UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

-SAVREMENE INFORMACIONE TEHNOLOGIJE-

Forenzika slike

- Master rad -

Mentor:
Doc.dr. Saša Adamović

_____

Student:
Veljko Vukčević

Br. indeksa: 410472/2013

Beograd, 2015.

Sadržaj:

1. Uvod ..... - 3 -
1.1 Cilj istraživanja ..... - 3 -
1.2 Predmet istraživanja ..... - 3 -
1.3 Doprinosi rada ..... - 3 -
1.4 Struktura rada ..... - 4 -
2. Forenzika digitalne slike ..... - 5 -
2.1 Osnovni principi u forenzici slike ..... - 6 -
2.2 Forenzika digitalnih slika ..... - 8 -
2.3 Tipovi digitalne forenzike slike ..... - 12 -
2.4 Analiza bazirana na signalima ..... - 15 -
2.5 Testovi prisustva komponenti ..... - 18 -
2.6 Testovi instanciranja komponenti ..... - 20 -
2.7 Rezime ..... - 23 -
2.8 Suzbijanje i sinteza obrađenih artefakta ..... - 24 -
3. Digitalna analiza slike i forenzika ..... - 36 -
3.1 Problem u radu sa slikama ..... - 36 -
3.2 Dečija pornografija ..... - 37 -
3.3 Digitalna autentfikacija ..... - 37 -
3.4 Metode za analiziranje slike ..... - 38 -
3.5 Mogućnosti za poboljšanje slike ..... - 39 -
4. Tehnike multimedijalne forenzike ..... - 40 -
4.1 Multimedijalna forenzika - principi i motivi ..... - 40 -
4.2 Vrste digitalnih dokaza i njihova karakterizacija ..... - 42 -
4.3 Tehnike za identifikaciju akvizicionog uređaja ..... - 44 -
4.4 Odstupanje sočiva ..... - 45 -
4.5 Tehnike za procenu integriteta slike ..... - 46 -
4.6 Trendovi budućnosti ..... - 47 -
5. Forenzička klasifikacija kamera: Vreifikacija senzora putem šuma ..... - 49 -
5.1 Pregled digitalne kamere: proces kreiranja slike ..... - 50 -

5.2 Šum senzora ..... - 51 -
5.3 Pristupi bazirani na korelaciji ..... - 52 -
5.4 Eksperimentalni rezultati ..... - 53 -
5.5 Referentni obrasci kamere ..... - 54 -
5.6 Identifikacija slike iz neprocesirane slike ..... - 54 -
5.7 Forenzika slike zasnovana na šumu senzora ..... - 57 -
6. Studije slučajeva ..... - 60 -
6.1 Studija slučaja 1: Varez Fabrika ..... - 60 -
6.2 Studija slučaja 2: Moonwalk ..... - 62 -
6.3 Studija slučaja 3: Vojnik ..... - 64 -
6.4 Studija slučaja 4: Dr. Ajman al Zavahiri ..... - 66 -
7. Zaključak ..... - 72 -
7.1 Ostvareni doprinosi ..... - 72 -
7.2 Predlog budućeg rada ..... - 72 -

1. Uvod

U ovom poglavlju predstavićemo cilj i predmet istraživanja, doprinose koje ćemo pokušati da ostvarimo i strukturu rada koja obuhvata sva poglvlja ovog rada.

1.1 Cilj istraživanja

Osnovni cilj ovog rada je upoznavanje sa svim aspektima forenzike slike. Kroz teoriju i studije slučajeva pokazaćemo efikasnost određenih metoda za analizu slike kao i njihove nedostatke u određenim situacijama. Na osnovu svega predloženog, ukazaćemo na značaj forenzičke analize slike za potrebu pribavljanja relevantnih dokaza za potrebe pravosudnih organa.

1.2 Predmet istraživanja

Digitalna forenzika predstavlja primenu naučnih metoda sa ciljem da identifikuje, prikupi i analizira digitalne podatke uz očuvanje njihovog originalnog integriteta. Takođe, može se predstaviti i prezentovanje digitalnih dokaza. Forenzički alati služe za povraćaj i analizu prethodno obrisanih, skrivenih i privremenih fajlova kojima se ne može pristupiti uobičajnim postupkom. Cilj digitalne forenzike jeste da primenom tehnike analize sudstvu obezbedili potrebni dokazi kako bi se metodama za čuvanje, sakupljanje, validaciju, identifikaciju, analizu, interpretaciju, dokumentovanje i prezentovanje izvršila rekonstrukcija događaja okarakterisanog kao kriminalni.

Živimo u eri visoke tehnologije. Elektronski uređaji poput „pametnih“ telefona, tableta, desktop ili laptop računara u kombinaciji sa internetom postali su moćno oruđe koje u pogrešnim rukama može pričiniti veliku štetu.

U paketu sa visokom tehnologijom dolazi i visokotehnološki kriminal. Zbog dostupnosti softvera namenjenih za izmenu digitalnih slika kao i života u dobu socijalnih mreža i elektronskih medija, slike su postale lako dostupne a sa upotrebom softvera i podložne izmenama. Zbog samog značaja i uticaja na svest određene (ciljane) grupe ljudi ili u slučaju vođenja krivičnog postupka protiv određene osobe, neophodno je utvrditi autentičnost slike i time otkloniti sumnje da li su na njoj izvršene određene korekcije ili ne. Tada „na scenu“ stupa forenzika slike!

1.3 Doprinosi rada

Doprinosi ovog rada ogledaju se u kvalitetnom teorijskom pregled metoda koji su danas u upotrebi za analizu slike, razmatraćemo načine preko kojih se detektuje kompjuterski generisana slika, osnovna razlika između ovih i drugih vrsta digitalnih slika kao i otkrivanje da li je došlo do izmena u analiziranoj slici u odnosu na njeno prvobitno stanje, opisaćemo tehnike za identifikaciju uređaja, kao i važnost takve analize, objasniti vremensku forenzika i zbog čega je značajna kao i koji se ciljevi ostvaruju kontra-

forenzikom, radom ćemo obuhvatiti neke česte i neke ne tako česte forenzičke metode za vađenje podataka iz digitalnih slika, opisati metode za razlikovanje prave slike od kompjuterski generisanih, i tako identifikovati ako je slika digitalno izmanipulisana, predstaviti principe i motive digitalne forenzike (sa fokusom na sliku i video) kao i opisivanje dva glavna načina pristupa u rešavanju dva osnovna pitanja: koji je izvor digitalnog sadržaja i da li je taj digitalni sadržaj autentičan ili nije? Na kraju istraživanja daćemo pregled dostupnih alata kojim će forenzičar otkriti poreklo, autentičnost i vlasništvo nad slikom. U cilju prikazivanja važnosti i sposobnosti ovih tehnika prikazaćemo nekoliko studija slučajeva kao i forenzičke pristupe za analizu u istražnom procesu.

1.4 Struktura rada

U prvom poglavlju govori se o tome koji je cilj ovog rada kao i šta je predmet istraživanja. Takođe, navedeni su doprinosi koji će biti ostvareni ovim radom. Na kraju poglavlja data je struktura rada.

Drugo poglavlje govori o forenzici digitalne slike. Biće reči o naciču na koji one nastaju, njihovim karakteristikama i o tragovima identifikacije. Govoriće se o razlikama između pasivne i aktivne forenzike slike kao i o načinima analiziranja slike.

U trećem poglavlju govori se o problemima koje digitalne slike mogu da izazovu. Na primeru će biti predstavljen jedan od vidova manipulacije slike kao i kakve to nosi posledice. Biće reči o dečijoj pornografiji kao i o analiziranju slike.

Četvrto poglavlje govori o identifikaciji uređaja i autentifikaciji slike. Biće reči o tehnikama za identifikaciju akvizicionog uređaja, tehnikama za procenu integriteta slike i o budućim trendovima.

Peto poglavlje govori o verfikaciji senzora putem šuma. Biće reci o identifikaciji slike iz neprocesirane slike, šumu senzora uređaja, načinu kreiranja slike. U eksperimentalnom delu će biti uporedni test 10 digitalnih kamera.

Šesto poglavlje govori se o studijama slučajeva. Biće predstavljena četiri slučaja. U prvom i četvrtom forenzika slike igra važnu ulogu zbog određivanja geografske lokacije mesta gde su slike nastale dok je u drugom i trećem slučaju bitna verodostojnost slike.

Na kraju, u poslednjem sedmom poglavlju dat je zaključak sa ostvarenim doprinosima i predlogom za budući rad.

2. Forenzika digitalne slike

Otkako je Kodakov inženjer Stiven Sason napravio prvu digitalnu sliku daleke 1975, svet je postao svedok tehnološkoj revoluciji koja je fundamentalno promenila način na koji se slike stvaraju, konzumiraju i percipiraju. Naslednici Sasonovog prototipa – kolosusa teškog oko 3,6 kilograma koji je stvarao slike u rezoluciji od 0,01 megapiksela, su u medjuvremenu sazreli da postanu sveprisutni saputnici u našem svakodnevnom životu. Danas, digitalni uređaji koji se lako koriste i jeftin skladišni prostor čine stvaranje digitalnih fotografija prirodnim načinom ljudskog shvatanja i interakcije sa stvarnim životom.

Istovremeno, sama priroda digitalnih podataka dovodi u pitanje mnoge od pozitivnih aspekata koje obično povezujemo sa digitalnim slikama. Digitalni podaci se mogu lako manipulisati. Moćan softver za obradu omogućava čak i relativno neiskusnimkorisnicima da jednostavno obrađuju digitalne slike na bezbroj načina. Dok manipulicije slika u opštosti nisu pojava koja je ekskluzivno vezana za digitalni svet, kritičari su izrazili zabrinutost da nikada nije bilo tako lako menjati sadržaj i smisao slike često do takvog savršenstva da je nemoguće vizuelno razlikovati falsifikovane od autentičnih fotografija. Stalan rast broja otkrivenih digitalnih manipulacija slika znači da ogroman uspeh digitalnog snimanja šteti pouzdanosti slika, posebno u situacijama u kojima društvo bazira važne odluke o njima: u sudu (u kojoj fotografije deluju kao dokazi), u nauci (gde fotografije pružaju empirijske dokaze), i na glasačkim kutijama (u kojoj fotografije oblikuje javno mnjenje).

Ovaj nesklad između sve većeg značaja digitalnih slika sa jedne strane i sumnji u pogledu njihove osetljivosti na manipulaciju na drugoj strani više nego ikad poziva pristupanju sistematskoj proceni pouzdanosti slika. Ono takođe ukazuje na još jednu ambivalentnost koja okružuje digitalne slike. Ne samo da je digitalne slike lako manipulisati , ali takodjelako podležu uticaju moćnih metoda računarske analize, koje pomažu da se prevaziđu ograničenja ljudske percepcije i spoznaje u otkrivanju ovakvih manipulacija. Iako ljudski vizuelni sistem prednjači u shvatanju semantičkih detalja prikazanog scene, računarske metode su obično superiorne u otkrivanju čak i najsuptilnijih tragovi na sintetickom nivou, tj. uvidom u same digitalne podatke slike ili digitalnim podacima koji su sačuvani sa slikom.

Farid i Lukas, početkom milenijuma, su prvi prijavili da post-obrada ostavlja karakteristične tragove u dobijenoj slici. Otprilike u isto vreme, Heerich i Kurosava su napravili slične napore da istraže inherentne tragove uređaja koji su napravili digitalnu sliku. Ovi radovi su postavili temelje iz oblasti digitalne forenzike slike. Od tada su stimulisani naučnici iz različitih istraživačkih zajednica, kao što su multimedijalna bezbednost, kompjuterska forenzike, snimanje i obrada signala, da razviju algoritme koji pomažu otkrivanju manipulacija i omogućavaju da se zaplene uređaji pravljenja proizvoljnih digitalnih slika. Obećanje digitalne forenzike slike je da povrati nešto od izgubljenepouzdanosti digitalnih slika. Pokrivenost u vodećim naučnim časopisima, veliko interesovanje medija, kao i prva praktična primena u primeni zakona sve ukazuje na veliki značaj digitalne forenzike slike u digitalnom društvu. Sve u svemu, možemo očekivati da ova rastuća disciplina igra sve više i više centralnu ulogu u praktičnoj proceniautentičnosti slike u širokom spektru realnih životnih situacija.

2.1 Osnovni principi u forenzici slike

Digitalna forenzika slika ima za cilj da povrati neke od izgubljenih verodostojnosti digitalnih slika i vrti se oko sledeća dva fundamentalna pitanja:

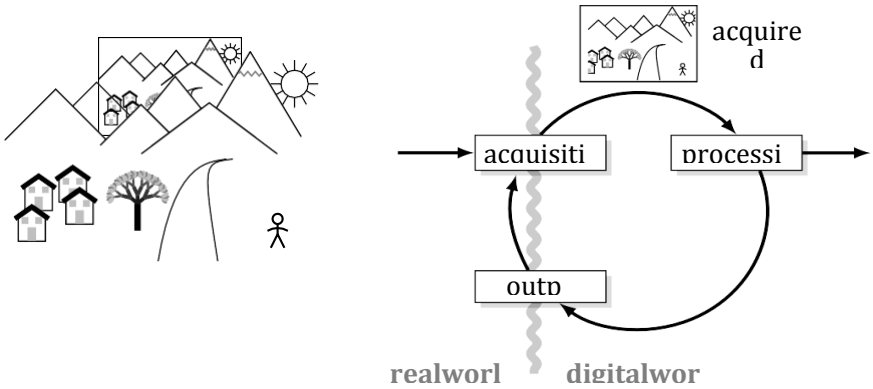
- Odakle slika dolazi?
- (Kako) Da li je slika obrađena nakon sticanja?

Da bi odgovorila na ova i slična pitanja, digitalna forenzika slika koristi činjenicu da karakteristike digitalnih slika zavise ne samo od označenog mesta , već i od određenog načina na koji je slika stečena i prerađena. Ovo omogućava da zaključimo da uređaji i post obrađeni koraci koji su uključeni u proces proizvodnje slike, samim tim mogu da sude o pouzdanosti digitalnih slika.

2.1.1 Akvizicija digitalnih slika

Digitalna slika je rezultat složenog procesa genesiranja slike koja projektuje kontinuirano scenu u diskretnoj reprezentaciji. Scena je deo stvarnog sveta i može se odnositi na bilo koji prirodni fenomen ili da opisuje proizvoljno imaginarnu pojavu koja proizilaze iz ljudskog stvaralaštva. Kao rezultat toga , slika prenosi informacije o prikazanoj sceni koja se, po ljudskoj interpretaciji, prevodi na određeno semantičko značenje. Sam proces generisanja slike može sadržati do tri glavne faze, u zavisnosti od konkretne instance:

- Faza prikupljanja slika je interfejs između realnog i digitalnog sveta, gde se scena projektuje na diskretnoj reprezentaciji. Takve projekcije mogu se održavati preko uređaja koji nabavlja slike koji je opremljen sa senzorom (na primer, digitalnom kamerom), ili može biti potpuno softverski vođeno (kao u slučaju kompjuterski generisanih slika).
- U fazi obrade, stečena slika se menja (ili njeni delovi), što dovodi do obrađene verzije. U ovoj fazi, razlikujemo obradu slike i manipulacije slike. Dok se obrada generalno odnosi na bilo koju promenu početne slike, manipulacija je preciznija i podrazumeva promenu imidža u semantičkom smislu. Drugim rečima, manipulacija narušava autentičnost digitalne slike.



Slika 2.1 Proces generisanja digitalne slike projektuje delove stvarnog sveta (scene) na digitalnu reprezentaciju(digitalna slika). Stečena slika može biti obrađena naknadno ili podvrgnuta ponovnom postupku digitalizacije.

- -Konačno, digitalna slika može proći kroz postupak ponovne digitalizacije, gde se slika ponovo uslika od strane izlaznog uređaja (na primer fotografije kompjuterskih ekrana ili skeniranja otisaka). Napominjemo da seponovna digitalizacija može takođe shvatiti kao poseban oblik post- obrade: rezultirana digitalna slika je modifikovana verzija slike koja se prikazuje na izlaznom uređaju.

Svaki od gore navedenih koraka može biti dalje podeljen na više nezavisnih komponenata. Ove komponente su specijalno instancirane za određene (klase) generacije procesa, gde klasa sažima niz generacija procesa koji dele zajedničke postavke. Različiti modeli digitalnih fotoaparata, na primer, mogu da se razlikuju u njihovom sistemu sočiva, tipu senzora, ili algoritma. Post obrada može sadržati operacije promene veličine ili kontrasta, ili njihove kombinacije.

