SAVREMENA DOSTIGNUĆA U FORENZICI DIGITALNIH SLIKA

Andreja Samčović, Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *Poslednjih decenija svedoci smo razvoju informaciono-komunikacionih tehnologija, počev od komunikacione i mrežne infrastrukture, preko standardizacije multimedijalne kompresije i tehnika za kodovanje multimedijalnih signala, pa do efikasnog pretraživanja multimedijalnih sadržaja. Kao rezultat toga, multimedijalni sadržaji postaju univerzalno dostupni. Tehnološki razvoj je prirodno doveo do toga da sadržaji i uređaji budu korišćeni od autorizovanih korisnika koji na to imaju pravo, a da u suprotnim slučajevima postoji mogućnost forenzičkog dokazivanja sa visokom pouzdanošću. U slučaju da se sumnja u autentičnost multimedijalnih sadržaja, forenzičke metodologije i alati se koriste kako bi se obavila rekonstrukcija šta se dogodilo sa multimedijalnim sadržajem i odgovorilo ko ga je krivotvorio, kada, gde i kako. Cilj ovog rada je da pruži uvid u relativno novo područje forenzike digitalnih slika, uzimajući u obzir savremene teorije i metodologije.*

Ključne reči: *forenzika, fotografija, kompresija, multimedija, slika*

1. Uvod

Široka zastupljenost digitalnih sadržaja u odnosu na tradicionalne fizičke medije kao što su film, dovela je do brojnih izazova koji se odnose na bezbednost multimedijalnih informacija. Digitalni sadržaj može da se menja, falsifikuje i ponovo distribuira relativno jednostavno. Ta činjenica ima značajne posledice na državne, komercijalne i društvene organizacije koje koriste digitalne informacije. Sa ciljem obezbeđivanja komunikacione infrastrukture i prevencije neautorizovanog pristupa, brojne kriptografske tehnike i tehnike autentifikacije su razvijene poslednjih godina [1]. Sa jedne strane je uloženo dosta napora u razvoju tehnika za povećanje bezbednosti multimedijalnih informacija, dok se sa druge strane njihova zaštita završava kada se digitalni sadržaji isporuče i dekriptuju. To je problematično, pošto dalje skoro da nema kontrole kako se digitalne informacije koriste ili obrađuju nakon isporuke. Štaviše, navedene tehnike ne mogu da obezbede multimedijalne sadržaje da ne budu manipulisani ili falsifikovani pre nego što se kriptuju ili digitalno potpišu.

U značajnim situacijama iz realnog sveta digitalne informacije potiču iz nepoznatog ili nebezbednog izvora. Kada se to desi, potencijalni napadač može lakše da manipuliše nad digitalnim sadržajima kao što su slike ili video signali i na taj način može da formira perceptualno realistični sadržaj koji izgleda kao original. Kriptografske tehnike ne mogu

da obezbede da informacije koje se prenose ne budu podložne promenama u tim situacijama. Pre nego što poverujemo u autentičnost multimedijalnih informacija potrebno je odgovoriti na nekoliko pitanja, kao što je koje je pravo poreklo digitalnih sadržaja. Kako su obrađene multimedijalne informacije kojima pristupamo? Da li je taj sadržaj autentičan ili je došlo do neke manipulacije? Poredeći sa naporima koji se ulažu u obezbeđivanju bezbednog i poverljivog prenosa informacija, istraživački pristupi koji bi odgovorili na postavljena pitanja su još uvek relativno novi.

U odgovoru na povećane potrebe za verifikacijom verodostojnosti multimedijalnih sadržaja stvoreno je novo polje koje se naziva forenzika informacija [2]. Forenzika informacija se odnosi na određivanje autentičnosti, istorije obrade informacija, i poreklo digitalnih multimedijalnih sadržaja bez uticaja bočnih kanala različitih od posmatranih sadržaja. Forenzika informacija ima dalje za cilj da odredi ko je, kada, kako i šta uradio sa multimedijalnim sadržajima. Kada informacija dalje prolazi kroz različite uređaje i obrade postoje trase koje ostavljaju tragove pri svakom koraku obrade. Te trase se odnose na tkz. unutrašnje otiske (*intrinsic fingerprints*) koji su od esencijalnog značaja za forenzičku analizu. Postoje brojne forenzičke tehnike za identifikaciju manipulacija koje koriste nevidljive tragove koje ostavljaju multimedijalni sadržaji prilikom prikupljanja (akvizicije) i obrade [3].

