekonstrukcije događaja da bi se utvrdilo da li je u pitanju kriminal ili ne.“*

Nažalost, ne postoji standardna ili konzistentna (dosledna) metodologija digitalne forenzike, već pre skup procedura i alata izgrađenih na osnovu iskustava kriminalističkih službi, administratora sistema i hakera. Palmer[8] sugeriše da evolucija digitalne forenzike nastaje iz *ad hoc* alata i tehnika, pre nego iz naučne zajednice, odakle su potekle mnoge od drugih tradicionalnih forenzičkih nauka. Ovo je problematično, jer se dokazi moraju dobiti korišćenjem metoda za koje je dokazano da pouzdano izdvajaju i analiziraju dokaze bez pristrasnosti ili modifikacije.[9]

Digitalna forenzika uključuje očuvanje, prikupljanje, potvrđivanje, identifikovanje, analizu, snimanje i predstavljanje informacija kriminalne scene.[10]

Kako je svet forenzike u informacionom ambijentu relativno nov, ali svet koji se razvija, za posledicu ima činjenicu da pojedini termini bivaju definisani i redefinisani. Upravo zbog toga, u upotrebi su, pored navedenih (računarska i digitalna

5 K. Cardwell & team /2007/: *The Best Damn Cybercrime and Digital Forensics*, Syngress Publishing, p. 3.

6 M. Reith, C. Carr, G. Gunsch /2002/: *An Examination of Digital Forensic Models*, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3, p. 2; K. Cardwell & team*: op. cit,* pp. 6–7.

7 M. Reith, C. Carr, G. Gunsch: *op. cit.* p. 2.

8 M. Reith, C. Carr, G. Gunsch, *ibid*. p. 3.

9 M. Reith, C. Carr, G. Gunsch, *ibid*, p. 3.

10 K. Cardwell & team *op. cit.* p. 7; D. R. Kamble, N. Jain /2015/, *Digital Forensic Tools: A Comparative Approach,* International Journal of Advance Research in Science and Engineering, Vol. 4, No. 2.

forenzika) i drugi termini, kao što su: elektronska forenzika ili e-forenzika, koja se ređe upotrebljava i kiber-forenzika, čija upotreba u praksi raste.[11]

Svi su relevantni, svaki relativno znači istu stvar, i u zavisnosti sa kim se razgovara, svaki naziv ima drugačiji smisao, ali nijedan se još nije pojavio *de facto* kao standard. Međutim, kako ova profesija, odnosno nauka, nastavlja da se razvija sigurno će dovesti do standardizacije termina. U ovom radu, od pomenutih termina biće korišćen termin *digitalna forenzika* koji je korišćen i u nazivu rada.

4. DIGITALNA FOTOGRAFIJA

Prošlo je skoro 100 godina od kada je fotografija počela da se koristi kao vizuelni zapis događaja, ljudi i mesta. Tokom godina skroman početak se razvio u tehnološku revoluciju u fotografskoj tehnologiji – digitalnu sliku. Danas digitalna slika predstavlja sastavni deo modernog života. Štaviše društvo je počelo da razume događaje kojim je okruženo na vizuelan način više nego ikada. Kao rezultat toga, digitalni mediji uopšteno ili digitalna slika kao deo su postali primarni izvor za vesti, zabavu i informaciju. Takođe mogu se koristiti kao delovi medicinskih dosijea, finansijskih dokumenata, ali i kao dokaz na sudu, sve u zavisnosti od vrste digitalnog medija. Ipak pored brojnih koristi koje nam donose digitalni mediji su sa sobom doneli mnoga nova pitanja i izazove koja su pre bila ili ne tako očigledna ili uopšte nisu ni postojala. Danas, više nego ikada, ljudi su shvatili da ne mogu uvek i tek tako da prihvate fotografiju samo kao neku vrednost odštampanu na papiru. Često se dešava da slika sadrži mnogo više nego što naše oko može da primeti. Moramo biti svesni da ono što vidimo nije uvek isto kao ono u šta verujemo.[12]

Fotografija je svoju nevinost izgubila pre mnogo godina. Samo nekoliko decenija nakon što je snimljena prva fotografija 1814. godine, nad fotografijama su vršene raznorazne manipulacije. Poslednjih godina, falsifikovanje slika ima značajan uticaj na nauku, pravo, politiku, medije i biznis, čak neki slučajevi falsifikovanja mogu dovesti do nacionalnih i međunarodnih problema. I dok problem falsifikovanja nije nov, tehnologije kojima se ono vrši su sve naprednije. Zahvaljujući digitalnim kamerama visoke rezolucije, moćnim računarima kao i sofisticiranim softverima za obradu slike, manipulacije na slici su postale prostije i teže uočljivije. Sa druge strane aparati za detektovanje manipulacija nad slikom su tek na početku svoga razvoja. Međutim, danas postoji jasna potreba za njima kako bi se povratilo opšte poverenje u digitalnu fotografiju.[13]

---

11 A. J. Marcella, D. Menendez /2008/, *CYBER FORENSICS – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach Publications, 2nd ed, pp. 4–5.

12 H. T. Sencar, M. Memon /2013/: *Digital Image Forensics*, Springer Science + Business Media New York, pp. v, vi.

13 B. Sarma, G. Nandi /2014/: *A Study on digital Image Forgery Detection,* International Journal of Advanced research in computer Science and Software Engineering, Volume 4, Issue 11, p. 878; H. Farid /2012/: Digital Image Forensics, http://www.cs.dartmouth.edu/farid/downloads/tutorials/digitalimageforensics.pdf, p. 4, 20.12.2016; P. Nampoothiri, N. Sugitha /2016/: *Digital Image Forgery – A threaten to Digital Forensics*, International Conference on Circuit, Power and

5. FALSIFIKOVANJE

Umetnost pravljenja falsifikovanih slika je, kao što je već napomenuto, stara koliko i sama fotografija. U svojim ranim godinama izrada fotografije je postala glavni metod za izradu portreta. Portret majstori su vrlo brzo shvatili da bi mogli da poboljšaju prodaju retuširanjem svojih fotografija. Fotografi su pored retuširanja počeli da koriste i tehnike za kombinovanje i spajanje više slika u jednu sliku. Jedan klasičan primer manipulacije nad fotografijom prikazan je na slikama 5.1. i 5.2, nastaloj 1865. godine, koju je snimio *Metju Brejdi*, čuveni fotograf, a kako se kasnije ispostavilo i majstor za manipulaciju nad fotografijom toga vremena. [14]

Slika 5.1.
Šerman sa francuskim oficirima, fotografija nakon manipulacije

Slika 5.2.
Šerman sa francuskim generalima, originalna fotografija

Na slici je prikazan general *Šerman* sa svojim oficirima. *Metju* je na originalnu fotografiju dodao još jednog francuskog oficira koji je imao značajnu ulogu u ratovima koje je Francuska tada vodila. Postoji još mnogo primera[15] iz ranijeg perioda koji se odnose na falsifikovanje fotografije, ono što im je zajedničko jeste da su manipulacije nad njima vršene uglavnom da bi se poboljšao kvalitet slike ili da bi se postigli efekti humora, odnosno nisu vršene radi prevare. Međutim sredinom dvadesetog veka, fotografi su otkrili da falsifikovanje slike može biti izuzetno moćno oružje kojim je moguće uticati na ljudsku percepciju, pa čak promeniti i istoriju. Tako je na primer nacistička Nemačka, koja je bila poznata po svojoj vrlo agresivnoj propagandi, često pribegavala falsifikovanju i manipulaciji slikom, kako bi držala stvari pod kontrolom.