2.1.2 Pouzdanost digitalnih slika

Kad god su digitalne slike shvaćene kao sredstvo za prenošenje informacija, važno je da se obezbedi pouzdanost te informacije. To naročito znači da slika mora da bude autentična, da slikom nije manipulisano i da prikazana scena važi za predstavljanje realnog sveta . Često, međutim, nije samo prikazana scena ta za koju se smatra da prenosti informaciju, ali takođe i poreklo slike i puke okolnosti koje su dovele do spomenute slike.

Primer 1 | Pouzdanost. Razmotrite na primer, fotografiju koja se nudi uglednom novinarskom listu, kako pokazuje popularnog političkog lidera kako predaje neki tajne dokument nekim sumnjivim lobistima. Odgovorni urednik može ili ne mora da odluči da stavi sliku na naslovnu stranu ne samo u zavisnosti od toga da li je slika prerađena. Takođe, ova odluka može da zavisi od toga da li je slika uzeta od strane renomiranog i pouzdanog novinara ili je procurela tom novinaru od strane osobe iz orbite na suprotnoj strani koji se takmiče za glasove na predstojećim izborima.

Dakle, suđenje o pouzdanosti digitalne slike znači da se mora izvesti zaključakiz istorije teslike. Dok gornji primer ilustruje da, generalno, pitanje verodostojnosti je

povezanosa pitanjem ko upravlja uređaje koji su uključeni u proces generisanja slika, mi ćemo ograničiti naše razmatranje o poreklu slike na utvrđivanje stvarnih uređaja:

1) Sama slika ne može da otkrije identitet operatora.

2)Umesto toga, mi ćemo razmotriti dostupne informacije o umešanim uređajima kao indikacije za poreklo slike, koje se dalje mogu kombinovati sa informacijama iz drugih izvora.

Drugim rečima, mi smo pre svega suočeni sa pitanjem koje komponente su sastavile proces generisanja slika. Na osnovu pretpostavke o procesu generisanja slika(i na osnovu dodatnih informacija), mi ćemo na kraju doći do zaključka u kojoj meri će se slika smatrativerodostojnom, ako uopšte može tako da se smatra. U Primeru 1, nizak kvalitet slike zbog jake JPEG kompresije artefakata može da nagoveštava na korak post obrade i na taj način smanjuje pouzdanost ponuđene slike (nezavisno od njenog stvarnog izvora). Na sličan način, urednik može staviti malo poverenja u sliku kad sazna da je zaista snimljena sa jeftinim potrošačkim uređajem, a za novinare je poznato da favorizujukamere visokog kvaliteta sa punim frejmovima.

2.2 Forenzika digitalnih slika

Primarni cilj forenzičkih nauka je sistematička rekonstrukcija događaja, kao i identifikacija subjekata koji su uključeni. Forenzičke analize digitalnih slika (ili forenzika digitalnih slika) se odnosi na rekonstrukciju procesa generisanja date digitalne slike, gde glavni fokus leži na zaključku o autentičnosti slike i njenog porekla. U užem smislu, termin "forenzički"označava primenu naučnih metoda u istrazi i krivičnom gonjenju zločina, ishodi forenzičke analize mogu poslužiti kao dokazna činjenica na sudu. Vođeni rasprostranjenošću digitalnih slika, termin "forenzika digitalnih slika" se koristi za šire kontekste u literaturi, sa širokim spektrom primene i izvan sudnice. Iako poverenje (i posebno autentičnost) je preduslov za slike da se uvode kao dokazi na sudu, očekujemo i zahtevamo pouzdanost u bilo kojoj situacija u kojojmoramo da se oslonimo na sliku. Ovo znači da primena digitalne forenzike slike nema samo pravnu već uopšte i veoma jaku socijalnu dimenziju.

Tokom ovog teksta, mi ćemo stoga razumeti digitalnu forenziku slike krajnje uopšteno kao i bilo koji sistematski pokušaj da se proceni pouzdanost digitalne slike na osnovu svog procesa proizvodnje. Poziv za sistematskim pristupima naglašava vezu sa forenzičkim naukama uopšte, a samim tim i mi ćemo se odnositi na predmet koji sprovodi analize digitalnih fotografija za potrebe digitalne forenzike sliku kao forenzički istražitelj.

2.2.1 Karakteristike slike i potencijalni tragovi identifikacije

Ključ za digitalnu forenziku slike je pretpostavka da komponente procesa proizvodnje slike utiču na karakteristike dobijene slike i da su ove karakteristike slika specifične za odgovarajuće procese genesiranja. Izbog samog postojanja određenih komponenti i zbog razlika u njihovoj proizvodnji i primeni, različiti procesi generisanja

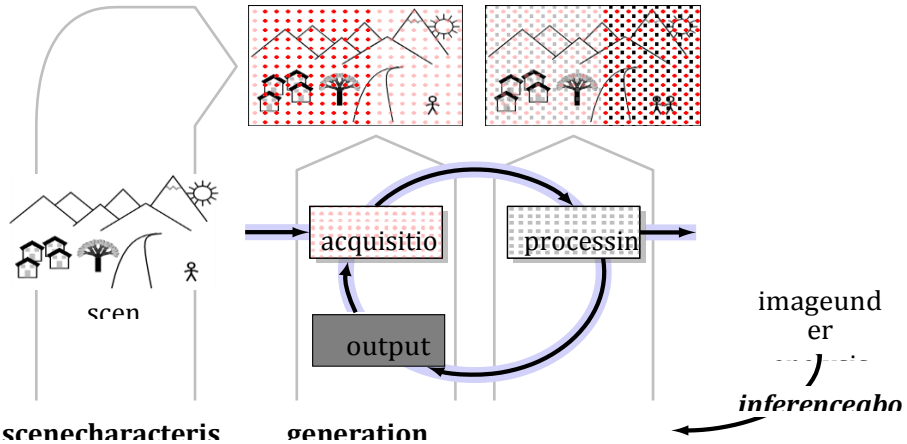
razlikuju se u načinu na koji oni utiču na karakteristike dobijene slike. Na kraju, ove varijacije dozvoljavaju zaključak o pojedinostima procesa generisanja slika i na taj način nam omogućavaju da procenimo pouzdanost date slike.

De Rosa preformuliše pretpostavku iznad kao dvodelnu dekompoziciju slike. Prvi deo se odnosi na svosjtva same scene i stoga prenosi semantički smisao originalne slike. Parametri procesa generisanja slika i njihov uticaj na rezultirajuću sliku određuje drugi deo. Iako ovadekompozicija izgleda prilično teoretski (jer digitalna slika po definiciji postoji samo preko određenog procesu proizvodnje, teško je zamisliti "idealnu" sliku koja je nezavisna od ovog procesa), mi ćemo usvojiti Ideju koja stoji iza ove konstrukcije i odsada ćemo praviti razliku između karakteristikeascene i karakteristika procesa generisanja, respektivno.

Slika 2.2 se nadovezuje na prethodnu sliku 2.1 i ilustruje uticaj karakteristika scene i procesa generisanja u kontekstu digitalne forenzike slike. Crveni krugovi i crni kvadrati pokazuju, u stilizovanom načinu, da svaka komponenta procesa generisanja može da ostavi sopstvenei karakteristike (ovde je prikazan primer za akviziciju i fazu obrade, respektivno). Tehnički, cilj forenzičkog istražioca je da identifikuje kojiproces generisanjaje doveo do analize slike.Iz tog razloga, govorimo o identifikaciji tragova kada govorimo o specifičnim obradivim karakteristikama digitalnih slika.

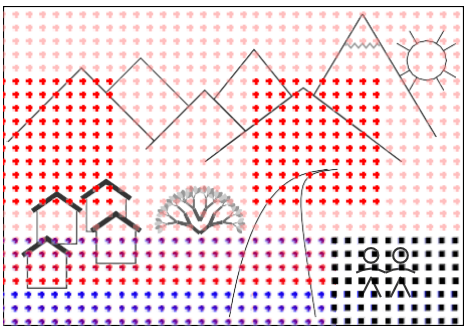
Tragovi identifikacije uopšte poseduju visoke interklasne sličnosti i niske intraklasne sličnosti. To znači da su odgovarajuće karakteristike veoma slične za sve slike istogprocesa generisanja, ali se razlikuju za slike različitihprocesa generisanja. Ovom identifikacionom problemuse prilazi upoređivanjem referentnih tragova poznatih slučajeva procesa generisanja sa tragovima pronađenim na slici pod istragom. Digitalna forenzika slika je otuda problem odluke, gde forenzički istražitelj treba da dodeli datu sliku nepoznatog porekla poznatomprocesu generisanja, ili nijednom od njih, kada nije pronađeno nijednopodudaranje.

Generalno, karakteristike različitih komponenti nisu nezavisne jedna od druge. Svaki pojedinačna komponenta procesa generisanja slika može ometati ili čak izbrisati tragove prethodnih komponenti. Ovo znači da karakteristike u ranijim fazama nisu više nužno prisutni u finalnoj slici. Forenzički istražitelji mogu proceniti autentičnost slike ne samo na osnovu prisustva identifikacionh tragova, već i eksplicitno na osnovu nepostojanja (očekivanih) tragova ili, uopšte, njihovoj nedoslednosti po tumačenju nestalih tragova identifikacije kao jake indikacije za post obradu slike. Nedoslednost ovde znači da tragovi koji su nađeni u slici pod istragom su kompatibilni sa referentnim tragovima različitih, možda kontradiktornih, procesa generisanja. U prvom primeru, na primer, može se ispostaviti da su delovi slike izrezani da bi sakrili prisustvo drugih političara sa ciljem da se slici promenisemantički smisao. Ovo dovodi do toga da veličina slike nije u skladu sa veličinom senzora modela fotoaparata kako je navedeno u pratećim Exif podacima.



Slika 2.2 Karakteristike digitalne slike podeljene na karakteristike scene i procesa generisanja, respektivno. Forenzika digitalnih slika pretpostavlja da komponente procesa generisanja slika ostavljaju tragove identifikovanja u kirajnoj digitalnoj slici. Ako su nađeni u slici pod analizom, ovi tragovi dozvoljavaju forenzičkim istražiteljima da zaključe o pojedinostima u procesu proizvodnje.

Uopšteno govoreći, možemo razlikovati između inter-karakterističnih i intra-karakterističnih nedoslednosti. Ovo neslaganje između rezolucije slike i Exif podataka je tipičan predstavnik bivšeg tipa, gde analiza različitih karakteristika dovodi do kontradiktornih zaključaka u vezi sa procesom generisanja slika. Intra-karakteristične nedoslednosti, sa druge strane, se odnose na prostorne varijacije jedne posebne karakteristike-verovatno zbog lokalnih manipulacija pojedinih regiona slike-koji dovode do nedoslednih zaključaka iz analize tragova u različitim delovima slike. Slika 2.3 daje ilustrativan primer, gde lokalna manipulacija u donjem desnom delu slike je dovela do tragova post-obrade kao i do nestalih tragova u fazi sticanja u odgovarajućem regionu slike. Ovo naravno podrazumeva da odgovarajuće karakteristike mogu biti analizirane lokalno, da respekticni identifikujući tragovi budu prisutni u različitim delovima slike. Gornji primer pokazuje da ovo nije preduslov za postojanje inter-karakterističnih nedoslednosti: veličina i metapodaci su karakteristike slike u celini.



Slika 2.3 Karakteristike slike utiču jedna na drugu. Lokalna obrada slike može dovesti do nedoslednih identifikacionih tragova (ovde u donjem desnom delu slike) . Pogledajte takođe Sliku 3.2

2.2.2 Kontra forenzika

Da bi opravdali poverenje koje dodatno stavljamo u digitalne slike preko forenzike, važno je da su granice forenzike slike poznate i da će na kraju biti prevaziđene. Pozivanje na proces generisanja slika je obično namerna radnja koja se sprovodi od strane čoveka zbog određenog razloga. Dobijena slika treba da prenese određenu informaciju, ili o

označenoj sceni (i subjekata i objekata na njoj) ili o samom tvorcu slike. Kao posledica toga, nema sumnje da će dalekovidni akteri dati sve od sebe da utiču na rezultat potencijalne forenzičke analize u povoljnom ishodu za sebe, da zadrže informacije koju žele da prenese slika. U navedenom prvom primeru, na primer, izvor pod znakom pitanja iz suprotne stranke možda želi da prikrije činjenicu da je sa slikom zapravo manipulisano i može pokušati da prikrije poreklo slike.

To čini digitalnu forenziku slika bezbednosnu disciplinu, koja treba da predvidi inteligentne falsifikatore, i koja mora da se meri po svojoj otpornosti na protivmere. Istraživačko polje koje izaziva digitalnu forenziku i sistematski istražuje svoja ograničenja protiv takvih falsifikata se zove kontra forenzika, ili anti forenzika. Oba termina se sinonimi u literaturi. Radije se koristi prvi izraz jer bolje odražava pragmatičnu reakciju na forenzičare, za razliku od normativnog neslaganja forenzičara.

U opštem okruženju, kontra forenzika je definisana po Harris-u kao svaki pokušaj «ugrožavanja dostupnosti ili korisnosti dokaza forenzičkom procesu». U kontekstu digitalne forenzike slike, kontra forenzika se prevodi kao modifikacija ili zamena (delova) originalnog procesa generisanja slike, tako da se rezultirani falsifikat ne pokazuje dovoljno korisnim pri identifikovanju tragova originalnog procesa generisanja. Falsifikatori, međutim, nisu potpuno slobodni u svom izboru protivmera, jer treba da sačuvaju namenjen semantički smisao slike. Osim toga, jasno je da falsifikatori treba da budu svesni novih tragova identifikacije, koji mogu potencijalno da povežu falsifikat sa modifikovanom postupkom generisanja slike. Ovo postavlja pozornicu za trku u naoružanju koja omogućava kontra forenzici da stoji u jednako produktivnom odnosu prema forenzici slike, kao što kriptoanaliza prema kriptografiji. Zato smo uzeli iz kriptoanalize terminologiju i nazvališematski napad kontra forenzike (protiv forenzike digitalne slike).

Osim potrebe da se proceni i poboljša pouzdanost forenzičkih metoda, još dva razloga motivišu istraživanje o kontra forenzici. Prvi, karakteristike procesa generisanja indirektno otkrivaju informacije o identitetu autora digitalne slike ili prikazanim predmetima na njoj. Ovo nije uvek poželjno. Istraživači su proučavali sisteme koje pružaju nepovezanost i anonimnost u digitalnoj komunikaciji dugo vremena. Svi ovi napori su beskorisni ako veza sa predmetom može biti ponovo uspostavljena od strane poruke forenzičke analize. Stoga kontra forenzičke tehnike u suzbijanju tragove porekla u digitalnim slikama su relevantni kamen temeljac za komunikacijuanonimne slike, što može biti korisno u praksi da se zaštiti identitet izvora, u slučaju legitimnog duvanja u pištaljku.

Drugi razlog je da neki autori tvrde da kontra forenzika, ako se implementira u sticanje uređaja za pravljenje slika, može biti korisna da se sakriju detalji unutrašnjeg cevovoda za snimanje i na taj način obeshrabre obrnuti inženjering. Napominjemo ovu motivaciju u potpunosti, ali treba ostati rezervisan utome da li je sadašnja kontra forenzika dovoljno zrela za tu svrhu. Naša glavna briga je da kontraforenzika često podrazumeva gubitak kvaliteta slike. Proizvođači kamera, na primer, se takmiče za kvalitet. Teško je poverovati da će žrtvovati konkurentsku prednost da bi otežaliobrnuti inženjering. Ipak, mi smo radoznali da vidimo obećavajuće aplikacije u budućnosti.

2.3 Tipovi digitalne forenzike slike

Do sada smo razmatrali digitalnu forenziku slike u veoma opštem ambijentu. Književnost obično shvata digitalnu forenziku slike u užem smislu i odnosi se na pasivno - slepu forenziku slike. Pre nego što budemo pratili ovu uspostavljenu konvenciju u nastavku ovog teksta, moramo da opišemo značenje “pasivno” i “slepo” u ovom kontekstu, i tako podesimo opseg pratećihdiskusija.

2.3.1 Pasivna u odnosu na aktivnu forenziku slike

Digitalna forenzika slike se može nazvati pasivnom ako forenzički istražitelj ne može da se meša u proces generisanja slike i u kontrolu tipa i / ili pojave identifikacionih tragova. Proces generisanja slika se smatra kao "read-only" postupak i forenzički istražitelj je ograničen na ispitivanje karakteristika slika koje su generisane ovim procesom.