Sa druge strane, postoje i spoljašnje bezbedonosne mere kao što su digitalni vodeni žigovi (*digital watermarking*) [4]. Digitalni žigovi se utiskuju u informacione sadržaje putem tehnika utiskivanja koje su uglavnom nevidljive za korisnike. Te trase se nazivaju spoljašnji otisci (*extrinsic fingerprints*). Rani radovi u vezi ovih tehnika iz kraja 90-ih godina su se uglavnom odnosili na utiskivanje informacija kako bi se zaštitila autorska prava ili verifikovali podaci o integritetu korisnika. Poslednja decenija je dovela do intenzivnih istraživanja na temu tradicionalnih tehnika robusnog votermarkinga sa ciljem utiskivanja tragova koji mogu da identifikuju pojedinačne kopije medijskih sadržaja. Drugi cilj ovih algoritama se odnosi na povezivanje kopije sa određenom jedinicom uređaja za akviziciju podataka.

Nakon uvodnog dela, u drugom poglavlju su predstavljene osnovne pretpostavke za forenziku digitalnih slika. Objašnjena je podela na pasivne i aktivne metode koje se koriste u forenzici slika, zavisno od toga da li je poznato poreklo slike. Zatim je obrađen ciklus slike, gde su od značaja za forenziku otisci koje ostavlja sa sobom digitalna slika. S tim u vezi, od značaja su akvizicija, kodovanje i editovanje otisaka. Naredna sekcija se bavi akvizicijom digitalne slike. Prilikom akvizicije slike treba uzeti u obzir tragove koji potiču od optičkih sočiva, senzora, kao i *Color Filter Array* (CFA). Kodovanje slike je objašnjeno u sledećem poglavlju, pre zaključnih razmatranja. Kod detekcije krivotvorenja naročito je važna dvostruka JPEG kompresija.

2. Forenzika slika

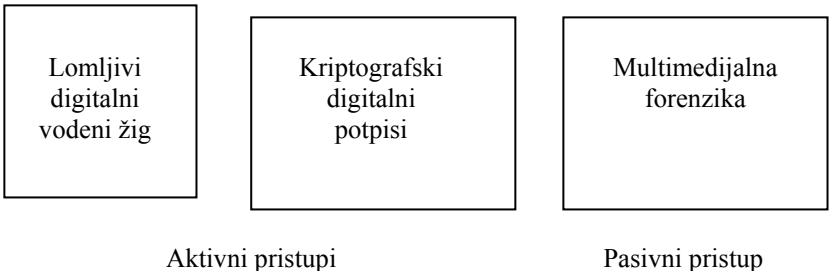
Slike, za razliku od teksta, predstavljaju efikasan i prirodan način komunikacije između ljudi, zahvaljujući jednostavnosti razumevanja sadržaja slike. Istorijski i tradicionalno, postojalo je verovanje u integritet vizuelnih podataka. S tim u vezi, prihvatana je verodostojnost slika objavljenih u novinama, koje su prihvatane kao dokaz istinitosti informacija. Takođe, snimci dobijeni video nadzorom uzimani su kao dokazni materijal na sudu.

Sa brzim širenjem i jednostavnim korišćenjem relativno jevtinih uređaja za akviziciju vizuelnih podataka, skoro svako danas ima mogućnost snimanja, memorisanja i razmene ogromnog broja digitalnih slika. U isto vreme, dostupnost softverskih alata za editovanje slika čini jednostavnim promenu sadržaja slika, ili kreiranje novih sadržaja, tako da mogućnost krivotvorenja vizuelnih sadržaja danas nije ograničena samo na eksperte na tom polju. Odgovarajući softverski alati omogućavaju formiranje fotorealistične računarske grafike tako da korisnici ne mogu da naprave jasnu razliku u odnosu na fotografske slike [5, 6].