U svim navedenim primerima, kao i u mnogim drugim, autentičnost fotografije je pitanje koje se stalno postavlja. Kako da se dokaže da su slike autentične ili kako da se dokaže da su slike modifikovane ili možda čak i računarski generisane? Kao rešenje se nameće digitalna forenzika.

Computing Technologies, p. 1; C. P. Bharti Tandel /2016/: *A Survey of Image Forgery Detection Techniques*, IEEE WiSPNET conference, p. 877.

14 H. Farid /2012/: *op. cit,* p. 4.

15 Photo Tampering Throughout History, http://www.cc.gatech.edu/~beki/cs4001/history.pdf, 10. 01.2017.

6. METODE MANIPULACIJA I FORENZIKA

Poslednjih godina mnogo se radilo na unapređenju tehnologija koje se koriste u forenzici slike. Pomoću tih tehnologija moguće je otkrivanje manipulacija koje su izvršene nad slikom bez obzira kojom kamerom je ona snimljena i pritom se ne oslanjajući na vodene žigove niti na neke specijalizovane hardvere. Za razliku od vodenog žiga, alati forenzike pretpostavljaju da svaka slika poseduje određene pravilnosti koje bivaju narušene ukoliko je nad njom izvršena određena manipulacija. Te pravilnosti mogu poticati iz različitih izvora, uključujući prirodno okruženje, kameru i naravno i samu sliku. Glavni zadatak svih alata vezanih za forenziku slike jeste merenje pravilnosti i detektovanje razlike između različitih merenja. Većina tehnika forenzike cilja tačno određene vrste manipulacija jer obično svaka od njih narušava samo neke pravilnosti koje slika poseduje. Ne postoji alatka koja je u stanju da otkrije sve moguće manipulacije izvršene nad slikom, ali većina postojećih alatki je u stanju da detektuje mnoge uobičajene manipulacije.[16]

Najosnovnije manipulacije slikom su *copy-move* ili metoda *kloniranja*. Ova vrsta manipulacije je neophodna ukoliko manipulator želi da prikrije deo slike i ona može biti izuzetno uspešna ukoliko je dostupno nešto homogenog sastava, kao što je na primer trava, pesak ili voda. Iako različite regije homogenog sastava mogu da perceptivno izgledaju kao da su sličnog kvaliteta, malo je verovatno da će to biti i numerički.[17]

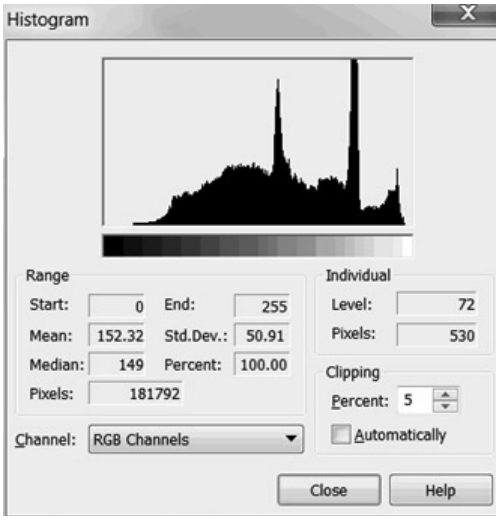
Za ilustraciju manipulacije slike metodom *copy-move* ili *kloniranjem* data su dva primera urađena u COREL Photo Paint X5. Takođe su prikazani i pripadajući histogrami na kojima su prikazane evidentne promene u odnosu na originale.

16 P. Nampoothiri, N. Sugitha: *op. cit*, p. 2; H. T. Sencar, N. Memon /2013/: *Digital Image Forensics*, Springer Science + Business Media New York, p. 257.

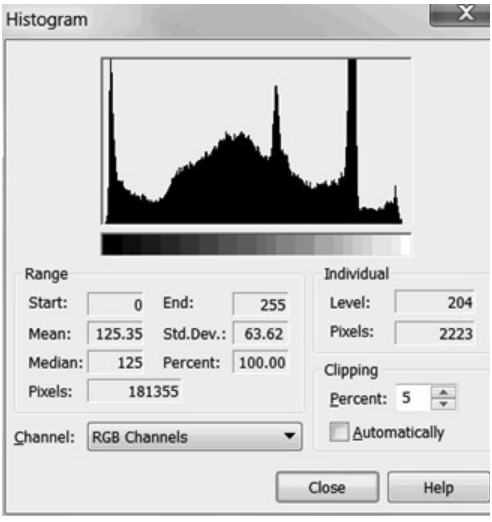
17 S. Mushtaq, A. H. Mir /2014/: *Digital Image Forgeries and Passive Image Authentication Techniques: A Survey*, International Journal of Advanced Science and Technology, Vol. 73, pp. 18–19; N. Parashar, N. Tiwari /2015/: *A Survey Of Digital Image Tempering Techniques*, International Journal of Signal Processing, Image Processing and Pattern Recognition, Volume 8, No. 10, p. 92; S. E. Thajeel, G. Sulong: /2014/, *A Survey of Copy-Move Forgery Detection Techniques*, Journal of Theoretical and Applied Information Security, Volume 70, No. 1, pp. 26–28; M. D. Ansari, P. S. Ghrera, V. Tyagi /2014/: *Pixel-Based Image Forgery Detection: A Reviw*, IETE Journal of Education, Volume 55, Issue 1, p. 42; S. Bayram, H. T. Sencar, N. Memon: *op. cit*, pp. 1–3; H. Farid /2009/: *Image forgery detection – A survey*, IEEE Signal Processing Magazine [16], p. 17.