Identifikacija tragova u pasivnoj forenzici slike u opštosti se delina karakteristike uređaja i obradu predmeta. Prvobitni se odnosi na inherentne varijacije između različitih sticanja uređaja i na taj način omogućava zaključak o poreklu date digitalne slike. Takve varijacije mogu postojati, na primer, jer proizvođači koriste različite komponente ili prilagođavaju podešavanja parametara za različite uređaje. Takođe mogu biti uzrokovane (neželjeno) inherentinm tehnološkim nedostacima, kao što je nedostatak senzora. Obrada artefakata, s druge strane, se odnosina identifikovanje tragova koji su opisani post-preradom stečene digitalne slike. Dakle, oni su sredstvo za procenu autentičnosti slike. Slično karakteristikama uređaja, različite procedure za obradu mogu da variraju u karakteristikama rezultirajućih tragova i time omogucuju zaključak o vrsti obrade. I karakteristike uređaja i prerada predmeta mogu biti testirani na njihovo prisustvo i doslednosti, pri čemu neuskladne karakteristike uređaja su sami po sebi prerađeni artefakt.

Aktivni pristupi se razlikuju od pasivnih pristupa u tome da je proces generisanja namerno modifikovan u ranijoj fazi da ostavi iza sebe specifične identifikacine tragove. Ovi pomoćni podaci, bi - kada budu vezani za sliku - uspostavili vezu sa poreklom slike ili bi obezbedili autentičnost slika. Tipični primeri aktivnih pristupa pridodaju metapodatke slici (npr , kriptografski potpis ili ugrađeni digitalni vodeni žig direktno u samoj slici). Imajte na umu da je proces generisanja slike na slici 2.1 i pojam identifikacije tragove su opšte dovoljni da pokriju i pasivne i aktivne pristupe. Razmislite na primer da je ugrađivanje digitalnog vodenog žiga, što je samo dodatna komponenta u ukupnom procesu generisanja slika, posebno osmišljen da proizvede identifikacione tragove.

Identifikacioni tragovi u aktivnoj forenzici slike su dizajnirani da povežu nastalu sliku sa svojim poreklom, ili da budu osetljivi ('krhki') napost-obradu slike. Po testiranjima na njihovo prisustvo i doslednost, ovi tragovi dozvoljavaju zaključak o odgovornoj komponenti, kao i za sledeću komponentu u procesu generisanja slika. Za razliku od identifikovanja tragova u pasivnim pristupima, vrsta i pojava takvih tragova mogu biti izabrane u očekivanju potencijalnih pratećih koraka u procesu generisanja slike. Takođe mogu biti dizajnirani na osnovu kriptografskih protokola da garantuju poverljivost putem matematičkih dokaza. Aktivni pristupi idealno treba da se primenjujuneposredno u uređaju pravljenja slike. Nije moguće izvesti zaključak o delovima procesagenerisanja pre aktivnog

ubacivanja odgovarajućih tragova. Ovo oslanjanje na namenski hardver je jedan od glavnih nedostataka aktivne forenzike slika: ne dozvoljava da se proceni pouzdanost proizvoljnih slika nepoznatog porekla. Osim toga, nedavni primeri hakovanih aktivnih authentifikacionih sistema velikih proizvođača digitalnih fotoaparata ukazuju na to da takvi sistemi stvaraju varljiv utisak poverenja kada se greške implementacije ne mogu isključiti. [1]

2.3.2 Slepa u odnosu na neslepu forenziku slike

Digitalne forenzike slika se zovu slepim ako je forenzički istražitelj ograničen na ispitivanje krajnjeg rezultata procesa generisanja. Posebno, znanje originalne scene niti bilo kojih drugih posrednih rezultata procesa generisanjanije dostupno u vreme analize. To uključuje nesigurnost za forenzičkog istražitelja o tome da li je slika pod analizom bila predmet bilo kakve post-obrade. Slepa analiza, međutim, ne podrazumeva nužno da forenzički istražitelj nema znanje ili pretpostavke o potencijalnim komponentama u procesu generisanja slika. Ovo se posebno odnosi na aktivnu forenziku slike, jer je proces generisanja slikanamerno modifikovan od strane istražitelja u ranijoj fazi. Ali i pasivni forenzički istražitelji se mogu osloniti na takve informacije. Na primer, često se zna (sa razumno visokom sigurnošću), kojim uređajem je slika snimljena kada se analizira za protivurečne karakteristike uređaja i potencijalnim manipulacijama.

Dodatne informacije o srednjim rezultatima pomažu ne-slepim forenzičarima da razdvoje scenu i karakteristike procesa generisanja, a samim tim i da donesu više informisane odluke. Ovi podaci mogu biti dostupni iz alternativnih izvora (na primer, iz ranijih verzija prerađene slike koja je objavljene na drugom mestu), ili su mogli biti namerno sačuvani unapred (najverovatnije o stečenoj slici). Informacije sa strane o originalnoj sceni takođe može biti preuzete od drugih (proverenih) slika koje postoje na istoj sceni. Ne-slepi pristupi generalno imaju prednost da ublaže neke od nesigurnostiforenzičara. Istovremeno, oni su često neodrživi u praktičnim podešavanjima. U stvari, ne - slepa forenzika isključuje ispitivanje proizvoljnih slika nepoznatog porekla.

Swaminathan dodatnodeli ne-slepu forenziku na polu-nametljivi i nametljivi pristup. Polu-nametljiva analiza razmatra proces stvaranja slike kao crnu kutiju, koja se hrani poznatim ulaznim signalimai omogućava zaključak o ukupnim ulazno-izlaznim odnosima. U nametljivoj analizi, forenzički istražitelj takođe ima znanje o ulaznim i izlaznim pojedinačnim komponentama procesa generisanja slike i ima za cilj da utvrdi njihov konkretan primerak. Ova razlika postaje naročito važna kada je forenzički istražiteljmanje zainteresovan za procenu pouzdanosti slike, ali u stvari za "reverse-inženjering" parametara procesa generisanja slika (gde je odobren pristup). Tad je moguće dizajnirati posebne ulaze, ili da se upotpuni proces generisanja ili pojedinačnim komponentama, koji su posebno pogodni za analizu i razlikovanje identifikujućih tragova raznih primeraka.

2.3.3 Pasivnoslepa forenzika slike

U nastavku ovog teksta, fokusiraćemo se na pasivno - slepu forenziku slike i koristićemo ovaj termin kao sinonim za digitalnu forenziku slike. To sledi iz gore navedenih diskusija koji govore da pasivno - slepi forenzički istražitelji ne mogu ni pristupiti niti kontrolisati komponentama procesa (pasivne) generisanja slika, niti ima saznanja o ulazima ili srednjim rezultatima. Njihova analiza je isključivo bazirana na osnovu bitnih karakteristika uređaja i obradi predmeta, koji su izvedeni iz slike pod istragom da se može zaključiti o pojedinostima datog procesa generisanja slika.

Pošto je pogled forenzičkog istražitelja ograničen što se tiče slike pod analizom, pasivno-slepa forenzika slika će uvek ostati netačna nauka. Sa digitalnom slikom kao projekcijom beskonačnog skupa svih mogućih scena, forenzički istražitelj ne može nikada u potpunosti znati da li je prikazana scena zaista predstavljanje realnog sveta, ili da li je slika izmanipulisana na neki način. U principu, uvek će postojati preostala mogućnost da određenascena nameće određene karakteristike slike koje se pojavljuju pred forenzičkim istražiteljom kao karakteristike uređaja ili prerađenog artefakta i na taj način dovode do pogrešnih odluka. Osim toga, svaki proces generisanja slika neizbežno uključuje i kvantizaciju. Po definiciji, kvantizacija uzrokuje gubitak informacija i samim tim ostavlja forenzičkog istražitelja sa dodatnim izvorom neizvesnosti. Kao posledica toga, bilo koji rezultat pasivno-slepe forenzike slike mora da se shvati kao indikacija, koja sama po sebi isključuje apsolutne zaključke.

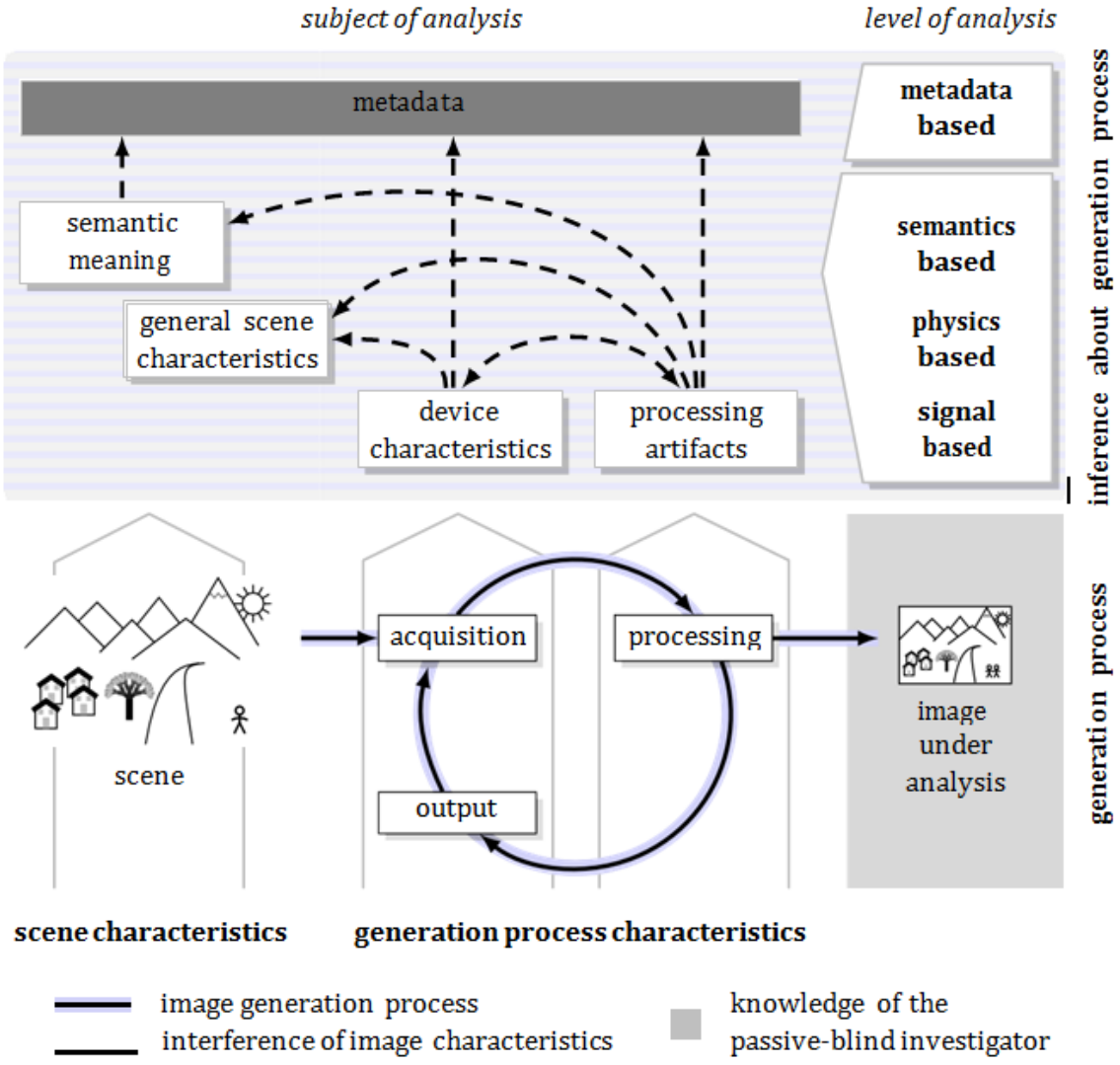
Međutim, prednost pasivno - slepe forenzike slika je njena univerzalna primenljivost. Posebno je primenljiva na analizu proizvoljnih snimaka nepoznatog porekla. Pasivna- slepa forenzika slika se ne oslanja na zatvorenoj infrastrukturi pouzdanih uređaja specijalne namene za prikupljanjekoji aktivno uvodetragove identifikacijerezultujućihslika. Iako ovo može biti održiva opcija za relativno malu primenu, svakako je preskupa i najverovatnije politički neodrživa da se realizuje u tipičnim potrošačkim uređajima.

2.3.4 Apstraktni slojevi u pasivnoslepoj forenzici slike

Pasivno-slepi forenzički istražitelji mogu ispitati identifikujuće tragove na različitim nivoima apstrakcije. Takvi slojevi apstrakcije - generalni koncept za forenzičku analizu bilo koje vrste digitalnih dokaza sa semantičkim značenjem – pomaže dase obuhvati i prouče osnovne osobine scene i karakteristika procesa generisanja, respektivno. Slika 3.4 ilustruje bitne slojeve apstrakcijeu kontekstu pasivno-slepe forenzike slike i služi kao plan za naredne diskusije. Nivoi analize i odgovarajuće karakteristike slike od interesa su raspoređeni po redovima u gornjem delu slike. Isprekidane strelice pokazuju kako se relevantne karakteristike “propagiraju”, tj. koje se karakteristike mogu ometati međusobno. Na najnižem nivou, forenzički istražitelji analiziraju karakteristike procesagenerisanja tumačeći digitalne podatke slike kao niz diskretnih simbola bez uzimanja bilo kakvog semantičkogznačenja u obzir. Viši nivoi apstrakcije iz običnog signala ispituju kako su karakteristike scene i semantičko značenje slika naročito pogođeni procesom generisanja slika. Pored ispitivanja karakteristika slike i osobina scene, forenzički istražitelji mogu dodatno da iskoriste pomoćne metapodatke koji se skladište sa slikom.

2.4 Analiza bazirana na signalima

Forenzička analiza bazirana na signalima gleda na sliku pod istragom kao na običan niz diskretnih simbola i ignoriše njen semantički smisao. I karakteristike uređaja i prerađeni artefakti mogu da utiču na pojavu ovog samog signala, gde prerada može rezultirati u nestale karakteristike ili u karakteristike uređaja koje nisu u skladu i obrnuto. Pošto je slika analizirana nezavisno od njenog semantičkog značenja, idealni identifikujući tragovi na nivou signalamogu postojati samo ako su nezavisni od sadržaja slike. To se ogleda u slici 2.4, koja ilustruje da forenzičke analize na niskom nivou ne uzimaju svojstva scene višeg nivoa u obzir.



Slika 2.4: Apstraktni slojevi u pasivno - slepoj forenzici slika

Za datu sliku pod analizom, pasivno - slepa forenzika slika zaključuje pojedinostima nepoznatog procesa generisanja slika na osnovukarakteristika uređaja i obrađenihartefakta. Ove karakteristike procesa generisanja ne samo da ometaju jedni druge, već i karakteristike scene i pomoćne metapodatke koji se nalaze sa slikom. Forenzičari stoga mogu sprovesti njihovu analizu na različitim nivoima apstrakcije.

U praksi, posmatramo kontinuum mogućih analiza iz nivoa signala ka višim nivoima. Prvo, određene procedure u procesu generisanja slike su sami po sebi prilagodljivi na sadržaj i forenzički istražitelji mogupripojiti ovo znanje. Drugo, neki delovi jedne slike treba da budu isključeni iz forenzičke analize ili da zahtevaju poseban tretman (npr zasićeni ili u velikoj meri homogeni regioni u otkrivanju kopiranja falsifikata). Konačno, indikacije nivoa signala mogu se kombinovati sa semantičkim informacijama, jer analiza na niskom nivou često nije dovoljna da odgovori na opšta pitanja da li je slika pod istragomautentična. Tačnije, sama detekcija post-obrade u celini ne otkriva da li je semantičko značenje slike promenjeno. Dakle, većina praktičnih forenzičkih algoritama - mada u potpunosti automatski u teoriji-danas zahtevaju ljudsku interpretaciju njihovih rezultata.

2.4.1Analiza bazirana na sceni

Eksplicitno uzimajući u obzir svojstva scene, forenzički istražitelji razlikujuapstraknte od diskretnih podataka slika i ispituju identifikacione tragove na višem nivou, slika 2.4. Odavde, mi dalje možemo razlikovati analizu baziranu na fizici i analizu zasnovanu na semantici. Prva se odnosi na opšte karakteristike scene koje su svojstvene (projekcijama) realnog sveta, dok se druga odnosi na semantičko značenje određene slike pod istragom.

2.4.2Analiza bazirana na fizici

Premisa bilo koji analize na bazi fizike je da (projekcije) pojave iz stvarnog sveta poštuju određena opšta fizička pravila, koja su izazvana prirodnim zakonima. Svako kršenje ovih pravila se shvata kao prerađeni artefakt i može poslužiti kao identifikujući trag u forenzičkoj istrazi. Ng i Čang su nazvali ovo "prirodni kvalitet scena" u digitalnim slikama i pomenuli su relevantne karakteristike kao što su osvetljenje, senke i refleksija objekata u slici. Drugi tragovi rezultiraju u geometrijskim ograničenjima, (na primer, relativni položaj objekata u realnom svetu), ili teksture i karakteristike površine. Kao što je prikazano na slici 4.4, karakteristike uređaja mogu uticati na određene opšte karakteristike scene. Tipičan primer su osvetljenje i senke na slici. Oni mogu varirati u zavisnosti od toga da li blicopaljen ili nije. Radijalna distorzija objektiva je još jedan primer. Ovde, originalne ravne linije u stvarnom svetu se pojavljuju savijene u označenoj sceni.