Može se reći da danas digitalni vizuelni objekti prolaze u svom ciklusu, od akvizicije do korišćenja, kroz nekoliko stanja obrade, kreirajući pri tome nove sadržaje mešanjem sa prethodno postojećim materijalom, ili čak falsifikujući sadržaje. Kao rezultat toga digitalna tehnologija narušava verodostojnost vizuelnih sadržaja, tako da danas korisnici ne mogu slepo da veruju u ono što vide [7, 8]. Treba naglasiti da navedeni problemi mogu samo da budu složeniji kako alati za obradu slika budu sve više sofisticirani.

Navedeno stanje osvetljava potrebu za metodama koje omogućavaju rekonstrukciju istorije digitalnih slika u cilju verifikacije njihove verodostojnosti. Pri tome se mogu postaviti dva pitanja: da li je slika snimljena pomoću uređaja za koji se tvrdi da jeste? Da li se posmatrana slika odnosi na originalno snimljenu scenu? Odgovor na prvo pitanje je od interesa kada saznanje o izvoru slike predstavlja dokaz po sebi, odnosno da li omogućava saznanje da li je korisnik uređaja snimio posmatranu sliku. Odgovor na drugo pitanje je relativno lak kada je poznata originalna slika. U realnosti, međutim, skoro da nikada nema a priori informacija o originalnoj slici. Forenzičari, prema tome, treba da autentifikuju istoriju slike na slepi način.

Da bi odgovorila na postavljena pitanja istraživačka zajednica na polju bezbednosti multimedijalnih informacija je predložila nekoliko pristupa koji mogu da se klasifikuju na aktivne i pasivne tehnologije, kao što je pokazano na Slici 1. Pod aktivnim tehnologijama podrazumeva se istraživanje informacija generisanih na strani izvora prilikom akvizicije, npr. na kameri, dok se pod pasivnim tehnologijama podrazumeva da postoji pristup samo digitalnom sadržaju koji se razmatra, a ne i uređajima pomoću kojih je obavljena akvizicija.



Slika 1. Blok-šema koja pokazuje moguće pristupe istoriji i kredibilnosti digitalnih slika

Aktivni pristupi se zasnivaju na ideji verodostojnosti kamera [9, 10], koji je predložen u prošlosti kao način autentifikacije digitalnih slika. Kamere mogu da utisnu digitalni

vodeni žig [4] ili digitalni potpis [1] na slici prilikom akvizicije, i bilo koja kasnija modifikacija slike može da se detektuje proverom vrednosti digitalnog vodenog žiga ili digitalnog potpisa pri momentu realizacije. Glavni nedostatak aktivnih rešenja je što digitalne kamere treba da budu opremljene posebnim čipom za digitalni votermarking, ili čipom za digitalni potpis, koji koristi privatni ključ za autentifikaciju svake slike koju kamera snimi pre nego što se memoriše na memorijskoj kartici. Implementacija verodostojnih kamera bi zahtevala od proizvođača da definišu standardne protokole. To je zahtev koji je teško ispuniti, jer bi ograničio aplikacije u vrlo specifičnim situacijama.

Da bi se prevazišli navedeni problemi nedavno su uvedeni metodi za autentifikaciju sadržaja digitalnih slika, koji nemaju potrebu za prethodnim poznavanjem informacija o nastanku slike, i zbog toga su ti metodi definisani kao pasivni metodi. Ta tehnologija se definiše kao *forenzika slika* [11] i zasniva se na posmatranju svake faze u istoriji slike, počev od procesa akvizicije pa do memorisanja u komprimovanom formatu, budući da postprocesiranje ostavlja jasne tragove na podacima u vidu digitalnog otiska. U tom slučaju je moguće identifikovati izvor digitalne slike ili odrediti da li je slika autentična ili modifikovana kroz detekciju prisustva ili odsustva digitalnih otisaka.

Forenzika slika se odvojila od klasične forenzičke nauke, koja koristi naučne metode u cilju pribavljanja fizičkih ili digitalnih dokaza. Zadatak alata forenzike slika je da pronađe tragove koje multimedijalni sadržaji ostavljaju pri svakom koraku svoga ciklusa, korišćenjem postojećih metoda digitalne obrade slike, kao i bezbednosti multimedijalnih informacija. Istraživačke aktivnosti na ovom polju su počele pre nekoliko godina i znatno su postala intenzivnija poslednjih meseci [12].