Slika 6.1.
Uklonjen objekat

Slika 6.2.
Originalna slika



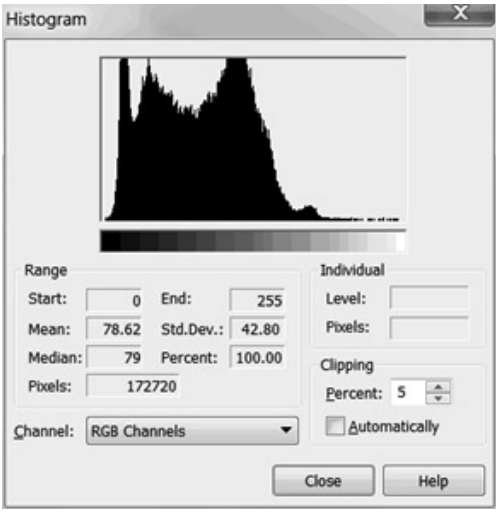
Slika 6.3.
Histogram obrađene slike



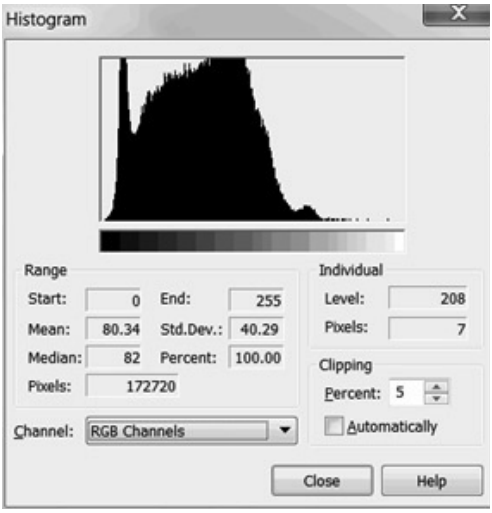
Slika 6.4.
Histogram originalne slike

Slika 6.5.
Kloniran objekat

Slika 6.6.
Originalna slika



Slika 6.7.
Histogram obrađene slike



Slika 6.8.
Histogram originalne slike

Druga osnovna manipulacija slikom jeste *spajanje* (splicing), tačnije fotomontaža. Za ovu vrstu manipulacije, manipulator kombinuje delove ili regije dve različite slike u jednu sliku. Jedna od tehnika za detekciju spajanja funkcioniše tako što traži nagle diskontinuitete u slici. Neke druge tehnologije se zasnivaju na proceni funkcije odziva kamere sa različitih regija slike.[18]

Ne tako retko, manipulator je prinuđen da *menja veličinu* slike ili da *rotira* određene delove u okviru nje. Ova vrsta manipulacije uglavnom podrazumeva resempling tehniku. Ovaj proces uvodi statističku korelaciju, koju je moguće detektovati pod određenim uslovima. Dodatno, ako je potrebno da manipulator sačuva sliku kao JPEG i ako je originalna slika uslikana kao JPEG format, rezultujuća slika će biti dva puta JPEG komprimovana (Double JPEG). Dva puta JPEG komprimovana slika takođe uvodi statističku korelaciju koja može da se detektuje forenzičkim tehnikama.[19]

Takođe *senzor digitalne kamere* se može koristiti za otkrivanje određenih manipulacija na slici. Tipični senzori prihvataju samo jedan od tri kanala boje za svaki piksel. Da bi se formirala RGB vrednost svakog piksela, nedostajući kanali boje se dobijaju interpolacijom sa susednih piksela koristeći CFA interpolacioni algoritam (demosaicing). Ovim algoritmom se znači vrši rekonstrukcija slike u boji na osnovu nekompletnih odbiraka boje koji se dobijaju sa senzora slike koji je obložen mrežom filtera boja (color filter array, CFA). I ovaj algoritam kao i resempling tehnika i dupli JPEG uvodi statističku korelaciju koja se može detektovati. Takođe *šum* koji nastaje u digitalnim senzorima može biti vrlo koristan za forenziku. Ovaj šum na neki način predstavlja digitalni otisak svake kamere, znači nešto po čemu se kamere međusobno razlikuju i na osnovu čega je moguće utvrditi koja grupa fotografija je slikana na primer istom kamerom. Jednom kada se izvrši procena šuma on se na dalje može koristiti za identifikaciju kamere kao i za otkrivanje manipulacije.[20]

Na kraju, *geometrijske tehnike* takođe mogu biti korisne za forenziku slike. Kada su na sceni prisutni poznati geometrijski oblici kao što su linije, krugovi i slično, oni se mogu koristiti za različita merenja, kao što je na primer merenje visine čoveka na osnovu poznate visine nekog objekta ili merenje razdaljine između objekta u istoj ravni.[21]

Većina sadašnjih forenzičkih tehnika se bazira na pravilnosti izvora koji su digitalni. Međutim sam proces snimanja uvodi i pravilnosti iz nedigitalnih izvora kao što su samo okruženje u kojem živimo i sočivo kamere, što znači da se i oni mogu koristiti u digitalnoj forenzici ukoliko im se te pravilnosti naruše usled određenih

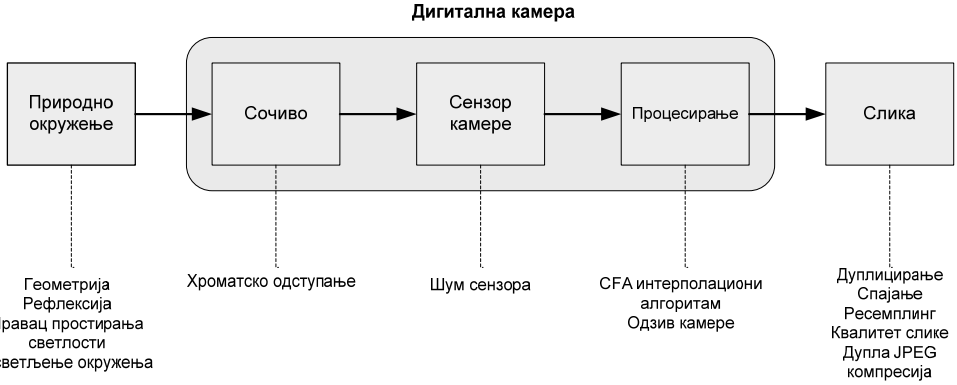
18 N. Parashar, N. Tiwari: *op. cit*, p. 92; S. A. Thajeel, G. Sulong G: *op. cit*, p. 26; M. D. Ansari, S. P. Ghrera, V. Tyagi /2014/: *Pixel-Based Image Forgery Detection: A Reviw,* IETE Journal of Education, Volume 55, Issue 1 pp. 40–43; H. Farid /2009/: *op. cit*, p. 17.

19 V. N, Bharti, P. Tandel /2016/: *A Survey of Image Forgery Detection Techniques*, IEEE WiSPNET conference, pp. 878–879; M. D. Ansari, S. P. Ghrera, V. Tyagi: *op. cit*, pp. 40–43; H. Farid /2009/: *op. cit*, pp. 18–19.

20 H. T. Sencar, N. Memon /2013/: *Digital Image Forensics*, Springer Science + Business Media New York, pp. 179–219; M. D. Ansari, S. P. Ghrer, V. Tyagi*: op. cit*, pp. 40–43; H. Farid /2009/: *op. cit*, pp. 19–21.