Sve navedene karakteristike imaju zajedničko to da se mogu proučavati bez eksplicitno znajući semantički smisao scene. To je pre sintaksa scene koja je od interesa ovde. Ipak, zato što su ove karakteristike ispitane na osnovu podataka digitalne slike, njihova analiza može biti vršena računarskim metodama. Mnogi forenzički algoritmi ove vrste su ipak polu - automatska u smislu da oni zahtevaju ljudski predizbor najbitnijih objekata za analiziranje i / ili ljudsko tumačenje rezultata.

2.4.3 Analiza bazirana na semantici

Na najvišem nivou, semantička analiza direktno se odnosi na semantičko značenje slike pod istragom (Slika 2.4). Ključno pitanje da se odgovori je da li su informacije prenešene na slici prihvatljive, tj., da li slika važi za predstavljanje realnog sveta. To podrazumeva tumačenje označene scene i na taj način zahteva kontekstualno znanje, kojepovezujedigitalnu sliku sa pretpostavljenom originalnom scenom u stvarnom svetu (na primer, ono što je prikazano na slici, gde i kada je slika nastal …). Nedoslednosti između konteksta informacija i semantičkog značenja slike su tada shvaćeni kao prerađeni artefakt. Pošto su kompjuterski algoritmi potpuno automatizovani i razumevanje slikezavisne od konteksta ne postoji, prava semantička analiza slika ostaje zadatak koji uključuje značajne ljudske interakcije.

2.4.4 Analiza bazirana na metapodacima

Pored samih podataka slike, forenzički istražitelji mogu da iskoriste bogat izvor pomoćnih digitalnih podataka, koji obično prate sliku pod istragom. Danas , poželjan način da se organizuju i sačuvaju takvi metapodaci je navedeno u standardu Ekif. U forenzičkoj analizi, metapodaci mogu pružiti informacije o uređaju sticanja i njegovim postavkama, vreme i mesto sticanja, softvera koji je korišćen za post-obradu i još mnogo toga. (To se ogleda u slici 2.4, gde polje metapodataka pokriva čitav spektar od karakteristika scene do karakteristika procesa generisanja). Osim toga, mnoge digitalne slike su u pratnji sa sličicom niske rezolucijeda se ubrza pregled u aplikacijama za pregled fajlova.

Oblik, sadržaj i struktura metapodataka i sličice mogu poslužiti kao izvor forenzičkih dokaza. Ove karakteristike omogućavaju da se pristupipouzdanosti slike nezavisno od stvarnih podataka slike. Takođe je moguće povezati ove informacije sa slikom i da se interpretirajunedoslednosti na nivou scene i na nivou signalakao što je obrada artefakta. U analizi na nivou signala, Ki i Faridna primer procenjuju parametre procesa generisanjasličice iz podataka slike. Semantičke nedoslednosti mogu biti otkrivene od strane visokog nivoa poređenje sličica i pune rezolucije slike ili testova za prihvatljivosti određenih podešavanja kamere (na primer brzina zatvarača, datum i vreme slikanja…).

Međutim, mana metapodataka je da se relativno lako mogu izmeniti. Pošto se metapodaci čuvaju odvojeni od stvarne slike, uvek je moguće izmeniti delove ili potpuno zameniti metapodatke i minijaturne slike u cilju prikrivanja pojedinosti tog procesa generisanja slika. Kao rezultat toga, forenzičke analize pomoćnih digitalnih podataka u većini slučajeva može biti samo prvi korak ka detaljnoj analizi zasnovanoj na podacima slike.

Specifični ciljevi pasivno-slepe forenzike slike:

Pasivno - slepa procena pouzdanosti slika podvodi niz konkretnijih ciljeva. Slika 2.5 ilustruje da možemo uopšte da razlikujemo tri kategorije. Testovi za samoprisustvo (ili odsustvo) komponenti procesa generisanja slike kod slikanja, post- obrade ili izlazne faze dozvoljava da se otkriju kompjuterski generisane, obrađene ili ponovo uslikane slike. Pregledom konkretne instancepojedinih komponenti, to je dalje moguće identifikovati

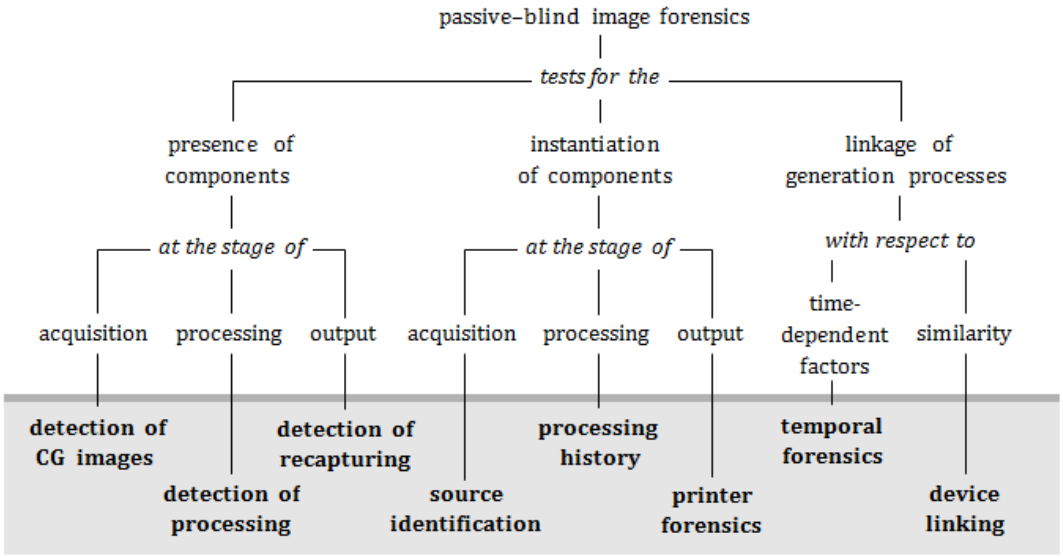
izvor slike, da se zaključio njenoj istoriji obrade, ili da se odredi izlazni uređaj u postupku ponovne digitalizacije. Konačno, veza između brojnihprocesa generisanja slika mogu biti od interesa, na primer sa pogledom na vreme njihovog pozivanja ili njihove ekvivalentnosti.

2.5 Testovi prisustva komponenti

U daljem tekstu sledi način na koji se detektuje kompjuterski generisana slika, osnovna razlika između ovih i drugih vrsta digitalnih slika kao i otkrivanje da li je došlo do izmena u analiziranoj slici u odnosu na njeno prvobitno stanje.

2.5.1 Detekcija kompjuterski generisanih slika

Otkrivanje kompjuterski generisanih slika pripada prvim problemima izučavanim u oblasti digitalne forenzike slika. Osnovna razlika između kompjuterski generisanih slika i drugih vrsta digitalnih slika je odsustvo uređaja za sticanja slika u procesu generisanja slika. Umesto toga, kompjuterski generisana slika je digitalna predstava imaginarnih prizora koji proizilaze iz ljudskog stvaralaštva. To je taj nedostatak pravog prirodnog fenomena u kombinaciji sa odsustvom uređaja sticanja koji je virtualno motivisalo sve postojeće detektore kompjuterski generisanih slika.



Slika 2.5 Specifični ciljevi pasivno-slepe forenzike slike

Preciznije, kompjuterski generisane slike mogu biti detektovane analizom na bazi fizike karakteristika opšte scene, gde je radna pretpostavka da se projekcije kompleksnih realnih prirodnih fenomena teško sintetišu sa računarom. Softver prevođenja slikeje ograničen od prostog modela stvarnosti, koji treba držati računski poslušnim. Uopšteno, veruje se da digitalne slike prirodnih pojava pokazuju zajednička statistička svojstva nezavisno od stvarnog uređaja sticanja i opisane scene. Ovi statistički podaci prirodne slike uključuju na primer empirijskih mere, kao što su zakon snage i obima invarijantnosti , ili prostorno i međurazmerne korelacije. Kompjuterski generisane slike ne mogu u potpunosti

da budu u skladu sa ovim karakteristikama i tako postaju detektovane . Na signal nivou, softver prevođenja slike obično ne oponaša tačan lanac obrade uređaja za snimanje, što čini kompjuterski generisana slika detektabilne zbog nestalih karakteristika uređaja.

2.5.2 Otkrivanje izmenjenih slika

Jedan od osnovnih problema u digitalnoj forenzici slika je zaključiti da li je slika pod analizom izmenjena nakon inicijalnog sticanja. Na nivou signala, obrađeni artefakti mogu biti otkriveni testiranjem bilo za postojanjem obradno-specifičnih karakteristika ili zanepostojanjem ili nekonzistentnih karakteristike uređaja. Što se tiče ovog drugog, u literaturi je do sada bilo najviše zabrinutosti zbog ispitivanja tragova nastalih u fazi sticanja i samo nekoliko radova su se fokusirali na karakteristike izlaznog uređaja. Nepodudarnosti se mogu javiti i u inter i u intra karakteristikama i mogu postati posebno indikativni kada se delovi različitih slika kombinuju u jednu sliku. Prednost karakteristika uređaja preko obrađenih artefakata je da istraga uopšte nije ograničena samo na identifikaciji tragova posebnih procedura post-obrade. U isto vreme, međutim, karakteristike uređaja su samo u ograničenoj upotrebi za zaključivanje o kompletnoj istorijom prerade.

Obrađeni artefakti se takođe mogu detektovati na nivou scene proveravajući konzistentne opšte karakteristike scene. Međutim, analize na nivou scene danas obično zahtevaju znatno veći stepen ljudske interakcije (i tumačenja) od analize na nivou signala.Analize na nivou signala, zbog visoke praktičnosti i relativnom lakoćom automatizacije, tradicionalno dobijaju veći interes. Ipak, analize na nivou scene nude neke dodatne prednosti forenzičkom istražitelju. Prvo, izazovan je zadatak da se stvore manipulacije slike koje se uzimaju u obzir i da se ispraveprezasićenosti složenih karaktestika. Drugo, analize na nivou scena rade na višem nivou apstrakcije i često su usko vezani za ispitivanje (projekcija) pojedinačnih objekata. To dovodi do određenog stepena invarijantnosti za smanjenja post-manipulacija rezolucije slike i / ili kvantizacije-ili, uopšte, bilo kakve operacije za smanjivanje informacija, što će uticati na suptilno identifikovanje tragova na nivou signala.

2.5.3 Otkrivanje ponovo uslikanih slika

Slike koje su ponovo digitalizovane od dvodimenzionalnih proizvoda izlaznog uređaja (npr otisaka) suštinski se razlikuju od direktnih projekcija stvarnog sveta, prirodnih fenomena. Kao posledica toga, ponovo uslikane slike nisu podložneotkrivanju samo na nivou signala testirajući karakteristike izlaznog uređaja, ali i analizom karakterisitka opštih scena.Ovo poslednje se odnose na opšta svojstva štampanih ili prikazanih slika (na primer, obrazac površinske teksture) i čini detekciju ponovo uslikanih slika izuzetak u smislu da se već prisustvo određenih osobina scene smatra identifikovanjem tragova odgovarajućeg procesa generisanja slika. Ova nedoslednost u terminologiji se može izbeći tumačenjem re-digitalizacije kao oblik post-obrade i razumevanje ovih tragova kao posebnim oblikom prerađenih artefakta.

2.6 Testovi instanciranja komponenti

Sledi tekst u kome će biti opisana tehnika identifikacije uređaja i važnost te analize. Biće objašnjena Vremenska forenzika i zbog čega je značajna kao i koji su ciljevi kontra-forenzike.

2.6.1 Identifikacija uređaja

Cilj identifikacije uređaja je da se poveže slika pod istragom sa određenom akvizicijom ili izlaznim uređajem. Prvi problem se obično naziva identifikovanje izvora, gde je problem uglavnomštampača forenzike koji je dobio interes na izlaznoj strani. Po samoj definiciji, identifikaciji uređaja se uopšte prilazi sa analizom na bazi signala ili na bazi fizike odgovarajućih karakteristika uređaja. Napominjemo, međutim, da forenzika štampača, na način na koji se govori u literaturi, nije uvek slepi problem. Za forenzičkog istražitelja se obično pretpostavlja da ima u posedu analogni izlaz i ima potpunu kontrolu nad korakom ponovne digitalizacije (tipično je to, skeniranje visoke rezolucije). To je više problem računarske forenzike, gde ponovna projekcija u digitalnom domenu isključivo služi kao sredstvo za podršku forenzičke analize. Zbog toga, mislimo na Chiang za detaljan pregled relevantnih pristupa identifikacije štampača i fokusiramo se na identifikaciju izvora u narednom delu.

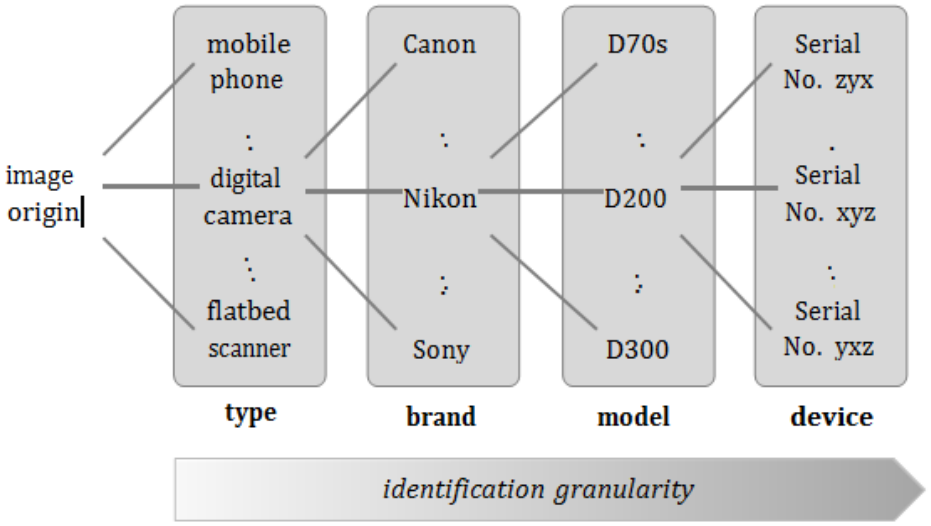
Iako je od glavnog interesa u teoriji, identifikacija samog uređaja nije uvek moguća iz praktičnih razloga. Pored situacija kada se ne zna za odgovarajuće identifikujuće tragove, sve postojeće metode zahtevaju pristup određenom uređaju koji treba da bude identifikovan, ili bar jednog broja referentnih slika dobijenih sa tim uređajem. Ako nisu ispunjeni svi ovi uslovi (tj, nema referentnih tragova uređaja koji su na raspolaganju), forenzički istražitelj može pribeći nižim nivoima identifikacije granulacija, kao što su model uređaja, marka ili tip (npr, potrošačka kamerom protiv signal-refleks kamere ili digitalni fotoaparat protiv ravnog skenera). Za razliku od identifikacije uređaja, nisko-granularni pristupi samo zahtevaju referentne tragove uređaja koji su reprezentativni za određene procese generisanja slika na datom nivou granularnosti. Na ovaj način, forenzički istražitelj može zaključiti bar neke informacije o poreklu slike. Empirijski rezultati iz literature, međutim pokazuju da se sa nijednom karakteristikom uređaja nemože napraviti razlika između nisko-granularnosnihi klasa sredstava za akviziciju. Praktična podešavanja mogu da stoga zahtevaju kombinaciju nekoliko karakteristika uređaja da bi suzili izbor određenog uređaj na najbolji mogući način.

Istorija obrade

Osim pitanja da li je slika pod analizom modifikovana, takođe je od interesa da se sazna kako je obrađena. Takva informacije je posebno koristna u proceni autentičnosti slike. Zaključivanje o istoriji obrade digitalnih slika podrazumeva da se odredi redosled post-obrađenih koraka koji su doveli do konačne slike, kao i parametrizacija odgovarajućih komponenti . To je uglavnom problem na nivou signala, jer analize na bazi scena može samo dati indikacije na visokom nivou (na primer, koja su objekti/delovi slike izmenjene).

Ako forenzički algoritmi za detekciju obrađenih slika ekploaitšu identifikaciju tragova određene vrste obrade, oni daju neke informacije o istoriji obrade slike. Ipak, potpuni oporavak istorije obrade je obično mnogo više uključen, jer identifikovanje tragova ranijih koraka obrade može biti promenjeno ili ublaženo kasnijim koracima u obradi. Kasnije, određenije pitanje proizilazi iz dvosmislenih obrađenih artefakata koji omogućavaju da se identifikuju određenu komponente za obradu , ali ne i njihova parametrizacija. Na primer, nekoliko parametara promene veličine su poznatida uvode ekvivalentne artefakte, ili mogu biti teško razlikovani od JPEG post - kompresije.