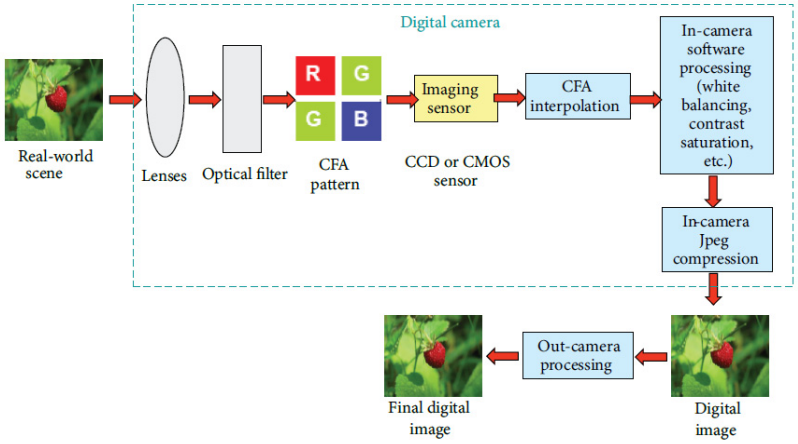
3. Ciklus digitalne slike

Slika 2 prikazuje kako istorija slike može da bude predstavljena kao kompozicija nekoliko koraka, koji mogu da budu grupisani u tri faze: akviziciju, kodovanje i editovanje. U procesu akvizicije svetlo koje dolazi iz realnog izvora se fokusira na sočivima senzora kamere CCD/CMOS (*Charged Coupled Device / Complementary Metal-Oxide Semiconductor*), gde se generiše signal digitalne slike. Međutim, pre nego što dođe do senzora svetlo se obično filtrira pomoću CFA (*Color Filter Array*) jedinica. CFA predstavlja tanak filtar na senzoru koji selektivno propušta određene komponente svetla ka senzoru. U praksi, to znači da svaki piksel (element slike) prikuplja samo jednu određenu glavnu boju (crveno – *Red*; zeleno – *Green*; plavo – *Blue*). Izlaz senzora se sukcesivno interpolira tako da se dobiju sve tri glavne boje za svaki piksel, kako bi se formirala digitalna slika u boji. Dobijeni signal prolazi kroz dodatno procesiranje unutar kamere, koje može da uključi balansiranje belog, obradu boje, izoštravanje slike, poboljšanje kontrasta, kao i gama korekciju.

Posle kodovanja, procesirani signal se memoriše u memoriji kamere. Kod većine kamera slika se komprimuje sa gubicima (*lossy compression*), pri čemu je kod komercijalnih uređaja uglavnom primenjen JPEG (*Joint Photographic Expert Group*) standard.

Tako generisana slika može da bude postprocesirana, na primer da bude poboljšana ili da sadržaj bude modifikovan. Bilo koji način editovanja slike može dalje da bude primenjen u ciklusu slike. Najčešći načini editovanja slike su: geometrijske transformacije (rotacija, skaliranje), zamućivanje, izoštravanje, podešavanje kontrasta,

splajsing (komponovanje slike od delova jedne slike ili od više delova koji potiču od više slika), kao i kloniranje slike (*copy-move*, odnosno replikovanje određenog iznosa iste slike). Nakon editovanja slika se obično ponovo pamti u JPEG formatu, tako da imamo ponovljenu kompresiju.



Slika 2. Blok-šema koja prikazuje korake prilikom uobičajenog ciklusa slike [2]

Osnovna pretpostavka na kojoj se zasniva forenzika slika je da se ostavljaju tragovi, kao što su digitalni otisci, kako u postupku kreiranja, tako i tokom drugih sukcesivnih procesa koji se događaju u istoriji slike. Digitalni tragovi mogu da se izdvoje i analiziraju kroz razumevanje istorije digitalnog sadržaja. Imajući u vidu predstavljanje ciklusa slike mogu se izdvojiti akvizicija otisaka, kodovanje otisaka i editovanje otisaka.