21 M. D. Ansari, S. P. Ghrera, V. Tyagi: *op. cit*, pp. 40–43; H. Farid /2009/: *op. cit*, pp. 23–24.

modifikacija. Uglavnom, danas postoji značajan broj forenzičkih tehnika za detekciju različitih vrsta modifikacija izvršenih na slikama. Tehnike koje se koriste u forenzici slike moguće je podeliti na osnovu toga šta je predmet njihove obrade. Pa tako imamo forenziku koja se zasniva na formatu slike, forenziku koja se zasniva na vrsti kamere koja se koristi, zatim forenziku koja se odnosi na piksele kao i forenzike koje se zasnivaju na statistici, geometriji i fizici.[22]



Slika 6.9.
Izvori pravilnosti u procesiranju slike i sadašnje tehnike forenzike koje koriste te pravilnosti[23]

Sa druge strane na osnovu toga da li forenzičar ima pristup komponentama procesa generisanja slika ili samo njihovim odgovarajućim ulaznim i izlaznim signalima, forenzičke metode se mogu podeliti i na pasivne i aktivne.[24]

Forenzika digitalne slike se smatra aktivnom ako je omogućeno namerno modifikovanje samog procesa generisanja slike u nekoj ranijoj fazi, sa ciljem da se u slici postave specifični identifikacioni tragovi. Ove dodatne informacije kada se vežu jednom za sliku uspostavljaju vezu sa poreklom slike čime garantuju njenu autentičnost. Tipični primer za podatke koji se umeću u sliku su kriptovani potpis ili digitalni vodeni žig. Identifikacioni tragovi koji se ugrađuju u sliku su dizajnirani tako da ukazuju na originalno poreklo slike ili su osetljivi na određene operacije u slici pa se pod njihovim uticajem menjaju.[25]

---

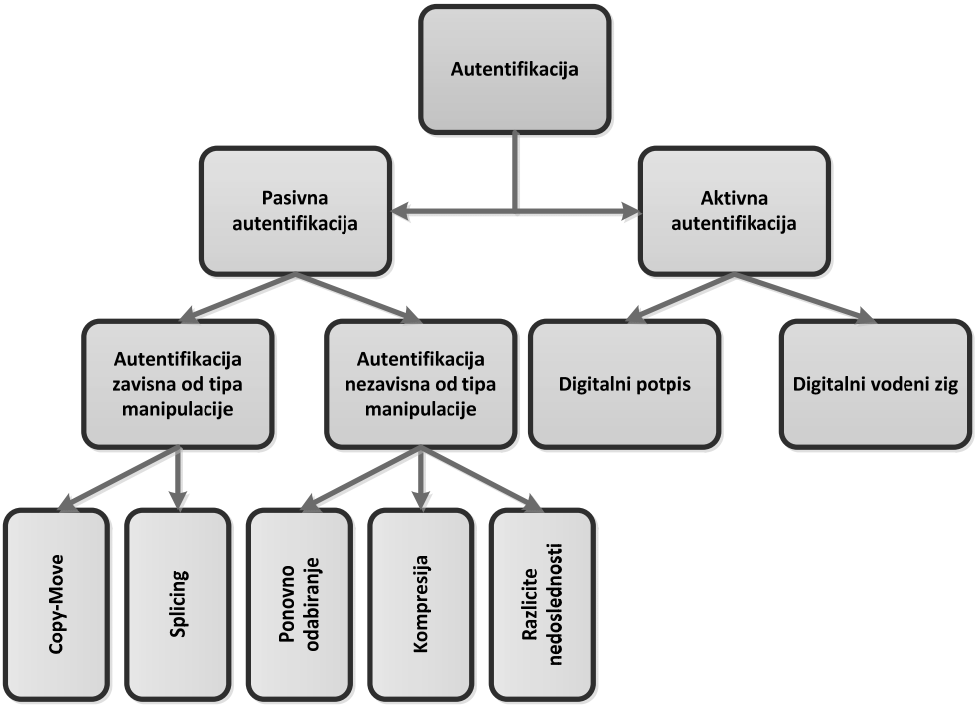
22 P. Nampoothiri, N. Sugitha: *op. cit*, pp. 4–5; N. Singhal, G. Gandhani /2015/: *Analysis of Copy-Move Forgery Image Forensics: A Review*, International Journal of Signal Processing and Pattern Recognition, Vol. 8, No. 7, pp. 266–267; H. Farid /2009/: *op. cit*, p. 16.

23 H. T. Sencar, N. Memon: *op. cit*, p. 258.

24 M. Kirchner /2011/: *Notes on Digital Image Forensics and Counter-Forensic*, The Department of Computer Science, TU Dresden, Germany, pp. 13–16; V. N, Bharti, P. Tandel: *op.cit*, p. 877; O. M. Al-Qershi, B. E. Khoo /2013/: *Passive detection of copy-move forgery in digital images: State-of-the-art,* Forensic Science International Elsevier, Ireland, p. 285.

25 N. Singhal, G. Gandhani: *op. cit*, pp. 265–266; N. Parashar, N. Tiwari: *op. cit*, pp. 92–93; S. Mushtaq, A. H. Mir: *op. cit*, pp. 16–17. M. Kirchner: *op. cit*, pp. 13–14; O. M. Al-Qershi, E. B. Khoo: *op. cit,* 285.

Sa druge strane forenzika digitalne slike se smatra pasivnom u slučaju da se forenzičar ne može umešati u sam proces generisanja slike i da na taj način kontroliše tip i prisustvo određenih identifikacionih tragova. Zato se identifikacija tragova u pasivnoj forenzici svodi na ispitivanje karakteristika uređaja, najčešće otiska kamere koji predstavlja trag nastao akvizicijom slike, i artefakta koja nastaju samim procesiranjem jer i ona mogu da variraju u karakteristikama tragova koje ostavljaju u slici, a koja se mogu iskoristiti kako bi se utvrdio tip obrade, odnosno proces koji je korišćen. Pasivne tehnike se takođe mogu podeliti na one koje su nezavisne od tipa manipulacije koja je izvršena i koje se oslanjaju na tri različite vrste artefakta kao što su tragovi ponovnog odabiranja, kompresija i razne nedoslednosti, kao i na one koje su formirane da bi otkrile tačno određenu manipulaciju nad slikom. U ovu grupu spadaju splicing i copy-move tehnike detekcije.[26]