Još jednom se ističe da se otkrivanje proizvoljnih obrada slika i namernih manipulacija slika ne mora podudarati. Na kraju krajeva, forenzičari treba da naprave razliku između legitimne i nelegitimne post- obrade kako bi se procenila autentičnost slike. Dok bilo koji tip prerade može dovesti u pitanje autentičnost slika, ona traži tumačenje i razumevanje ako i kako je otkrivena obrada uticala na semantički smisao slike. Iako je od velikog praktičnog značaja, literatura je bila veoma neodređena u tom pogledu. Pojmovi kao što su " falsifikovanje", "ometanje" i " manipulacije" korišćeni su više ili manje kao sinonimi, ponekad pojačanietiketom “zlonamerno” da se bolje razlikuje obrada slike i manipulacija slike.



Slika 2.6: Nivoi identifikacije granuliteta u identifikacionom izvoru

2.6.2 Testovi povezanosti procesa generisanja

Pored analiza pojedinačnih slika, ispitivanje odnosa između velikog broja digitalnih slika u pogledu njihovih proizvodnih procesa može biti od interesa. Najvažnija su pitanja da li je grupa slika generisana korišćenjem istog ulaznog ili izlaznog uređaja, ili u kojim je vremenskim redosledima veliki broj datih slika izgenerisana.

2.6.3 Povezivanje uređaja

Testovi za zajedničke ulazne ili izlazne uređaje su poznati kao povezicanje uređaja. Slično identifikaciji uređaja, proučavano je pod pretpostavkom da će slike istog porekla izlagati zajedničke karakteristike uređaja na nivou signala. Scenario se razlikuje od obične identifikacije uređaja u odnosu tragoveskupa potencijalnih uređaja koji ne mora da se zna. Problem se prilazi ekstrakcijom odgovarajućih karakteristikama uređaja od jedne ili više slika, koje su zatim testirane protiv svih preostalih slika. Povezivanje urađaja je u suštini najteži zadatak: Referentni podaci u izvornoj identifikacijisu obično pouzdaniji (ili od većeg kvaliteta) jer su dobijeni pod kontrolisanim uslovima.

2.6.4 Vremenska forenzika

Cilj vremenske forenzike je da se uspostavi red jednog broja slika - obično stečene sa istim uređajem - u odnosu na vreme njihovog generisanja. Preciznije, možemo razlikovati dva scenarija u zavisnosti od toga da li su se slike napravile nezavisno jedne od drugih, ili se pretpostavlja da su sve slike obrađene verzije jedni drugih. Neophodan uslov za prvi scenario je da se određene karakteristike uređaja razvijaju tokom vremena, i da su odgovarajući referentni tragovi barem u jednom trenutku na raspolaganju. Kako je istaknuto od strane Fridriha i Goljana, pogodni identifikujući tragovi su najverovatnije slični zbog neželjene nesavršenosti uređaja i nosećih efekata koji nisu deo procesa generisanja po dizajnu. Drugi scenario je u tesnoj vezi sa određivanjem istorije obrade. U izvesnoj meri ovaj problem nije slep, jer forenzički istražitelji posmatraju srednje rezultate procesa generisanja slika, međutim, ne znajući kako se oni odnose jedni prema drugima.

level of analysis	CG detection	detection of processing	detection of recapturing	source identification	processing history	printer forensics	temporal forensics	device linking
semantics	(×)	×			(×)		(×)	
physics	×	×	×	×	×	×	×	×
signal	×	×	×	×	×	×	×	×
metadata	×	×	×	×	×		×	×

Tabela 2.1: Odabrani ciljevi pasivno-slepe forenzike slike i važni aprstaktni slojevi

Treba imati na umu da poznate analize na bazi signala i na bazi fizike ne mogu da odrede tačno vreme generisanja slike , već nagoveštavaju na mogući vremenski interval. Tačnoodređenje vremena je moguće samo sa dodatnim informacije o stvarnom svetu (bilo zbog semantičkih informacija ili suptilnih tragova prirodnih pojava sličnih frekvencijom električne mreže u digitalnom video i audio analizu), ili podrškom za metapodatke.

2.7 Rezime

Tabela 2.1 sumira prethodne dve sekcije i navodi različite specifične ciljeve pasivno- slepe forenzike slike zajedno sa odgovarajućim relevantnim nivoima analize. Za potpunost, napominjemo da metapodaci mogu pratiti analize na bazi signala i fizike u gotovo svim gore navedenim diskusijama o problemima sa izuzetkom štampane forenzike. Čista semantička analiza, s druge strane, je jedino održiva u pogledu otkrivanja obrađenih artefakata. U posebnim slučajevima, ona takođe može izložiti kompjuterski generisane slike zbog nerealnog sadržaja. Ili može otkriti informacije o vremenu sticanja (npr, kada je prikazan kalendar ili sat).

2.7.1 Specifični ciljevi kontraforenzike

S obzirom na Harisovu široku definiciju kontra- forenzike, jasno je da su napadi kontra –forenzike relevantni za svaki od gore navedenih specifičnih problema u digitalnoj forenzici slike. Međutim , to nije naša namera da ponovimo svaki detalj iz perspektive falsifikatora. Falsifikator na kraju teži da je falsifikata koji se pojavljuje pouzdan ida ne podiže sumnju za forenzičkog istražitelja. Ovo se svodi na dva glavna cilja koja falsifikator može ostvarivati:
-suzbijanje identifikacionh tragova, ili
-sinteza veštačkih identifikacionih tragova.

Tabela 2.2 pokazuje da se suzbijanje i sinteza mogu odnositi na ili karakteristike uređaja ili preradu artefakata.

	suppression	**synthesis**
device characteristics	hide image origin	forge image origin; remove processing-related inconsistencies
processing artifacts	hide traces of processing	remove processing-related inconsistencies

Tabela 2.2: Specifični ciljevi kontra-forenzike

2.7.2 Suzbijanje i sinteza osnovnih karakteristika uređaja

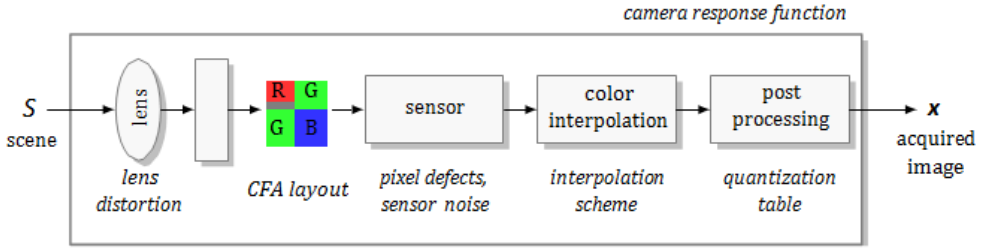
Karakteristike uređaja dozvoljavaju forenzičarima da poveže sliku pod istragom za određeni uređaj ili klasu uređaja. Falsifikatori, koji žele da sakriju poreklo slike, će pokušati da suzbije relevantne karakteristike uređaja, tako da forenzička analiza slike ne otkrije koji uređaj je deo procesa generisanja slika Napadi protiv prevara identifikacija uređaja mogu dalje imati za cilj da falsifikuju poreklo slike, tj., pustiti da slika izgleda kao

da je generisana korišćenjem uređaja koji se razlikuje od prvobitnog. Ovde, falsifikator ne treba samo da suzbije tragove pravog uređaja, ali takođe treba da sintetiše tragove ciljnog uređaja. Ovaj tip napada se obično smatra težim, jer to može dovesti do lažne optužbe u vezi sa vlasnikom lažnog uređaja.

Sinteza karakteristika uređaja je takođe element u stvaranju mogućih manipulacija slike. U očekivanju forenzičara koji testiraju za dosledno prisustvo određenih karakteristika uređaja, falsifikatori moraju da uklone nedoslednosti u vezi obrade. Oni to čine sintezom relevantnih karakteristika uređaja, koji se odnose na ili original ili potpuno novi uređaj.

2.8 Suzbijanje i sinteza obrađenih artefakta

Kontra - forenzički napadi sa ciljem da se prikriju tragovi post - obrade ne samo da treba da se uvere da se karakteristike uređaja pojavljuju konzistentnima, već će morati da suzbiju obradu artefakata u celini. Često, ovaj prilično strogi uslov je opušten "zamenom" upadljivih sa verodostojnim obrađenimartefaktima, na primer eksploatišući gubitke JPEG kompresije. Na ovaj način, suptilni, a ipak govoreći tragovi ranijih manipulacija su zbrisani, a uspostavljene navike sugerišu da očigledni JPEG artefakti nisu sami po sebi presudni u mnogim situacijama.



Slika 2.7: Obrađeni cevovod digitalne kamere. Relevantni identifikujući tragovi su štampaju u Italiku.

Napominjemo da postoje i situacije u kojima je sinteza obrađenih artefakta održiva. Uzmimo, na primer, manipulaciju gde je promenjenaveličina samo delovima slike da bi promenila semantički smisao slike. Jer, menjajući svoju veličinu - ako se primenjuje na celoj slici - može ne narušiti autentičnost, kontra - forenzički napad može pokušati da sintetiše tragove promena veličine u preostalim delovima slike (bez zapravo premene veličine ovih delova). Uklanjanjem ovakvih nedoslednosti u vezi obrade, cela slika se konstantno pojavljujesa promenjenom velilčinom i na taj način sakriva manipulaciju.

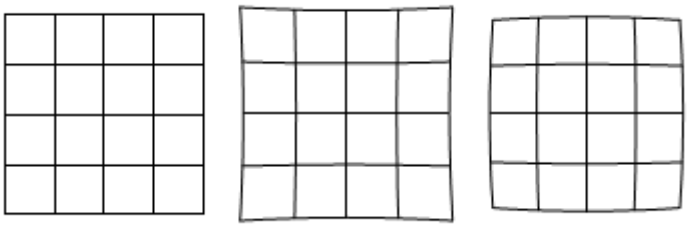
2.8.1 Odabrani identifikujući tragovi

Zatvaramo ovo poglavlje sa kratkim neformalnim pregledom nekih od najvažnijih karakteristika uređaja i obrađenih predmeta koji su pronašli primenu u literaturi. Namera ovog dela je da ne da detaljno izlaganje konkretnih forenzičkih algoritama, već da diskutuje o opštim karakteristikama za identifikaciju tragova koje ovi filter algoritmi mogu iskoristiti.

2.8.2 Karakteristike uređaja

Komponente uređaja za slikanje i izlaznih uređaja, ostavljaju karakteristične tragove u nastalojslici. Testiranjem na prisustvo i doslednost ovih karakteristika uređaja u datoj slici pod analizom, forenzički istražitelji zaključuju o detaljima o poreklu slike i njenoj autentičnosti. Fokusiramo se na karakteristike uređaja, a posebno na digitalnih fotoaparata. S obzirom na njihovu široku primenu u svakodnevnom životu, ovaj tip uređaja su dobili najviše interesovanja u literaturi. Ipak,o mnogimod karakteristika uređaja ćemo raspravljati u nastavku, oni takođe imaju svoje mesto u forenzičkim pregledima drugih vrsta uređaja, ravnim skenerima. Mi ćemo pomenuti relevantne razlike kada će to biti potrebno. Pozivamo zainteresovane čitaoce da prouče Chianga za sveobuhvatni pregled karakteristika skenera.

Slika 2.7 prikazuje stilizovanu obradu cevovoda tipičnog digitalnog fotoaparata sa svojim najvažnijim komponentama. Dolazeća svetlost scene se fokusira na senzor sistemom sočiva. Optički filter je umetnut između ovih komponenti da se smanje neželjene svetlosne komponente (npr infracrvena svetlost). Tipični digitalni senzori slike snimaju piksele slika po posebnim CCD ili CMOS senzornim elementima koji hvataju dolazeće svetlosti i izlaze električnog naboja proporcionalnih svetlu na toj lokaciji. Iako se kamere digitalne slike obično sastoje od tri boje kanala crvene, zelene i plave (RGB), sam senzor je daltonista, jer jedino može meriti intenzitet svetlosti. Da bismo dobili sliku u boji, ogromna većina digitalnih fotoaparata zapošljava niz filtera u boji (CFA), tako da svaki element senzora samo zapisuje svetlo u određenom opsegu talasnih dužina. Preostala informacija boja se onda procenjuje iz okolnih piksela sirovog slike (nakon eventualne pred-obrade i belog balansiranja). Ovaj proces se obično naziva interpolacijaniza filtera u boji ili upošljavanje. Nakon CFA interpolacije, slika je podlegnuta nekolikimpost-obradnim kamerna-internim koracima, uključujući korekcije boje, ivica pribora, i na kraju kompresije.



Slika 2.8: Radijalna distorzija objektiva omogućava početnim pravim linijama da se javljaju zaobljene na slici. S leva na desno: idealna pravougaona mreža, i ista mreža koja je predmet bureta i distorzija jastučića za čiode, respektivno.

2.8.3 Distorzija objektiva

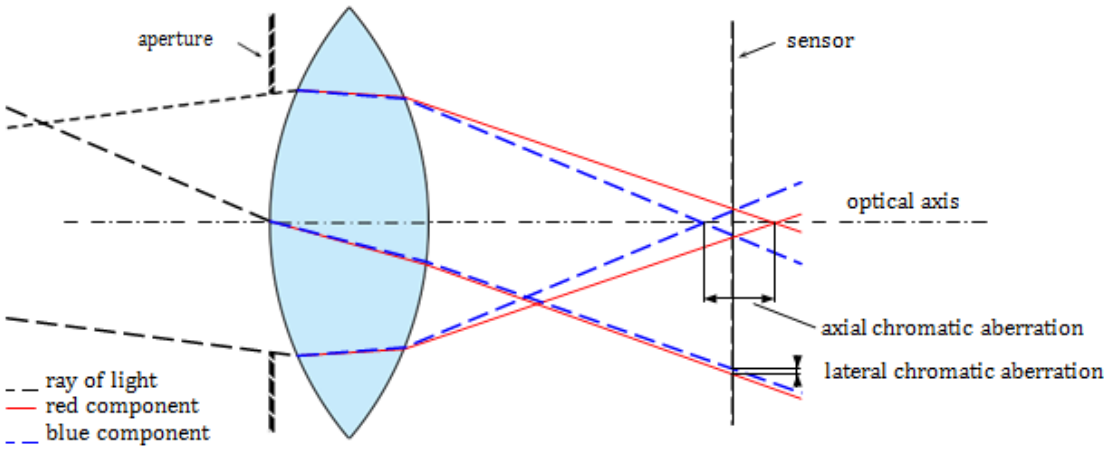
Svaki digitalni fotoaparat je opremljen sa složenim optičkim sistemom koji projektuje scenu do senzora od mnogo manjih dimenzija. Ova projekcija u celini nije savršena i mnoštvo distorzija objektiva (ili aberacija) mogu se naći u digitalnim slikama i pored velikih napora proizvođača objektiva i kamera.

Zbog toga što različiti modeli kamera koriste različite optičke sisteme, koji svi imaju svoj individualni profil distorzije, ove aberacije mogu da posluže za identifikovanje tragova specifičnog modela fotoaparata. Čoi je prvi taj koji je predložio da se iskoristi

radijalna distorzija objektiva u forenzičkom kontekstu. Radijalna distorzija objektiva je nelinearna geometrijska distorzija koja omogućava početnim pravim linijama da izgledaju zakrivlje. U principu, možemo praviti razlikuizmeđu buretadistorzije jastučića za čiode, dok oblik i jačina zavise od konkretnog objektiva u upotrebi.

Van je napravio slične napore u vezi sa analizom hromatskih aberacija, koje se javljaju zbog varijacija specifičnog sočiva u indeksu disperzija za svetlosne komponente različitih talasnih dužina. Ovo , po Snelovom zakonu, izaziva polihromatski zrak svetlosti koji se prostire na različitim pozicijama u ravni senzora. Ovde, osno-hromatska aberacija se odnosi na longitudalne varijacije zavisne od talasne dužine uzdužne kod ključne tačke duž optičke ose, dok bočna hromatska aberacija objašnjava van - osna raseljavanja različitih svetlosnih komponenata u odnosu jedne na druge. Iako je često ignorisano od strane gledaoca, posebno bočne hromatske aberacije su vidljivi deo skoro svakog digitalnog fotoaparata, gde se manifestuju u boji duž ivica.