3.1 Akvizicija otisaka

Svaka komponenta digitalnog uređaja za akviziciju signala menja ulaz i ostavlja unutrašnje otiske na konačnom izlazu slike, zahvaljujući specifičnom optičkom sistemu, senzoru slike i softveru koji podržava kameru. Svaki korak se odvija prema izboru određenog proizvođača kamere, tako da tragovi mogu da zavise od brenda kamere i/ili modela. To znači da pri svakom stanju kamera uvodi nesavršenosti koje ostavljaju otiske u konačnoj slici, uvodeći potpis tipa kamere, ili čak individualnog uređaja u okviru slike. Prisustvo nekonzistentnosti kod ovih artifakata može biti uzeto kao dokaz krivotvorenja slike.

3.2 Kodovanje otisaka

Kompresija sa gubicima neizbežno ostavlja karakteristične otiske, koji se odnose na specifičnu arhitekturu za kodovanje signala. Većina literature do sada je bila usmerena ka istraživanju istorije procesiranja JPEG komprimovanih slika, imajući u vidu da višestruka primena JPEG kompresije uvodi različite otiske u odnosu na jednu JPEG kompresiju. Prisustvo nekonzistentnosti kod artifakata kodovanih slika može takođe biti uzeto kao dokaz krivotvorenja slike.

3.3 Editovanje otisaka

Svaka obrada primenjena kod digitalnih slika, čak i ako ne može da se vizuelno detektuje, menja osobine slike ostavljajući tragove u skladu sa postupkom obrade slike.

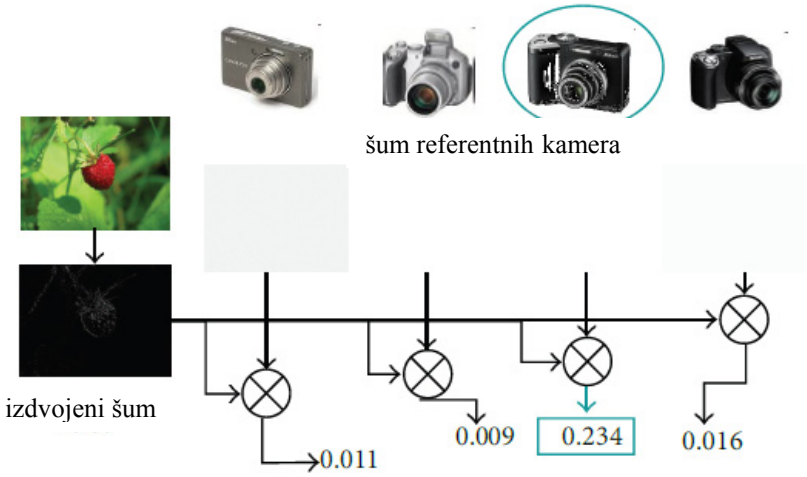
Prethodni tragovi mogu da se koriste sa dva cilja: identifikacija izvora i detekcija krivotvorenja. U slučaju identifikacije izvora obavlja se neka vrsta balističke analize. Neki tragovi akvizicije se obično izdvajaju sa slike koja se analizira i zatim se upoređuju sa nizom podataka mogućih otisaka specifičnih za određenu klasu, brend ili model uređaja. Većina sličnih otisaka u nizu podataka ukazuje na uređaj kojim je slika snimljena. Sa druge strane, u slučaju detekcije krivotvorenja, treba da se prikažu tragovi semantičke manipulacije imajući u vidu dve moguće strategije: detekciju nekonzistentnosti ili odsustvo otisaka akvizicije i kodovanja u okviru razmatrane slike. Odsustvo otisaka indirektno ukazuje na to da ih je uništilo neko postprocesiranje slike. Detekcija editovanja otisaka ukazuje da je postprocesiranje slike dovelo do manipulacije.

4. Akvizicija slike

Pri procesu akvizicije slike od strane kamere treba uzeti u obzir tragove koji potiču od optičkih sočiva, senzora, kao i CFA. Osim toga, akvizicija slike može da se obavlja i pomoću digitalnih skenera, tako da su brojne tehnike koje su prvobitno razvijene za analizu otisaka kamere primenjene i kod analize skenera. Slike mogu takođe da budu i odštampane i ponovo snimljene, tako da treba uzeti u obzir i digitalno/analognu (D/A) konverziju. Od ne manjeg značaja su i slike dobijene fotorealističnom računarskom grafikom, koje zahtevaju transport fizičkog osvetljenja i modele akvizicije kamere.