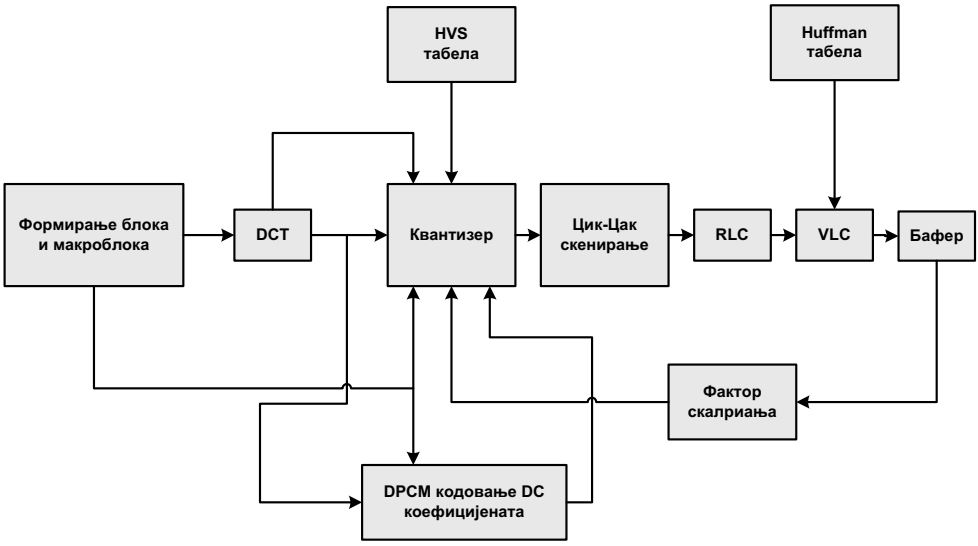
Slika 6.10.
Klasifikacija metoda autentifikacije slike[27]

26 N. Singhal, G. Gandhani: *op. cit,* p. 266; N. Parashar, N. Tiwari: *op. cit*, p. 92; S. Mushtaq, M. H. Mir*: op. cit*, p. 17; O. M. Al-Qershi, B. E. Khoo: *op. cit*, p. 285.

27 S. Mushtaq, A. H. Mir: *op. cit*, p. 16.

7. FORENZIKA ZASNOVANA NA FORMATU SLIKE

Da bismo mogli da objasnimo forenzičku tehniku kao što je na primer dupla JPEG kompresija (Double JPEG), moramo dobro da razumemo samu JPEG kompresiju. Razlikujemo dve vrste kompresije. *Kompresija bez gubitaka* koja se zasniva na tome da su unapred poznate osobine izvora koji emituje informaciju u stvari suvišna informacija, takozvana redundansa. *Kompresija sa gubicima* koja pored toga što se zasniva na uklanjanju redudanse zasniva se još i na tome da ljudska čula ne mogu percipirati određena odstupanja primljenog od originalnog signala.[28]



Slika 7.1.
Blok šema intrafrejm kodovanja[29]

JPEG (Joint Photographic Expert Group) predstavlja standard za kompresiju koji je nastao 1993. godine. Ovom kompresijom se dobijaju takozvane intrakodovane slike, što znači da je sama kompresija izvršena unutar jedne slike. Intrafrejm kodovanje se zasniva na prostornoj, statističkoj i subjektivnoj redudansi. *Prostorna redudansa* se bazira na tome da je mala verovatnoća da će se dva susedna piksela razlikovati u sjajnosti. *Statistička redudansa* se zasniva na tome da se simboli koji se češće pojavljuju koduju sa kraćom kodnom reči. *Subjektivna redudansa*, koja za razliku od prethodne dve podrazumeva kompresiju sa gubicima, zasniva se na osobinama ljudskog psihovizuelnog i psihoakustičkog sistema. Kompresija mirne slike zasniva se na hibridnoj metodi, radi se u transformacionom i osnovnom domenu. Može se opisati u nekoliko koraka: [30]

28 I. Reljin, A. Gavrovska /2013/: *Telemedicina*, Akademska misao Beograd, pp. 31–38.

29 I. Reljin, A. Gavrovska: *ibid*, p. 42.

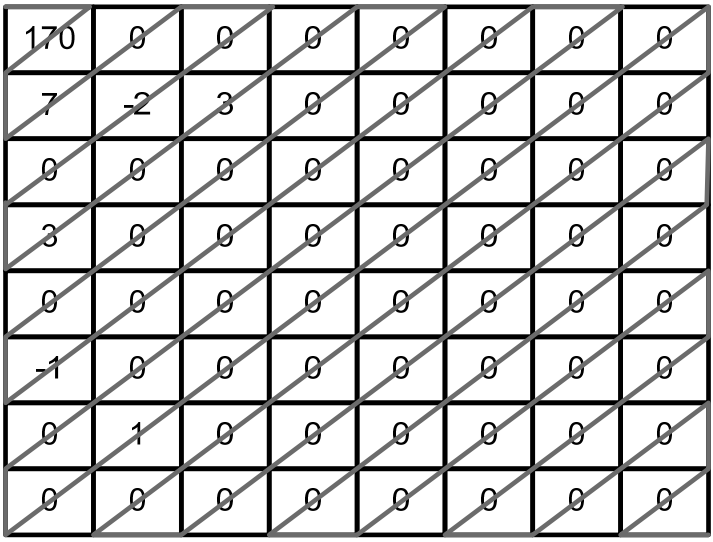
30 I. Reljin, A. Gavrovska: *ibid*, pp. 32–49.

1. *Dekompozicija slike u blokove*. Slika se deli u blokove 8x8 piksela. Svaki blok je označen sa 64 broja vrednosti od 0 do 255 (kada se vrši digitalizacija sa 8 bita) za luminentni signal i –128 do 127 za hrominentni signal.
2. *Diskretna kosinusna transformacija (DCT)* se primenjuje na date blokove. Njene osnovne karakteristike su visok stepen pakovanja energije, kao i raspoloživi brzi algoritmi za njeno izračunavanje. Svojstvo pakovanja energije ima za posledicu da samo nekoliko DCT koeficijenata ima značajne vrednosti. Sitniji detalji na slici predstavljaju visoke frekvencije i koduju se grubom kvantizacijom, dok se krupniji detalji koduju finijom kvantizacijom. Koristi se dvodimenzionalno transformaciono kodovanje pri čemu se prelazi u domen prostornih frekvencija. Koeficijent X(0,0) predstavlja jednosmernu komponentu slike, dok su ostali koeficijenti naizmenične komponente. Rezultat transformacije je opet matrica 8x8 piksela ali u frekvencijskom domenu. Znači prvi koeficijent prve vrste je koeficijent jednosmerne komponente. Drugi koeficijent odgovara energiji najkrupnije strukture u horizontalnom pravcu, dok poslednji koeficijent u prvoj vrsti odgovara energiji najfinije strukture slike u horizontalnom pravcu. DCT slike dimenzije NxN, čija je funkcija osvetljaja *x(k,l),* gde su *k,l* koordinate odgovarajućeg piksela na posmatranoj slici, data je sledećim relacijama:

$$X(0,0) = \frac{1}{N}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} x(k,l) \tag{1}$$

$$X(u,v) = \frac{2}{N}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} x(k,l)\cos\left[\frac{(2k+1)u\pi}{2N}\right]\cos\left[\frac{(2l+1)v\pi}{2N}\right] \tag{2}$$

3. *Tresholding i kvantizacija.* Pošto oko ne razlikuje fine detalje luminanse ispod neke vrednosti, male vrednosti DCT koeficijenata zamenjujemo nulom, a ostale kvantizujemo. Te nule su uglavnom na najvišim frekvencijama. Proces kvantizacije predstavlja proces diskretizacije signala, tačnije njegovih odbiraka, po amplitudi.
4. *Cik-cak skeniranjem* se vrši očitavanje vrednosti iz DCT matrice, pri čemu se vrši transformacija dvodimenzionalne matrice u tok podataka. Cik-Cak skeniranjem se brzo „istroše“ niske frekvencije, a ostaju visoke, gde po pravilu očekujemo veliki broj nula. Nizovi nula su sada duži ali ih je znatno manje za razliku od linijskog skeniranja kod kojeg se očitava red po red pa su nizovi nula kraći, ali ih zato ima mnogo.