Vinjetiranje je još jedna od vidljivih distorzija sočiva koje opisuje radijalno smanjenje intenziteta svetlosti prema uglovima slike. Kao i kod hromatskih aberacija, za njegovu pojavu severuje da je karakteristična za optički sistem zaposlen od strane modela fotoaparata i na taj način dovodi do primene u identifikaciji izvora.



Slika 2.9: Formiranje osovinskih i bočnih hromatskih aberacija zbog varijacija u disperzionom indeksu objektiva za svetlosne komponente različitih talasnih dužina. Ova figura je preuzeta i predstavlja složeni optički sistem stvarnih digitalnih fotoaparata u stilizovanom načinu kao jedan objektiv.

Opšti utičući faktor na pojavu i snagu većine distorzija sočiva širom različitih regiona slike je (radijalna) udaljenost do optičkog centra slike. Dakle, kao je prvo detaljno objašnjeno po Džonsonu i Faridu za određeni primer hromatske aberacije, manipulacije slikamogu dovesti dointra-karakterističnih nedoslednosti kada se delovi slike zamene sa delovima slike sa neusaglašenim lokalnim profilu distorzije. Slika 4.10 daje konkretan primer i ilustruje kako bočne hromatske aberacije variraju u zavisnosti od položaja na slici. Nedavno , Yerushalmi i Hel - Orsu proširili ovo zapažanje da se tzv ljubičaste iskrivljene aberacije (FPA), pripisuju (između ostalog) mikro-sočivima ispred pojedinih elemenata senzora.

2.8.4 Nedostaci senzora

Ne samo da optički sistem nosi nesavršenosti, ali i senzor u procesu pretvaranja dolazećeg svetla za digitalnu sliku. Nesavršenosti senzora izazvane promenama u procesu proizvodnje i habanje senzora su na dnevnom redu forenzičara od samog početka.

Preciznije, svaki senzor uvodi određenu količinu smetnji u dobijenojslici - neznatnih oscilacija u intenzitetu pojedinačnih piksela čak i kada je senzorni prostor upaljen apsolutno homogeno. Senzor smetnje uglavnom svrstava u vremenskom smetnje i prostornesmetnje. Komponente smetnji koje se stohasticki nezavisne u različitim aktiviranjima procesa generisanja slika pripadaju prvom tipu, sa smetnjom snimka i read-out smetnje kao tipičnim predstavnicima. Naprotiv, prostornesmetnjesu relativno stabilne tokom vremena i variraju samo preko pojedinih elemenata senzora. Ovo čini prostornesmetnje posebno zanimljivim forenzičara jer ne samo da mogu da posluže kao "otisak prsta" određenoj digitalnoj kameri, ali se takođe mogu testirati za doslednopojavljivanje širom slike. Glavne komponente prostornihsmetnji su foto-odgovorio ne-uniformnost (PRNU) i tamne struje. PRNU je multiplikativni šum koji je uzrokovan razlikama u kvantnoj efikasnosti pojedinih elemenata senzora zbog neizbežnih varijacija u svom proizvodnom procesu. Tamna struja je termalni efekat, što za posledicu ima slobodne elektrone, čak i ako senzor nije izložen bilo kakvoj svetlosti. Ipak, njegova relativna snaga zavisi od pojedinačnih elemenata senzora.



Slika 2.10: Bočne hromatske aberacije u digitalnoj kameri u obliku crvenkaste boje duž ivica, koje su označene crvenim strelicama na uveličanim (i uvećane u kontrastu) detaljima na desnoj strani. Pojava i snaga tih boja ruba uopšte varira u zavisnosti od položaja odgovarajuće ivice na slici (ovde, one se samo pojavljuju na ivicama okrenutim dalje od centra slike). Originalna slika jedne Apple MacBook Pro tastature je napravljenasa Nikon 18-200 mm zumom pri žižnoj daljini od 150 mm.

Standardni model različitih izvora smetnji je dat u sledećoj jednačini gde senzor funkcije: $R^{MN} \rightarrow ¥^{MN}$ mapira dolazeće svetlo **s** u sirovu digitalnu sliku **r**:

$\boldsymbol{r}$=sensor($\boldsymbol{s}$)=$g^{\gamma}\boldsymbol{\kappa s}+\boldsymbol{\eta}^{\gamma}+\boldsymbol{v}$.

Multiplikativni PRNU je predstavljen vektorom **k** , dok $\boldsymbol{\eta}$ podvodi razne aditive u smislu smetnji (uključujući tamne struje ,smetnje slikanja i očitavanje smetnji) , a $\boldsymbol{v}$ označava kvantizaciju smetnji. Skalari **g** i **y** su fiksni parametri fotoaparata koji kontrolišu dobitak faktor i gama korekciju izlaznog signala.

Već Heerich, 1998. godine, aludira na upotrebu senzora smetnji kao sredstvo da se identifikuje specifian uređaj koji slika (faks mašina u konkretnoj studiji). Revolucionarna istraga o korišćenju tamne struje i odziva slike i neuniformnosti od Kurosave i Fridricha, je od tada motivisala veliki broj pratećih studija o identifikaciji uređaja na bazi smetnji. Pošto je izlazni senzor predmet za dalju obradu unutar uređaja, što je verovatno da ometa suptilne karakteristike smetnji, senzor za smetnju bi idealno bio ispitan na osnovu sirovog izlaznog senzora. Na primer, nakon interpolacije filtera boja, integracijom nekoliko susednih elemenata senzora, utiče na karakteristike smetnji pojedinačnih piksela. Empirijski rezultati pokazuju, međutim, da u posebnom PRNU je veoma indikativan identifikujući trag u proizvoljnim digitalnim fotoaparatima, koji čak može da preživi ciklus štampanje – skeniranje.

Odziv slike i neuniformnost su nakođe našli primenu u ispitivanju skeniranih slika. Evo, tipičan senzor linija skenera ponavlja prostorne karakteristike smetnji duž redova. Ovo omogućava forenzičarima da naprave razliku između slika digitalnog fotoaparata i skenirane slike. Dalje treba napomenuti da ne samo prisustvo specifičnog obrasca smetnji, ali i više opšte karakteristike kao što su relativne snage i statističke distribucije senzora smetnji mogu da posluže kao tragovi za identifikaciju u forenzičkim podešavanjima.

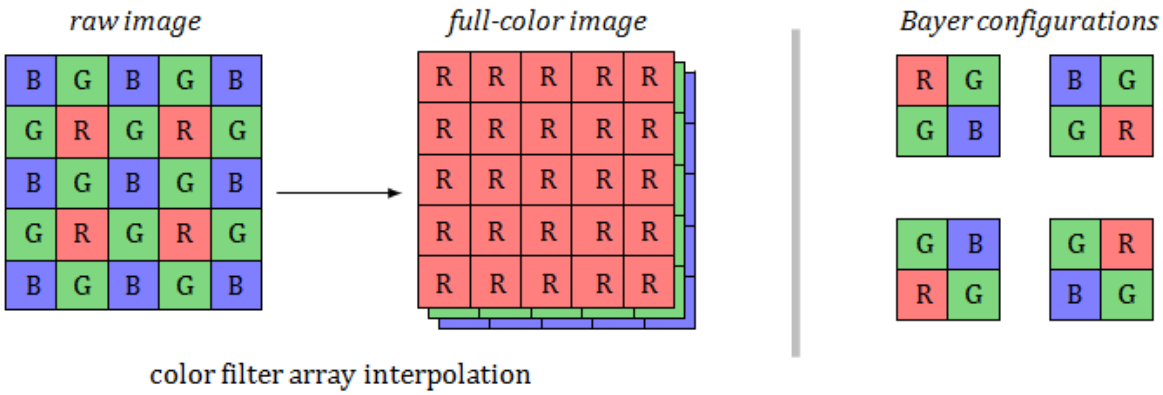
Osim smetnji senzora, mane senzora su još jedna nesavršenost senzora od forenzičkog značaja. Mane senzora se odnose na elementesenzora koji konstantno isporučuju suviše visokeili niske vrednosti intenziteta. Pojava i položaj ovih nedostataka su ponovo specifične za individualni digitalni fotoaparat i akumuliraju tokom vremena, koji takođe dovode do primene u vremenskoj forenzici. Sličan efekat je uzrokovan česticama prašine na senzornom zaštitnom staklu. Ova vrsta identifikacije tragove je uglavnom prisutna u fotoaparatima sa izmenljivim objektivima. Ipak, i senzorni nedostaci i čestice prašine mogu se relativno lako korigovati. U principu, njihova pojava u velikoj meri zavisi od sadržaja slike i podešavanja sočiva, što ove karakteristike uređaja čini manje pogodnim za opšte namene forenzičke analize.

2.8.5 Karakteristike niza filtera u boji

Zato što senzor može samo meriti intenzitet dolaznog svetla, generisanje slike u boji zahteva da se svetlo razdvoji svojim odgovarajućim komponentama (obično crvene , zelene i plave). Većina dizajna digitalnih fotoaparata kombinuju jedan senzor sa nizom filtera u boji, tako da različiti uzorci sirovog signala predstavljaju različite informacije u boji. Informacije koje nedostaju o boji se zatim dobijaju iz procedure demosaicing.

Poseban način kako su ovi filteri boja uređeni se naziva CFA konfiguracija. Različiti modeli koriste različite kamere CFA konfiguracije, čineći ovaj parametar vrednom karakteristikom uređaja u forenzičkoj analizi digitalnih slika. Iako, u teoriji, konfiguracija CFA nije ni zabranjena za snimanje isključivo crvene (R) , zelene (G) i plave (B) komponente, niti je ograničena na određeni raspored, često je jedan od četiri 2 × 2 Baier Obrazac koji se ponavljaju celoj ravni slike. Ovde, dva zelena elementa su

raspoređeni u dijagonali i svaki crveni i jedan plavi elemenat popunjuju preostali prostor.



Slika 2.11: Tipični digitalni fotoaparati koriste niz filtera u boji (obično jedan od četiri Baier konfiguracije prikazane na desnoj strani). Svaki element senzora beleži samo svetlost određene talasne dužine (ovde crvene, zelene i plave). Slika u puno jboji dobija se interpolacijom preostale informacije boja od okolnih piksela sirove slike.

Demosaicing podrazumeva da samo najviše jedna trećina svih piksela u RGB slici sadrže iskrenu informacije iz senzora elemenata. Preostali pikseli interpoliraju iz susednih uzoraka sirovog signala,
$\boldsymbol{x}$ˆ = demosaic .$\boldsymbol{r}$, $\boldsymbol{C}$., gde je funkcija demosaic: ¥^{MN}×{R,G,B}^{MN} →¥^{3MN} je demosaic algoritam.

Matrica **C** je od dimenzije M × N i predstavlja konfiguraciju filtera boja niza, a $\hat{\boldsymbol{x}}$ je demosaiced slika u punoj boji. Posledica KFA interpolacije je da susedni pikseli postaju visoko međuzavisni i , kao što su prvi spomenuli Popescu i Farid, redovno struktura tipičnih CFAs dovodi do periodičnih varijacija tokom cele slike. Ho je dalje dodao da se slični zavisnosti javljaju između različitih boja kanala slike. Post-obrada može zbrisati ove tragove i na taj način dovodi do nedoslednosti instra karakteristika. Ipak, potpuno odsustvo CFA artefakata takođe može biti pokazatelj slike koja nije slikana sa kamerom.

Konkretna forma demosaicing zavisnosti između piksela ne zavisi samo od konfiguracije CFA, ali i od demosaicing algoritma. Ovo zapažanje je motivisalo Bajrama i Svaminathana, između ostalog, da razumeju takve karakteristike kao identifikacione tragove od konkretnog modela fotoaparata, ili, kako kažu Cao i Kot, od sirovog softvera za obradu slika koji se koristi za kreiranje konačne slike.

2.8.6 Karakteristike JPEG kompresije

Nakon KFA interpolacije, demosaiced slika prolazi kroz veliki broj obradivih koraka unutar uređaja, x = procesa (xˆ) , proces: ¥ 3MN → ¥ 3mn . Sa stanovišta forenzičara, JPEG kompresija je među najvažnijim od ovih procedura zbogtri razloga. Prvo, JPEG je kvazi - standard za skladištenje slika digitalnih fotoaparata, jer nudi

potrošačima razumni kompromis između vizuelnog kvaliteta i veličine datoteke. Drugo, zbog gubitaka karaktera, JPEG će verovatno da ublaži neke od karakteristika uređaja prethodnih komponenti uređaja. Konačno, JPEG kompresija uvodi svoje identifikacione tragove, koji mogu biti testirani i za postojanje i doslednosti. Ovi tragovi su od posebnog interesa jer je JPEG kompresija obično poslednji korak u lancu obrade u kameri, samo post-obrada van fotoaparata može ugroziti njihovo postojanje.

JPEG kompresija radi tako što sliku razdvaja u nepreklapajuće blokove x_{ij} od 8x8 piksela, gde x_{ij} označava i-vektorisan blok. Svaki blok se predstavla u dvodimenzionalnojdiskretnoj kosinusnoj transformaciji (2D - DCT) da bi se dobilo 64 DCT koeficijenata, $c_{ij}=(c_{ij}1,...,c_{ij}64)$, koji se zatim kvantiziraju koristećispecifični koeficijent faktorakvantizacije, $\dot{q}j, 1\leq j\leq 64$. Snaga kompresije je kontrolisana od strane niza kvantizacionih tabela koje su sačuvane sa JPEG slike. Farid navodi da su ovetabele dobar pokazatelj digitalnog modela fotoaparata. Proizvođači kamera su slobodni da fino podese kvantizacionetabele u skladu sa svojim željama, a samim tim i veliki broj različitih tabela može se naći u divljini. Ki dalje napominje da nijedan model kamere izgleda ne deli tabele sa široko upotrebljivim alatom Photoshopom za obradu slika.

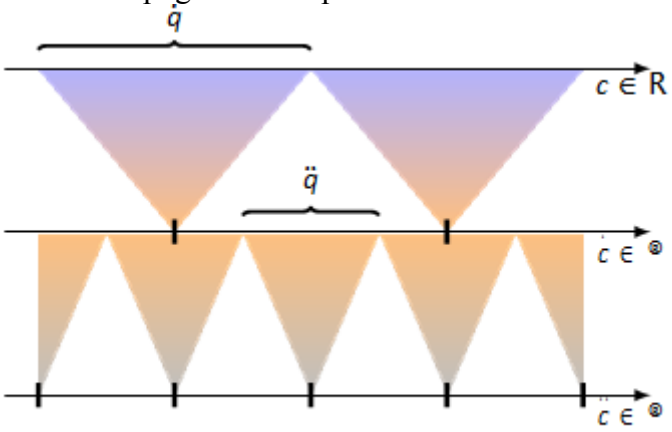
Po samoj definiciji, kvantizacija JPEG kompresije cevovoda utiče na distribuciju DCT koeficijenata. Posebno, kvantizacija uvodi praznine u histogram DCT koeficijenata , dok širina ovih praznina zavisi od faktora kvantizacije , q_j (na odgovarajućojm tabeli kvantizacije). Ako se ovaj ' JPEG otisak prsta ' nalazi u slici koja je u formatu koji ne gubi na kvalitetu, slika je vrlo verovatno JPG kompresovana pre. Distribucija DCT koeficijenata je dodatno uticalo obradom artefakata zbog dodatnih koraka kvantizacije (izvan uređaja) . Na primer, poseban slučaj dvostruke kompresije sa kvantizacionih faktorima q_j i q_j nameće sledeći odnos za j DCT koeficijente i bloka :

$$c_{ij} = q_j \left\lfloor \frac{c_{ij}}{q_j} + 1/2 \right\rfloor q_j \left\lfloor \frac{c_{ij}}{q_j} \cdot \frac{q_j}{q_j} + 1/2 \right\rfloor,$$

gde c_{ij} i d_j označavaju dekvantizaciju DCT koeficijenta nakon prvog i drugog koraka kompresije. Karakteristični vrhovi i nedostaci se javljaju u odgovarajućem histogramu u zavisnosti od specifične kombinacije kvantizacionih faktora. Ovo se može eksploatisati da se otkriju slike koje su ponovo sačuvane kao JPEG više puta. Slika 2.12 ilustruje ovaj efekat za posebno indikativni slučaju kada je drugi kvantizacioni fasktorje polovina prvog kvantizacionog faktora, $q' = 2q''$. Tipičan primer histograma dvostruko-kvantiziranih DCT koeficijenata je prikazan naslici 4.13. Lukaš i Fridrih su prvi primetili da takve karakteristike histograma multi-kvantizacionih DCT koeficijenata dozvoljavaju da se zaključi okvantizacionim tabelama ranijih JPEG kompresionih koraka (npr tabela u uređaju kompresije). To je dovelo do velikog broja povezanih studija. Lokalne nedoslednosti zbog tragova multi-kompresije mogu dalje da služe kao pokazatelj lokalizovane post-obrade.