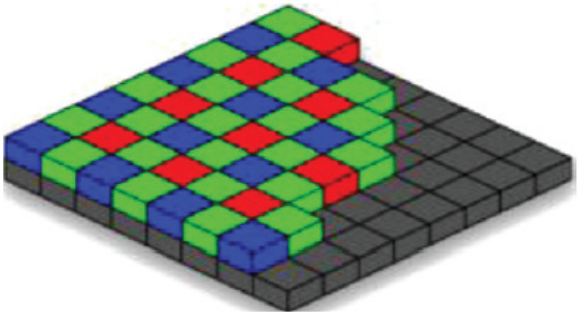
Šum senzorskog *paterna* se javlja pretežno zbog nesavršenosti senzora slike, što ima za posledicu malu razliku između senzorske scene i slike snimljene kamerom. Dominantna komponenta šuma senzorskog *paterna* je šum usled neuniformnosti fotoodgovora (*Photo Response Non-Uniformity* – PRNU), koji nastaje usled kombinacije faktora uključujući nesavršenosti u procesu proizvodnje CCD/CMOS, nehomogenosti strukture silicijuma, kao i termičkog šuma. PRNU je visokofrekvencijski multiplikativni šum, koji je generalno stabilan pod normalnim radnim uslovima kamere, i jedinstven je za svaku kameru. Navedene osobine čine PRNU pogodnim ne samo za identifikaciju uređaja, već i za detekciju krivotvorenja, ukoliko dođe do nekonzistentnosti PRNU paterna unutar slike. Slika 3 pokazuje kako je moguće identifikovati izvornu kameru korelacijom šuma sa slike i PRNU svakog posmatranog uređaja.

Nekonzistentnosti u izdvojenom šumu senzora mogu da se koriste pri utvrđivanju da li deo slike ne dolazi sa očekivanog uređaja. U stvari, ako je deo slike snimljene kamerom zamenjen delom slike snimljene drugim uređajem, onda će PRNU maska u tom regionu biti nekonzistentna sa maskom od originalne kamere. Prema tome, test sa dve hipoteze (krivotvoreno/nije krivotvoreno) može da se obavi u blokovima unutar slike, kako bi se lokalno utvrdio integritet i ustanovila pozicija područja slika gde je došlo do krivotvorenja.



Slika 3. Identifikacija kamere preko korelacije šuma sa slike i PRNU [2]

Osim PRNU, još jedan važan artifakt koji ostavljaju kamere za vreme akvizicije slike postoji zahvaljujući prisustvu CFA. U stvari, osim kod profesionalnih trostrukih CCD/CMOS kamera, osvetljenje koje dolazi se filtrira pomoću CFA, pre nego što dođe do senzora (CCD ili CMOS), kao što je pokazano na Slici 4. Za svaki piksel se prikuplja samo jedna određena boja.



Slika 4. Primer CFA

Da bi se dobile vrednosti piksela koji nedostaju za sva tri sloja boje pri procesu interpolacije se polazi od jednog sloja koji sadrži mozaik crvenih, zelenih i plavih piksela. Taj proces ostavlja specifične korelacije u pikselima slike koji mogu da se detektuju. Radovi koji se odnose na CFA kao otisak mogu da se podele na dve klase: algoritme koji se bave procenom parametara pri interpolaciji boje i strukturom paterna filtara, kao i algoritme koji se bave procenom prisustva ili odsustva tragova. Algoritmi iz prve grupe su uglavnom usmereni ka klasifikovanju različitih izvora kamere, pošto svaki brend kamere može da prihvati različite konfiguracije CFA i različite šeme za interpolaciju. Druga grupa algoritama se fokusira na detekciji krivotvorenja. U idealnom

slučaju, slika koja dolazi sa digitalne kamere će pokazati odgovarajuće artifakte ako nema sukcesivnog procesiranja. Nasuprot tome, nekonzistentnosti između različitih delova analizirane slike mogu da dovedu integritet slike u sumnju.