Slika 7.2.
Cik-cak skeniranje[31]

5. *Run Lenght Coding (RLC)* definiše sekvence za početak i kraj ponovljene vrednosti. Koduju se samo vrednosti različite od nule, zajedno sa brojem nula.
6. *Variable Lenght Coding (VLC)* je poznato kao Hafmanovo ili entropijsko kodovanje. Osnovni princip Hafmanovog kodovanja je dodeljivanje kodnih reči promenljive dužine simbolima iz posmatranog skupa simbola. Na taj način se dobija kod sa minimalnom redundansom. Prosečan broj bita, za kodovanje svakog od simbola je minimalan. Hafmanov algoritam se sastoji od sledećih koraka:
   - skup simbola se uredi po nerastućim vrednostima apriori verovatnoća pojavljivanja;
   - udruže se dva simbola, sa najmanjim vrednostima apriori verovatnoća, u novi simbol čija je apriori verovatnoća jednaka zbiru njihovih apriori verovatnoća;
   - preuredi se skup novih simbola po nerastućim vrednostima apriori verovatnoća;
   - ponovi se proces udruživanja simbola sa najmanjim apriornim verovatnoćama
   - formira se novi simbol čija je apriori verovatnoća jednaka zbiru njihovih apriori verovatnoća;
   - postupak se ponavlja sve dok se ne dobije jedan simbol čija je apriori verovatnoća jednaka jedan;

31 I. Reljin, A. Gavrovska: *ibid*, p. 41.

- u procesu udruživanja, binarni simbol „0“ se dodeljuje gornjem simbolu, a binarni simbol „1“ donjem simbolu;
- kodna reč svakog simbola formira se kao niz dodeljenih binarnih simbola, počevši od simbola čija je apriori verovatnoća jednaka jedan.

Svaka manipulacija nad slikom zahteva, u najmanju ruku, otvaranje slike u programu za obradu slika, a zatim i njeno čuvanje nakon izvršene obrade. Kako se danas većina slika čuva u JPEG formatu, velika je verovatnoća da će modifikovana slika, kao i originalna slika biti sačuvana u tom formatu, što praktično znači da se modifikovana slika dva puta komprimuje. Kako je JPEG format zasnovan na kompresiji sa gubicima, ovo dvostruko komprimovanje (*Double JPEG*) uvodi specifične efekte (artefakta) koji ne postoje u jednostruko komprimovanim slikama. Prisutnost tih efekata može se koristiti kao dokaz određene vrste manipulacija. Međutim mora se uzeti u obzir da dvostruka JPEG kompresija ne mora nužno značiti maliciozno menjanje slike. Tako na primer moguće je nenamerno sačuvati sliku nakon njenog pregleda.[32]

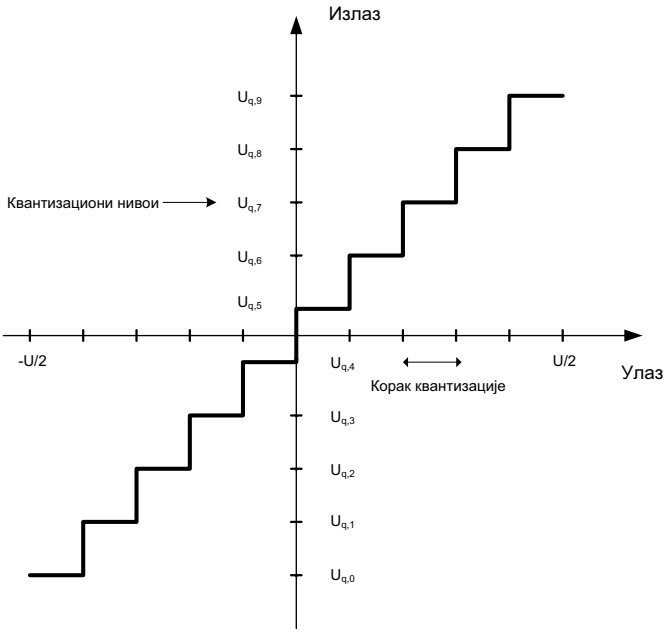
Kao što je ranije objašnjeno kodovanje JPEG slike podrazumeva tri osnovna koraka: DCT, kvantizaciju i entropijsko kodovanje. Dekodovanje komprimovanog toka podataka podrazumeva tri inverzna procesa i to obrnutim redosledom: entropijsko dekodovanje, dekvantizacija i inverzna DCT. Posmatrajmo na primer diskretan jednodimenzionalan signal f(x). Proces kvantizacije se može opisati pomoću funkcije: [33]

$$q_a(u) = \left\lfloor \frac{u}{a} \right\rfloor \tag{3}$$

gde je a korak kvantizacije, dok *u* označava vrednost iz opsega gore pomenute f(x) funkcije.

32 J. Yang, J. Xie, G. Zhu, S. Kwong, Q. Y. Shi: /2014/, *An effective Method for Detecting Double JPEG Compression With the Same Quantization Matrix,* IEEE Transactions on Information Forensics and Security, Vol. 9, No. 11, pp. 1933,1934; H. Farid /2009/: *op. cit*, pp. 18–19; H. Farid /2012/: *op. cit*, pp. 15–24;

33 J. Yang, J. Xie, G. Zhu, S. Kwong, Q. Y. Shi: *op. cit*, pp. 1933–1934; H. Farid /2009/: *op. cit*, 18–19; H. Farid /2012/: *op. cit*, pp. 15–24.