Jer se svaki 8 × 8 blok transformiše odvojeno, JPEG kompresija dovodi do poznatih (i često vidljivih) blokirajućih artefakata u prostornom domenu. Slično DCT karakteristikama koeficijenta histograma, takvi tragovi mogu nagoveštavati da prethodno JPEG kompres slike se nalaze u formatu bez gubitaka . Blokirajući artefakti mogu takođe biti testiraniza doslednost.

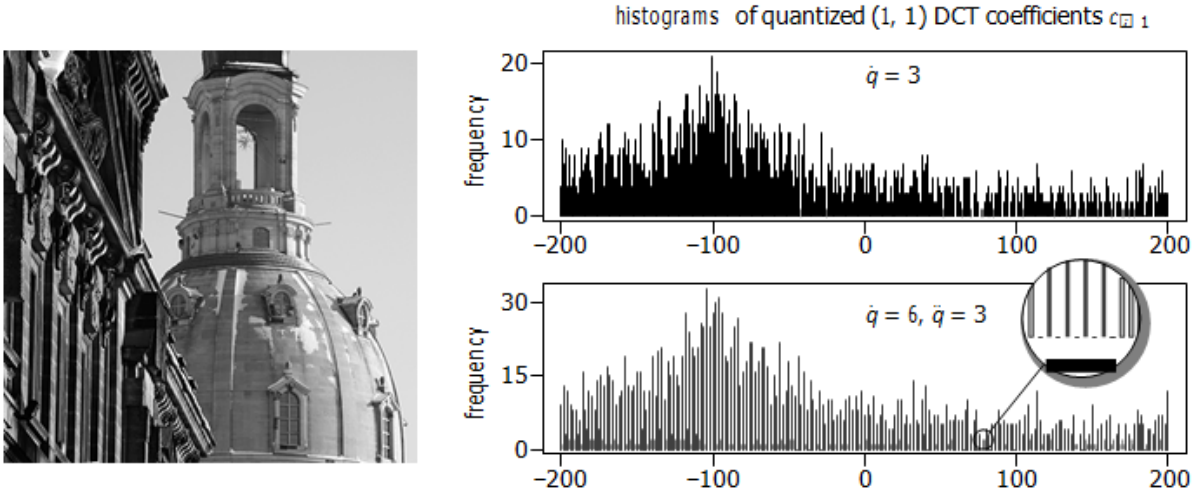
Može doći do nedoslednosti, na primer, ako su delovi (prošle) JPEG slike obrađeni ili zamenjeni nekompresovanom zakrpom. Osim toga, kombinacija dve ili više JPEG slika može dovesti do nedosledne blok granice kada postupak deljenja ignoriše regularnu 8 × 8 rešetku i stavi pogrešne zakrpe.



Slika 2.12: Formiranje praznina u DCT histogramu koeficijenta posle duple kompresije sa $q^{\cdot} = 2q^{\cdot\cdot}$.

U prvom koraku kompresije, realno vredni koeficijenti **c** su mapirani na celih $\mathring{c}$koji su sadržatelj sa odgovarajućim faktorom $q^{\cdot}$ kvantizacija . U drugom koraku kompresije, svaka drugisadržalac kvantizacionog faktora$q^{\cdot\cdot}$nema nijednu odgovarajuću ulaznu vrednost. Zasenčeni trouglovi vizuelizaciju koeficijent intervala koji se kvantizuje do sam diskretne vrednosti.

Na opštijem nivou, artefakti kvantizacije nisu ograničeni na konkretnom slučaju JPEG kompresije na osnovu 8 × 8 blokova slika. Različiti izvorni koderi mogu da se razlikuju u veličini blok i zadatom transformišućem domenu i na taj način da predstave svoje identifikacione tragove.



Slika 2.13: Dvostruko kvantizovani DCT koeficijent

2.8.7 Obrađeni artefakti

Post-obrada se ne može otkriti samo pomoću nedoslednihe ili nestalih karakteristika uređaja, ali i zbog specifičnih predmeta za obradu koje pojedini primitivci obrađenih slika ostavljaju iza u dobijenoj slici. Dok prošla ima prednost što je relativno nezavisna od stvarnog oblika post- obrade, druga dozvoljava ciljanu analizu pojedinih klasa post-obrade. Ovo može da obezbedi forenzičarima dodatne informacije o istoriji obradu slike pod analizom. Shodno tome, jedan broj specifičnih predmeta za obradu su dobili interesovanje u literaturi, od kojih će se o tri razgovarati detaljnije u nastavku.

2.8.8 Manipulacije kopiranja – pomeranja

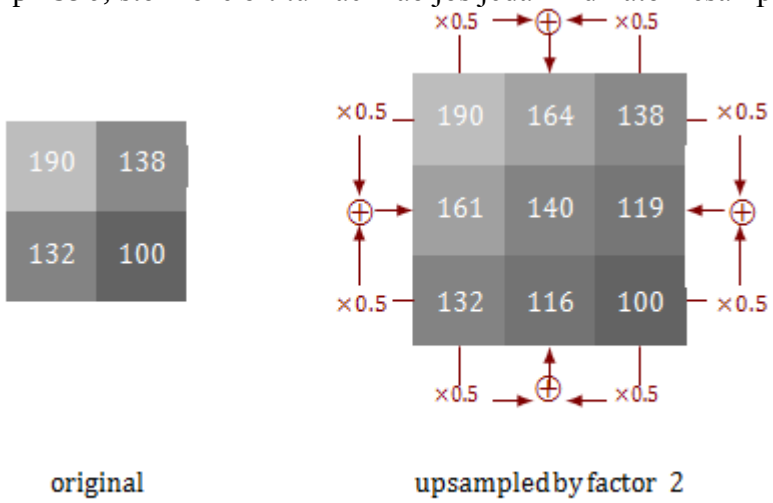
Među velikom klasama za obradu predmeta, tragovi manipulacija kopiranja i pomeranja su dobili poseban interes u literaturi. Manipulacija kopiranja i pomeranja kopira deo slike da bi ih dodala u drugi deo iste slike, obično sa ciljem da se prikrije ili naglasi detalj originalne slike. Slika 2.14 daje tipičan primer i prikazuje manipulaciju kopiranja i pomeranja na slici jednog iranskog raketnog testa . Po samoj definiciji , manipulacija kopiranja i pomeranja uvodi duple regije na rezultirajućoj slici . Fridrih je bio prvi da shvati ovo kao identifikujući trag u forenzičkom kontekstu. Autori takođe pomenjuju da forenzički istražitelji, u realnijem okruženju,radije susreću gotovo duplirane slike regiona. Prvo, kopiranu regiju često treba dodatno obrađivati kako bi se bolje uskladila sa okolinom sadržaja slike. Drugo, izmanipulisana slika će često biti JPG kompresovana pre objavljivanja. Ovo zapažanje je dovelo do mnoštvo detektora kopiranja-pomeranja, što se u suštini sve razlikuju samo u definiciji “skoro duplikat”. Konkretni slučajevi uključuju, na primer, detekciju zamućenih regiona ili tzv otrovno kloniranje. Potonji prinosi posebno privlačnu manipulaciju mešanjem granica kopiranog regiona fleksibilnog njegovom susedstvu. Konačno, opštiji oblik manipulacije kopiranja-pomeranja može da sadrži i geometrijsku transformaciju (npr , skaliranje ili rotaciju) kopiranog regiona. Pozivamo se na dva nedavna istraživanja od Christlein za sveobuhvatan pregled relevantnih pristupa za detekciju kopiranja-pomernaja.



Slika 2.14: Tipičan primerak manipulacije kopiranja-pomeranja, primenjen u saopštenju fotografa iranskog raketnog testa. Nefunkcionišuća raketa u pretpostavlja se originalnoj slici(prikazanoj na levoj strani) je zamenjena kopijom drugerakete (sredina). Izmanipulisana slika se pojavila na naslovnoj strani jednog broja glavnih zapadnih novina. Desna slika prikazuje rezultat Popeskovog and Fairdovgdetektora kopiranja-pomeranja i oznake skoro dupliranih regiona.

2.8.9 Resamplovanje

Ne samo manipulacija kopiranja-pomeranja često zahteva delovi digitalne slike da se promenei ili rotiraju kako bi se bolje uskladili sa ostatkom sadržaja slike. Generalno, sve geometrijske transformacije-bilo primenjena na specifičnom regionu slike ili slike u celini-je od interesovanja kada se zaključuje o istorijiobrade slike ispod analizom. Tehnički, geometrijska transformacija se može opisati kao resampling mreže originalne slike na novu mrežu slika. Interpolacija je ključ za glatku i vizuelno privlačnu transformacije. Međutim, gotovo neizbežan sporedni efekat interpolacije je da se uvode linearne zavisnosti između grupa susednih piksela. Popesku i Farid i Gallagher su prvi put shvatili da ove zavisnosti periodično variraju u slici i na taj način se može razumeti kao identifikovanje tragova prethodne resampling operacije. Dužina perioda u generalnom zavisi od parametara transformacije koji omogućavaju zaključak o konkretnoj transformaciji koja se primenjuje na slici. Slika 2.15 prikazuje formiranje periodičnih linearnih zavisnosti za posebno indikativne slučajeve nadogradnjom za da faktora koristeći bilinearnu interpolaciju. Kasnije je napomenuto da resampling takođe ometa karakteristike prethodne JPEG kompresije. Preciznije, geometrijska transformacija ne samo preslikava samu sliku na novu mrežu slika, ali i utiče na oblik postojećih JPEG blokirajućih artefakata. U navedenom primeru nadogradnja sa faktorom dva,transformisani "JPEG blokovi" će imati veličinu 16 × 16 umesto 8 × 8 piksela, što može bititumači kao još jedan indikator resamplinga.



Slika 2.15: Nadogradnja 2 × 2 bloka (slika levo) sa faktorom dva koristeći bilinearnu interpolacija (desno). Pikseli u svakom drugom redu (ili koloni) su linearne kombinacije njihovih direktnih vertikalnih (ili horizontalnih) komšija. Jer slika sa promenjenom veličinom se sastoji od velikog broja takvih blokova, periodične linearne zavisnostise javljaju.

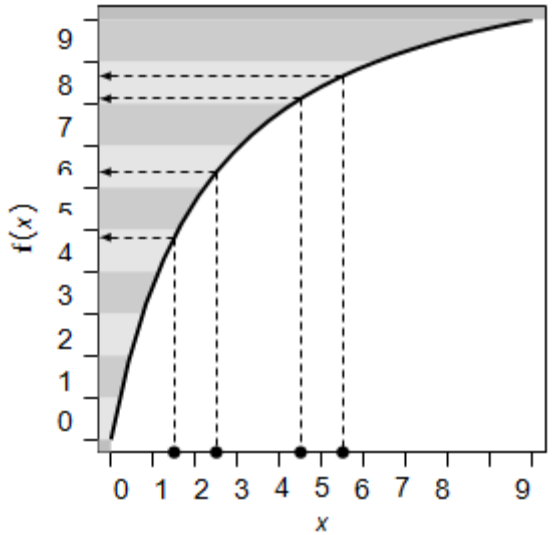
2.8.10 Poboljšanje kontrasta

Naš poslednji primer posebnih obrađenih predmeta se odnosi na identifikaciju tragova opšte klase intenziteta piksela mapiranja: $x_i \rightarrow [f(x_i)+1/2]$, gde je f: ¥→

¥monotona i nelinearna funkcija. Ovakva mapiranja (sa f da se monotono povećava) se često koriste poboljšanja konstrasta digitalnih slika i samim tim posebnim pritivima obrađene slike. Korekcija game je poseban sličaj gde f uzima formu

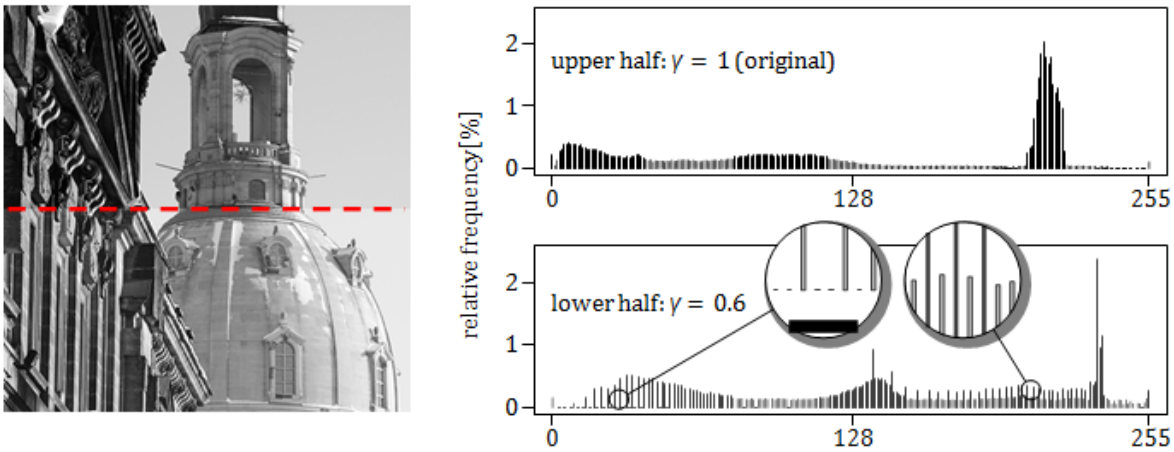
$$f(x_i) = (2^A - 1) \cdot \frac{\cdot\cdot}{2^A - 1} \cdot {}^{v}.|$$

Iako poboljšanje kontrasta samo po sebi neće ugroziti autentičnost slike, detekcija toga je još uvek od velikog značaja u digitalnoj forenzici slike iz nekoliko razloga (osim opšteg pitanja o istoriji obrade slike pod analizom). Na primer, mnoge forenzičke tehnike se oslanjaju na neku vrstu pretpostvke, koje ne mogu da se održe posle nelinearne obrade. Štaviše, poboljšanje kontrasta može biti deo složenije manipulacije, gde se primenjuje lokalno sa ciljem da prilagodi manipulisane regionesa njihovim okruženjem.



Slika 2.16: Formiranje vrhova i procepa u histogramu u digitalnoj slici poboljšanog kontrasta.

Vrh se dešava se više diskretnih ulaznih vrednosti, posle zaokruženja, mapiraju na istu izlaznu vrednost(ovde na primer f(4) = f(5) = 8). Suprotno tome, procep se dešava ako specifična izlazna vrednost nema nijednu odgovarajuću ulaznu jedinicu(na primer f(x) = 5). Menjajuća tamno siva i svetlo siva regija odgovara zaokružujućim intervalima koji se mapiraju na istu vrednost.



Slika 2.17: Tipični sivi histogrami pre i posle korekcije game.

Gornja polovina slike je ostala nemodifikovana, dok je donja polovina bila predmet smanjenja kontrasta sa i = 0,6. Gama korekcija uvodi karakteristične vrhove i praznine po histogramu koji nisu prisutne u histogramu gornjeg dela slike.

Pošto poboljšanje kontrastamodifikuje intenzitet vrednosti pojedinačnih piksela, nije bez uticaja na histogramu nastalog prikaza. Preciznije, Stam i Liu su primetili da histogrami slikapoboljšanog kontrasta pokazuju karakteristične vrhove i praznine, koji nisu prisutne u histogramu tipične originalne digitalne slike. Slika 2.16 zamišlja kako kombinacija nelinearnosti i zaokruživanja vodi do ovih identifikacionih tragova. Prateći Slika 3.17 - za poseban slučaj gama korekcije – poredi se histogram originalne slike sa histogramomslike poboljšanog kontrasta. Stam i Liu dalje napominju da položaj vrhova i praznina u histogramu zavisi od specifičnog oblika poboljšanja kontrasta, koji omogućava da se zaključi o parametara za mapiranje f (x) . [2]

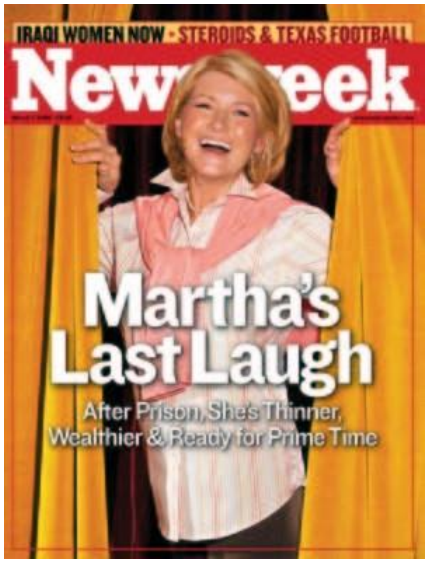
3. Digitalna analiza slike i forenzika

Digitalni fotoaparati i video softver su omogućili lakše nego ikada stvaranje visoko kvalitetnih slika i video klipova. Usluge kao što su MySpace, Google Video, i Flickr distribuciju slike čine trivijalnom, a mnoge su preuzete od strane masovnih medija. Međutim, postoji problem: kako možete da kažete da li su video ili slika stvarni? Da li je kompjuterski generisana ili modifikovana? U svetu gde su slike uticajnije od reči, od suštinskog je značaja da razlikujemo činjenice od fikcije . Ovaj rad "pokriva" neke česte i neke ne tako česte forenzičke metode za vađenje podataka iz digitalnih slika. Rad opisuje metode za razlikovanje prave slike od kompjuterski generisanih, i identifikuje kako je slika digitalno izmanipulisana.