Slično otiscima kamere, otisci skenera takođe mogu da se koriste za identifikaciju uređaja. Štaviše, detekcija krivotvorenja skeniranih slika je od naročitog značaja, imajući u vidu da banke prihvataju skenirane dokumente kao dokaz adrese i identiteta.

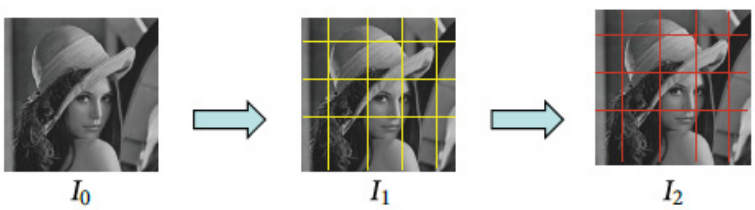
Što se tiče računarski generisanih slika, postoje algoritmi koji automatski prave razliku između realnih i sintetičkih slika. Osnovna pretpostavka je pri tome da su neke statističke karakteristike fundamentalno različite između kamera i računarski generisanog softvera.

5. Kodovanje slike

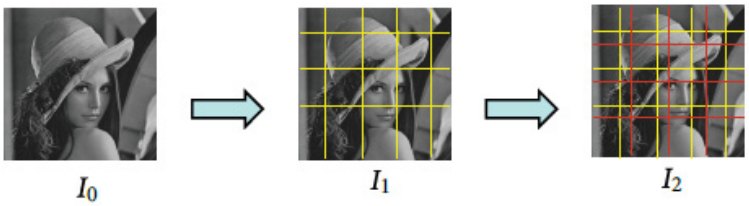
Kompresija slike sa gubicima je jedan od najčešćih postupaka koji se obavlja nad digitalnim slikama. Kompresija je neophodan postupak, imajući u vidu veliku količinu informacija koju poseduje slika, tako da je znatno jednostavnije memorisati i prenositi manju količinu informacija. U stvari, većina kamera komprimuje svaku sliku nakon snimanja. Zbog prirode gubitaka informacije, kodovanje slike ostavlja karakteristične otiske koji mogu da se detektuju i predstavljaju značajni alat pri detekciji krivotvorenja.

U nekoliko scenarija digitalna slika je dostupna u domenu piksela u bitmapiranom formatu, bez *a priori* poznavanja prethodnog procesiranja. U ovim slučajevima od interesa može da bude poznavanje istorije slike, i posebno treba detektovati da li je slika prethodno bila komprimovana i koji su parametri kompresije bili korišćeni. Kodovanje slika zasnovano na blokovima, kao što je JPEG, ostavlja karakteristične tragove kompresije u domenu piksela ili u transformacionom domenu, što može da bude iskorišćeno u forenzičkim metodama.

JPEG format je prihvaćen u većini digitalnih kamera i alata za obradu slike, tako da može da se očekuje da će manipulisani sadržaj često biti rekomprimovana JPEG slika. Stoga, prisustvo krivotvorenja može da se analizira pomoću odgovarajućih artifakata koji se dešavaju pri JPEG rekompresiji kada se formira krivotvorena slika. Takvi artifakti mogu da se podele u dve grupe, prema tome da li je druga JPEG kompresija usvojila mrežu diskretne kosinusne transformacije (DCT) iz prve kompresije, što je pokazano na Slici 5, ili nije, što se vidi na Slici 6. Prvi slučaj se odnosi na poravnatu dvostruku JPEG (*aligned double* JPEG, A-DJPG), a drugi na neporavnatu dvostruku JPEG (*nonaligned double* JPEG, A-DJPG) kompresiju.



Slika 5. Primer za poravnatu dvostruku JPEG kompresiju test-slike „Lena“



Slika 6. Primer za neporavnatu dvostruku JPEG kompresiju test-slike „Lena“

U primeru sa Slike 5 nekomprimovana test-slika „Lena“ I_0 se najpre komprimuje sa mrežom blokova, čime se dobija komprimovana slika I_1. Ta slika se dalje ponovo komprimuje sa mrežom koja je poravnata sa prethodnom mrežom, čime se dobija krajnja slika I_2. Sa druge strane, u primeru sa Slike 6, komprimovana slika „Lena“ I_1 se ponovo komprimuje sa mrežom koja se razlikuje u odnosu na prethodnu mrežu, čime se dobija finalna slika I_2.