Slika 7.3.
Opšti oblik karakteristike ravnomerne kvantizacije[34]

Dekvantizacija vraća kvantizirane vrednosti u njihove prave vrednosti.

$$q_a^{-1}(u) = a * u \tag{4}$$

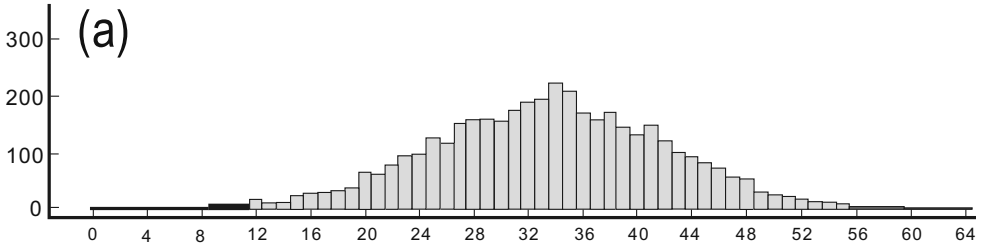
Ono što je važno napomenuti jeste da dekvantizacija nije inverzan proces kvantizacije. Dvostruka kvantizacija je opisana pomoću dva parametra *a* i *b* i oba predstavljaju korak kvantizacije.

$$q_{ab}(u) = \left\lfloor \left\lfloor \frac{u}{b} \right\rfloor \frac{b}{a} \right\rfloor \tag{5}$$

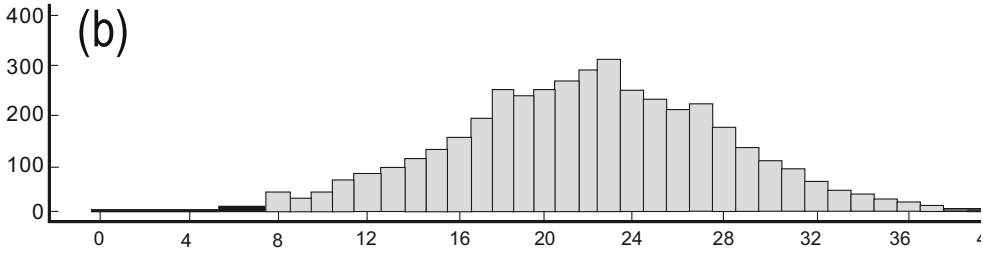
Treba primetiti da se dvostruka kvantizacija sastoji iz tri koraka: kvantizacija sa korakom b koja je praćena dekvantizacijom sa korakom b koja je praćena kvantizacijom sa korakom a. Razmotrićemo primer u kom su odbirci pomenutog signala f(x) ravnomerno raspodeljeni u opsegu [0,127]. Da bismo pokazali prirodu posledica dvostruke kvantizacije, kvantiziraćemo signal f(x) na četiri različita načina i rezultate prikazati odgovarajućim histogramima. Na slici 7.4. redom su prikazani histogrami signala nad kojim je izvršena jednostruka kvantizacija (histogrami (a) i (b)) samo sa različitim koracima i tog istog signala nad kojim je izvršena dvostruka kvantizacija i to kvantizacija sa korakom tri praćenim kvantizacijom sa korakom dva i obrnuto. Kada se korak kvantizacije smanjuje neki diskretni intervali histo-

34 M. L. Dukić /2008/: *Principi telekomunikacija*, Akademska misao, Beograd, p. 287.

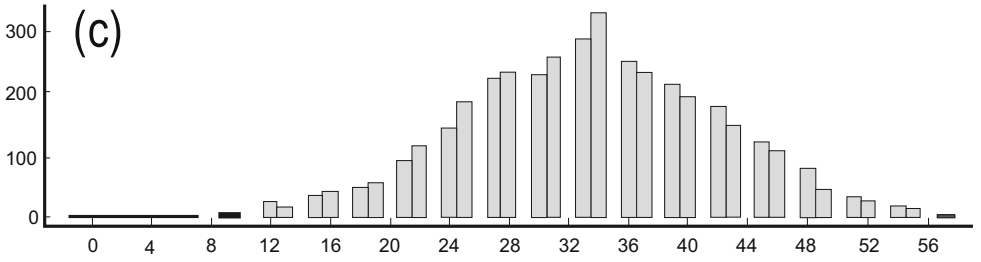
grama su prazni, dok u slučaju porasta koraka kvantizacije neki diskretni intervali histograma sadrže više odbiraka nego njihovi susedi. Ono što takođe treba primetiti u oba slučaja dvostruke kvantizacije jeste periodičnost posledica koje su predstavljene datim histogramima i upravo ta periodičnost se koristi za otkrivanje dvostruke JPEG kompresije. Kao što se može primetiti, ova tehnika nam omogućava da utvrdimo da li je JPEG slika bila podvrgnuta dvostrukoj kompresiji, dok nam neke druge tehnike kao što je na primer JPEG Ghost omogućavaju da utvrdimo u kom delu slike je izvršena dvostruka konverzija.[35]



Slika 7.4.
Histogram jednostruke kvantizacije sa korakom 2

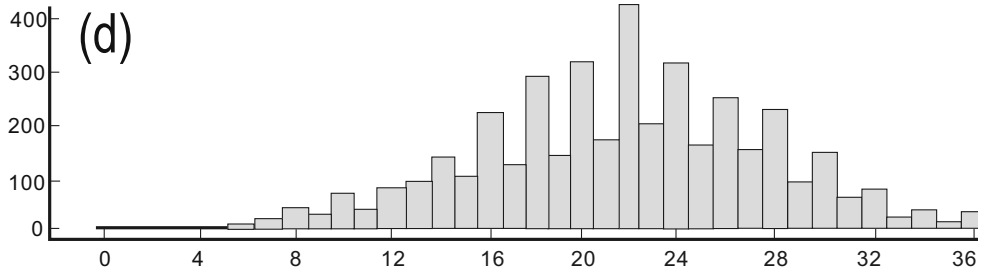


Slika 7.5.
Histogram jednostruke kvantizacije sa korakom 3



Slika 7.6.
Histogram dvostruke kvantizacije sa korakom 3 praćeno sa korakom 2

35 H. Farid /2009/: *op. cit*, pp. 18–19; H. Farid /2012/: *op. cit*, 15–24; J. A. Redi & W. Taktak & J. Dugelay /2011/: *Digital image forensics a booklet for beginners*, Multimed Tools Appl (2011) 51:133–162, pp. 150–152.



Slika 7.7.
Histogram dvostruke kvantizacije sa korakom 2 praćeno sa korakom 3

8. ZAKLJUČAK

Nesporno je da živimo u dobu u kojem se svakodnevno na razne načine i u raznim situacijama susrećemo sa vrlo obimnom količinom podataka multimedijalnog sadržaja. Razlog tome je činjenica da je multimedija postala glavno područje istraživanja, rada i razvoja. Nažalost, multimedijom, a to znači i digitalnom slikom o kojoj je ovde reč, zahvaljujući vrlo snažnim softverskim alatima, što potvrđuju i izloženi primeri, može se vrlo uspešno manipulisati sa posledicama u lepezi od trivijalnih do vrlo ozbiljnih, a da otkrivanje i dokazivanje tih zloupotreba zahteva vrlo uska i visoko specijalizovana znanja i veštine. Ove konstatacije naglašeno ukazuju na potrebu da se u značajnoj meri ojačavaju i uvećavaju pravne i profesionalne mogućnosti za uspešno suprotstavljanje ovoj velikoj društvenoj pretnji. Značajnu ulogu u tome bi svakako trebalo da ima i nauka. Iz tih razloga, a imajući u vidu činjenicu da je klasična forenzika postala primitivna u informacionim uslovima, svi društveni faktori, koji su odgovorni za stanje u ovoj oblasti, trebalo bi da fokus svog delovanja usmere na intenzivno školovanje i obuku kadrova koji će biti u stanju da uspešno odgovore svim izazovima novog informacionog doba.

LITERATURA

Al-Qershi M. O, Khoo E. B, *Passive detection of copy-move forgery in digital images: State-of-the-art,* Forensic Science International 231, 284–295, Elsevier, Ireland 2013.

Ansari D. M, Ghrera P. S, Tyagi V, *Pixel-Based Image Forgery Detection: A Reviw,* IETE Journal of Education, Volume 55, Issue 1, November 2014.

Bayram S, Sencar T. H, Memon N, *A survey of copy-move forgery detection techniques*, IEEE Western New York Image Processing Workshop, September 2008.

Bergslien E, *Chapter 1, A Brief History of Forensic Science and Crime Scene Basics*, from *An Introduction to Forensic Geoscience*, First Edition, Published 2012 by Blackwell Publishing Ltd, http://media.wiley.com/product_data/excerpt/56/11182279/1118227956–16.pdf

Cardwell K. & team, *The Best Damn Cybercrime and Digital Forensics*, Syngress Publishing, 2007.

Bharti N. C, Tandel P, *A Survey of Image Forgery Detection Techniques*, IEEE WiSPNET conference, 2016.

Dukić L. M, *Principi telekomunikacija*, Akademska misao, Beograd, 2008.

Farid H, *Digital Image Forensics*, http://www.cs.dartmouth.edu/farid/downloads/tutorials/digitalimageforensics.pdf, 20.12.2016.

Farid H, *Image forgery detection – A survey*, IEEE Signal Processing Magazine [16] March 2009.

Forensic Analysis, Encyclopedia of Polymer Science and Technology, http://docs4.chomikuj.pl/333787021,PL,0,1,Forensic-Analysis.pdf, 15.12.2015.

Forensic, http://en.wikipedia.org/wiki/Forensic, 15.12.2016.

Judith A. Redi & Wiem Taktak & Jean-Luc Dugelay, *Digital image forensics a booklet for beginners*, Multimed Tools Appl (2011) 51:133–162

Kamble R. D, Nilakshi Jain, *Digital Forensic Tools: A Comparative Approach,* International Journal of Advance Research in Science and Engineering, Vol. 4, No. 2, February 2015.

Kirchner M, *Notes on Digital Image Forensics and Counter-Forensic*, The Department of Computer Science, TU Dresden, Germany, 2011.

Marcella J. M, Menendez D, *CYBER FORENSICS – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach Publications, Second Edition, 2008.

Mushtaq S, Mir H. M, *Digital Image Forgeries and Passive Image Authentication Techniques: A Survey,* International Journal of Advanced Science and Technology, Vol. 73, 2014.

Nardoni D, So C, *Introduction to Computer Forensics*, 2005, http://www-scf.usc.edu/~itp499cf/Lectures/USC.Introduction.to.Computer.Forensics.Day.1.pdf

Nampoothiri P, Sugitha N, *Digital Image Forgery – A threaten to Digital Forensics*, International Conference on Circuit, Power and Computing Technologies, 2016.

Parashar N, Tiwari N, *A Survey Of Digital Image Tempering Techniques,* International Journal of Signal Processing, Image Processing and Pattern Recognition, Volume 8, No. 10, 2015.

Photo Tampering Throughout History, http://www.cc.gatech.edu/~beki/cs4001/history.pdf, 10.01.2017.

Reith M, Carr C, Gunsch G, *An Examination of Digital Forensic Models*, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3.

Reljin I, Gavrovska A, *Telemedicina*, Akademska misao Beograd, 2013.

Sarma B, Nandi G, *A Study on digital Image Forgery Detection,* International Journal of Advanced research in computer Science and Software Engineering, Volume 4, Issue 11, November 2014

Sencar T. H, Memon N, *Digital Image Forensics*, Springer Science + Business Media New York 2013

Singhal N, Gandhani G, *Analysis of Copy-Move Forgery Image Forensics: A Review*, International Journal of Signal Processing and Pattern Recognition, Vol. 8, No. 7, 2015.

Thajeel A. T, Sulong G, *A Survey of Copy-Move Forgery Detection Techniques,* Journal of Theoretical and Applied Information Security, Volume 70, No. 1, December 2014.

Yang J, Xie J, Guopu Zhu, Sam Kwong, Yun-Qing Shi, *An effective Method for Detecting Double JPEG Compression With the Same Quantization Matrix,* IEEE Transactions on Information Forensics and Security, Vol. 9, No. 11, Novembar 2014.

Ranko Petrović
Vlatacom Institute, Belgrade

Irini Reljin
Faculty of Electrical Engineering

THE ROLE OF FORENSICS IN DIGITAL IMAGE FORGERY DETECTION

SUMMARY

Considering that the development of information technology has completely changed the way of accessing, processing and sharing of information, and that nowadays, thanks to the Internet, the vast amount of information is literally at our fingertips, negative consequences of this phenomenon increasingly come to the fore, especially when it comes to multimedia data. Thanks to the sophisticated softwares, it has become relatively easy to preform manipulation of the image, audio or video material in order to undermine their integrity and authenticity without leaving any trace that man can visually notice.

This paper analyses the current problem of manipulation of the digital image which role may be to hide, emphasize or to completely change some specific information in the image, with consequences ranged from trivial to catastrophic ones. Moreover, the focus of this paper is the role of digital forensics in detecting and proving performed manipulations.

Regarding to this, the paper briefly describes the most common manipulations that can be performed on the image, copy-move or cloning and splicing or photomontage. Copy-move manipulation is achieved by copying a specified region of the original image and pasting it to another part of the same image in order to conceal useful information, while splicing manipulation is achieved by combining parts of two different images into one, final image. This paper also presents concrete examples of copy-move manipulations done in Corel Photo Paint X5 program, as well as changes in the image histograms caused by the manipulation, which proves that the image has undergone some changes. However, every manipulation of the image leads to disrupting of certain regularities that each image owns and which originate from the natural environment, the camera and the image itself. It is exactly these regularities and their deviations that detection techniques are based on. Accordingly, we distinguish detection techniques based on statistics, geometry and physics, then detection techniques based on sensor and noise of the camera that is used, and lastly detection techniques based on the format and quality of the image, compression and so on.

The paper also discusses the active and passive approach of digital forensics in accordance with ability to modify the process of generating images itself by inserting specific identification marks such as watermark or digital signature. At the end, the process of forensic technique based on the image format, so-called double JPEG, is described. It is shown how the double compression, which is almost inevitable in the process of manipulation, introduces some specific effects that do not exist in the single compressed image.

The aim of this paper is to highlight the need and importance to preserve the identity and authenticity of digital images, as well as to point to the possibilities of manipulation of the image, and finally, if the manipulation has been performed, to reveal it and irrefutably prove it, and digital forensics certainly plays the main role in it.

Key words: digital image, forgery, double JPEG, digital forensics