6. Zaključak

U ovom radu su predstavljeni alati za forenziku digitalnih slika. Alati su klasifikovani u odnosu na poziciju u istoriji slike na kojima se ostavljaju digitalni otisci. Istaknuto je kako otisci pri akvizicije slike proizilaze iz ukupne kombinacije pojedinih tragova koji su ostavljeni pri svakom stanju u kaskadi procesa akvizicije slike. Alati koji se zasnivaju na tim tragovima normalno zahtevaju da su slike snimljene u kontrolisanim uslovima, ili na tome da je više slika dostupno od strane jednog uređaja. To nije moguće uvek ostvariti, posebno kada se uzmu u obzir jevtini uređaji sa komponentama sa velikim šumom. Prilikom projektovanja algoritama koji rade u realnim scenarijima poželjno je staviti naglasak na kompletan sistem za akviziciju.

Što se tiče otisaka koji se odnose na kodovanje slike, većina literature do sada je bila usmerena ka istraživanju istorije procesiranja JPEG komprimovanih slika. Predloženi metodi su usmereni ka tome da detektuju da li je slika bila JPEG komprimovana, da odrede parametre kvantovanja i da identifikuju tragove koje ostavlja dupla JPEG kompresija.

Literatura

[1] A.J. Menezes, S.A. Vanstone, P.C.V. Oorschot: „*Handbook of Applied Cryptography*“, CRC Press, Boca Raton, USA, 1996.

[2] M. Stamm, M. Wu, K.J. Ray Liu: „Information forensics: an overview of the first decade“, *IEEE Access*, Vol. 1, pp 167-199, 2013.

[3] A. Piva: „An overview on image forensics“, *ISRN Signal Processing*, Hindawi, Volume 2013, Article ID 496701, 22 pages

[4] I.J. Cox, M.L. Miller, J. Bloom, J. Friedrich, T. Kalker: „*Digital Watermarking*“, Morgan Kaufmann, 2001.

[5] G.W. Meyer, H.E. Rusheimer, M.F. Cohen, D.P. Greenberg, K.E. Torrance: „An experimental evaluation of computer graphics imagery“, *ACM Transactions on Graphics*, Vol. 2, No. 2, pp 30-50, 2003.
[6] „Fake or foto“, http://area.autodesk.com/fakeorfoto, 2012.
[7] B. Zhu: „When seeing isn't believing (multimedia authentication technologies)“, *IEEE Signal Processing Magazine*, Vol. 21, No. 2, pp 40-49, 2004.
[8] „Photo tampering throughout history“, http://www.fourandsix.com/photo-tampering-history, 2012.
[9] P. Blythe, J. Friedrich: „Secure digital camera“, *Proceedings of the Digital Forensic Research Workshop DFRS'04*, pp 17-19, 2004.
[10] V. Conotter: *Active and passive multimedia forensics*, PhD dissertation, University of Trento, Italy, 2011.
[11] H. Farid: „Image forgery detection“, *IEEE Signal Processing Magazine*, Vol. 26, No. 2, pp 16-25, 2009.
[12] A. Samčović: „Multimedijalna forenzika – deset godina razvoja“, *XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel 2013*, Saobraćajni fakultet, Beograd, str. 407-416, 3-4. decembar 2013.

Abstract: *In recent decades, we have witnessed the evolution of information and communication technologies from the communication and networking infrastructure, over the standardization of multimedia compression and coding schemes, to effective multimedia content retrieval. As a result, multimedia content has become ubiquitous. This path of technological evolution has naturally led that content and devices are being used by authorized users, and to be able to forensically prove with high confidence when otherwise. When security is compromissed, forensic methodologies and tools are employed to reconstruct what has happened to multimedia content in order to answer who has done what, when, where and how. The goal of this paper is to provide an overview on relative new field of image forensics regarding theories and methodologies.*

Keywords: *compression, forensics, image, multimedia, photography*

RECENT ADVANCES IN DIGITAL IMAGE FORENSICS

Andreja Samčović