3.1 Problem u radu sa slikama

Slike imaju moć. Da li je šatl eksplodirao tokom lansiranja, čovek hodao po mesecu, ili vojnici podižu zastavu na Ivo Džimi tokom Drugog svetskiog rata, močne slike utiču na društvo. Pojava sofisticiranog softvera za obradu i foto-realistična grafika omogućava umetnicima da ojača slike ili prenese alternativna značenja. Nažalost, mnogi izmenjeni slike su predstavljene kao prave.

Pre digitalnog doba, moćne slike su ponekad bile izrežirane, editovane tehnikama kao što je airbrush, ili prosto drugačije nazvane kako bi im se izmenilo značenje. Softver za digitalnu obradu je doveo do toga da se izgubi potreba za fizičkim stvaranjem iznova. Slike mogu biti spojene, grafički uvećane ili u potpunosti kompjuterski generisane. Detektovanje manipulisanih slika može predstavljati poteškoću. Mnoge identifikovane manipulacije bile su propraćene kontroverzom. Na primer, u martu 2005 godine Njuzvik je predstavio Martu Stjuart na naslovnoj strani (slika 3.1).



Slika 3.1 Marta Stjuart

Slika prikazuje glavu Marte Stjuart na tuđem telu. To je dovelo do oštrih kritika upućenih Njuzviku zbog obmanjivanja.

Problem sa ovakvim slikama takođe može biti kopirajt, odnosno zaštita autorskih prava.

Problem sa manipulacijom slike može dovesti do pitanja autorskih prava. Mnoge poznate ličnosti, uključujući i Sandru Bulok i Pamelu Anderson, imale su svoje glave postavljene na slike golih žena kako bi se stekao utisak da su zapravo one obnažene. U tim slučajevima dočazi do zloupotrebe i narušavanja njihovih autorskih prava.

3.2 Dečija pornografija

Postoji mnogo tamnija strana digitalnog sveta. 1996. godine, u SAD izglasan je zakon o činu sprečavanja dečije pornografije (CPPA). Ovaj zakon sprečava korišćenje dece u seksualno eksplicitnim materijalima. Međutimnije napravljena razlika između "prave" dece i komjuterski generisane/ilustrovane dece. U 2002. godini, Vrhovni sud SAD-a je odlučio da CPPA prekršio prava slobode govora. Tehnički, ako dete nije stvarno, onda nijedno dete nije bilo povređeno i zbog toga se CPPA ne primenjuje. Ova odluka je stvorila razliku između "dječije pornografije" (CP) i "virtuelne dečije pornografije" (VCP).

- dečija pornografija - upotreba stvarnie dece u seksualno eksplicitnim situacijama je zabranjeno od strane CPPA.
- virtuelna dečija pornografija - slike koje ne koriste prave decu su klasifikovane kao "pornografije" zaštićene su kao sloboda govora.

Za sprovođenje zakona, razlika između CP i VCP je izuzetno važna u slučaju gonjenja pedofila. Slučaj na osnovu VCP je mnogo teže opravdati nego onaj koji koristi CP. Kao rezultat toga moraju se identifikovati različiti aspekti manipulacija slikama. Na primer, ako se algoritam uljane slike nanosi na stvarnu sliku, onda je slika digitalno modifikovana ali i dalje predstavlja pravo dete. Nasuprot tome, u potpunosti kompjuterski generisano dete jeste VCP -. ako je moguče identifikovati je kao da je kompjuterski generisana. Postoje i slučajevi "Deca Frankenštajni" gde su slike više dece sastavljene u jednu i sačinjavaju jedno dete ali to još nije testirano od strane sudova.

3.3 Digitalna autentfikacija

Mnogi veb sajtovi zahtevaju potvrdu identiteta u cilju rešavanja pritužbe za imitaciju. U nekim slučajevima, zahtevaju se fotografije ili kopije od ličnih dokumenata. MySpace je jedan od primera gde se zahteva fotografska potvrdu identiteta. Prilikom prijavljivanja na mrežu uljeza ili prethodno prijavljenog otetog naloga, MySpace zahteva digitalnu sliku kao potvrdu identiteta. Slika treba da bude takva da vlasnik naloga drži znak koji uključuje broj MySpace naloga. Međutim, MySpace nema očiglednih sredstava da potvrdi autentičnost slike. Kao rezultat toga, MySpace je pogrešno prihvatio sledeće vrste falsifikovanih slika za uklanjanje ili otimanje naloga korisnika:

- **Ne ja** - MySpace nema načina da utvrdi da je slika zapravo od vlasnika naloga, bilo koja osoba držeći odgovarajući znak može tvrditi da je vlasnik naloga.

- **Lažni tekst** - Ako vlasnik računa ima njegovu sliku na kojoj drži bilo koju vrstu table ili papira, onda Photoshop može da se koristi u svrhu zamene teksta.
- **Lažni znak** - Slika važećeg vlasnika naloga može se photoshopovati tako da izgleda da drži znak.

Iako postoje napredne metode za otkrivanje falsifikovanih slika, problematika gorenavedenih slika je predstavljena MySpace-u i takvi nalozi su uklonjeni.

3.4 Metode za analiziranje slike

Analiza slike se bavi pitanjima o manipulaciji slika:

- Da li je slika prava, CG (kompjuterska grafika), ili digitalno uvećana?
- Ako je slika realna: gde je snimljena, kada i kako (na primer, kamera, model)?
- Ako slika je digitalno poboljšana: sa čim je manipulisano i kako je manipulacija izvršena?
- Ako slika je CG: koliko je slika stvorena?

Postoje četiri različita pristupa analizi slike:

- **1.Posmatranje**. Mnogo puta falsifikati mogu biti identifikovani kroz direktno posmatranje; bez potrebe za alatima za analizu slike.
- **2.Osnovna poboljšanja slike.** Kroz uobičajne algoritame kao što su oštrenje, zamućenje, skaliranje, ponovo bojenje, atributi u okviru slike mogu više da se razlikuju.
- **3.Analiza formata slike.** Promena slika menja format. U slučaju JPEG-a i drugih sličnih formata slike, promene slike se mogu detektovati.
- **4.Napredna analiza slike.** Analiza signala može da otkrije manipulaciju. Pristupi u rasponu od analize nivoa grešle do analize principijelnih komponenti (PCA) i wavelet transformacije (talasanja)

3.4.1 Obzervaciona analiza

Najjednostavniji pristup analiziranju koristi ljudska zapažanja da se izvuku informacije iz slike. Nedoslednosti obično sugerišu digitalno pojačanje ili CG. Predmeti u okviru slike mogu se koristiti za identifikaciju gde i kada je slika nastala. Glavne stavke za pretragu unutar slike su:

- **Spekularna svetlost i senka.** Oštre svetlosti i senke ukazuju na pravac svetlosti. Kad su stavke spojena u jednu sliku, one ne mogu imati isto osvetljenje.
- **Boja tona u anti-aliasing.** Slike retko imaju oštre i jasne ivice. Umesto toga, anti-aliasing tehnika Blur ujedinjuje susedne boje. Kada objekat isečen na jednoj slici i nalepljen na drugu, ivice mogu da sadrže boju koja se ne podudara sa pozadinom.
- **Refleksija.** Kada su slike editovane, refleksija možda neće biti izmenjena. Na primer, uklonjeni objekat može biti prisutan u refleksiji. Slično, dodatom objektu će možda faliti refleksija.

- **Skaliranje.** Pri kombinovanju slika postoji verovatnoća da one neće biti proporcionalne.
- **Rutovanje.** Ljudi ili predmeti spojeni u sliku mogu da izgledaju kao da plutaju/lebde.
- **Predmeti**. Uobičajne stavke u slici mogu biti regionalne ili vremenski specifične. Na primer, električne utičnice se razlikuju od kontinenta do kontinenta. Tekst i valuta na slici može da identifikuje lokaciju. Satovi i kalendari otkrivaju vreme. Isto tako, fotografije koje pokazuju kompjuterske ekrane mogu prikazati specifičnu primenu, operativni sistem ili prepoznatljivi veb sajt.
- **Dupliranje.** Predmeti unutar slika mogu biti kopirati i duplirani na drugim lokacijama unutar slike. Duplikati ne moraju biti modifikovai, smanjeni, rotirani, prevrnuti, ili na drugi način izmanipulisani.

Nažalost, mnogi predmeti se ne mogu jasno prepoznati bez jačanja slike. Osnovne metode jačanja slike mogu pojasniti elemente unutar slike za lakše identifikovanje.

3.5 Mogućnosti za poboljšanje slike

Većina alata za uređivanje fotografija sadrži funkcije za osnovna poboljšanje slike. To se može koristiti za razjašnjenje slika (ili određenih delova unutar slika). Uobičajne funkcije za poboljšanje su:

- **Osvetljenje i kontrast**. Ovi algoritmi mogu da osvetle tamnija područja, otkrivajući skrivene predmete ili da toniraju svetlost ispranih slika.
- **Podešavanje boja.** Osvetljenje može dramatično uticati na šemu boja u slici. Mnogi alati dozvoljavaju promenu temperature slike (frekventni opseg) ili prilagođavanje individualne boje komponente.
- **Invertovanje.** Invertovanje delove slike (negativ) može otkriti informaciju opstruiranu usled pojave sličnih boja.
- **Izoštravanje i blurovanje**. Predmeti koji nisu u fokusu ili su zamućeni zbog kretanja mogu biti korigovani sa ovim funkcijama.
- **Normalizacija i histogrami.** Napredni alati omogućavaju gledanje i modifikaciju opsega boja. Na primer, ako slika izgleda suviše ravnomerno, onda će normalizovana slika volja stvoriti veći opseg boja.
- **Skaliranje.** Kod nekih formata slika objekti se mogu zumirati do stvaranja distorzija. Na primer, visoke rezolucije JPEG mogu da se zumiraju čak 200% dok slika ne postane previše iskrivljena. Slično tome, veoma velike slike mogu biti smanjen za lakše gledanje. [3]

4. Tehnike multimedijalne forenzike

Identifikacija uređaja i autentifikacija slike

Multimedijalna forenzika može biti definisana kao nauka koja pokušava (analizranjem određene digialne imovine) da pruži procenu za takav sadržaj kao i da "izvuče" informacije koje mogu biti korisne u istrazi koja je vezana za analizirani dokument. Osnovna ideja multimedijalne forenzike oslanja se na posmatranju da svaki proces akvizicije (potvrđivanja) i svaka post-procesna operacija ostavljaju izrazit otisak na podatke (nešto u vidu digitalnog otiska). Analize takvog otiska mogu da odrede poreklo slike ili videa kao i da uspostave autentičnost digitalnog sadržaja.

Forenzički alati rade bez ikakvih dodatnih informacija. Jedine karaktersitike koje mogu biti procenjene jesu one koje su usko povezane sa digitalnim sadržajem. Osnovna ideja multimedijalne forenzike oslanja se na posmatranju da svaki proces akvizicije (potvrđivanja) i svaka post-procesna operacija ostavljaju izrazit otisak na podatke (nešto u vidu digitalnog otiska), što znači da procena takvog otiska sugeriše kako da se proceni digitalni trag, pretvorivši ga u pravi dokaz.

Cilj ovog poglavlja jeste predstavljanje principa i motiva digitalne forenzike (sa fokusom na sliku i video) kao i opisivanje dva glavna načina pristupa u rešavanju dva osnovna pitanja:

- Koji je izvor digitalnog sadržaja?
- Da li je taj digitalni sadržaj autentičan ili nije?

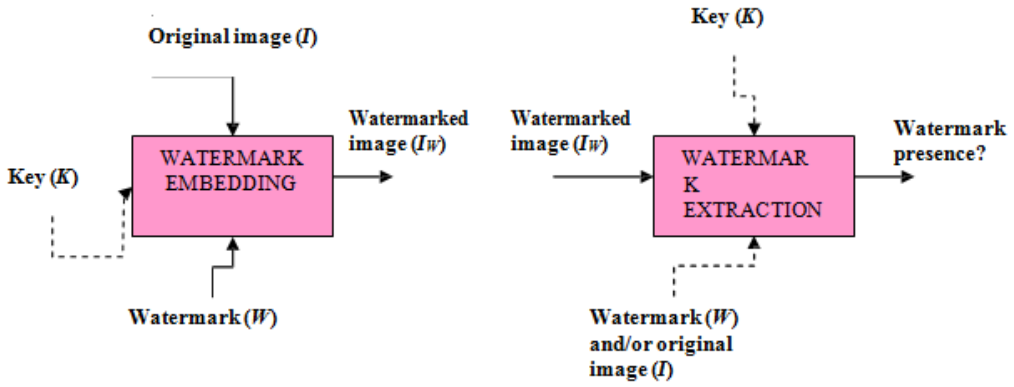
4.1 Multimedijalna forenzika - principi i motivi

Multimedijalna forenzika se može definisati kao nauka koja pokušava, analizirajući digitalna sredstva, da proceni sadržaj i da izvuče informacije koje mogu biti od koristi i da pruži podršku u istrazi povezanoj za scenu zastupljenu u tom digitalnom dokumentu. Multimedijalna forenzika mora biti u stanju da razvije efikasne instrumente koje će se baviti različitim digitalnim uređajima koji mogu da generišu slike i, iznad svega, sa različitim alatima za obradu koja takođe omogućava nekvalifikovanom korisniku manipuliše digitalnim dobrima. U nastavku, uvode se dva osnovna pristupa. Nakon toga, neki od mogućih scenarija primene ove tehnologije u kojoj bi mogao da bude zahtev za rad su opisani i na kraju širok pogled na to koji se mogući digitalni otisci prstiju traže u datom multimedijalnom sadržaju.

4.1.1 Moguć pristupi

Kada su digitalni snimci (video) morali da budu zaštićeni ili da se utvrdi njihova autentičnost ili, štaviše, da se prati njihovo poreklo, rešenje je bilo da se u originalne podatke ubace ugrađeni, obično neprimetni, podaci koji su kasnije dozvoljavali da se utvrdi šta se desilo, u kom delu sadržaja i u nekim slučajevima - od strane koga. Ova vrsta tehnike koja može biti grupisana pod nazivom Digitalno vodeno žigoisanje (Barni, 2004), sledi "aktivni" pristup koji je neophodano za rad na originalnom dokumentu koji mora da bude dostupan od početka: zahtev je gotovo uvek teško zadovoljiti. Ugrađivanje vodenog

žiga u sliku, na primer, (Slika 4.1) može da se izvede primenom nekoliko konkretnih lakših modifikacija originalnog dokumena I prema informacijama sadržanim u vodenom žigu W i, često, privatnog ključa K; nakon toga je sadržan sadržaj Iw.



Slika 4.1: Ugrađivanje vodenog žiga (levo) i ekstrakcija vodenog žiga (desno).

Ako je neophodno izvršiti procenu da li se nešto dogodilo sa vodenim žigom, faza detekcija se vrši propuštanjem, zajedno sa privatnim ključem K (ukoliko algoritam nije "slep", takođe je potrebno ioriginalnu sliku), kroz detektor koji daje odgovor ponovnim izvlačenjem vodenog žiga W ili upoređivanjem verifikacionih parametara sa određenim pragom. Zbog same kompletnosti, takođe bi trebala da bude uključena i kriptografska analiza unutar kategorije "aktivne" metode. Takav pristup koristi digitalni potpis ne bi li se verifikovao autor i vreme potpisa kao i autentifikacija sadržaja poruke. Digitalni potpis je postignut kalkulisanjem klasifikovanih digitalnih podataka heš funkcijom i enkripcijom privatnim ključem; tako potpisana klasifikacija je smeštena zajedno sa slikom i može biti korišćena u dokazivanju integriteta podataka ili da se pronađe njeno poreklo. Postoje neke slabosti u ovom kriptografskom pristupu:

- Klasifikacija signala mora biti vezana za sam sadržaj i time se onemogućava upotreba drugačijeg formata ili autentfikacija podataka nakon D/A (digitalne/analogne) konverzije
- Klasifikacija se menja čim se napravi promena na signalu time učinivši da je nemoguće napraviti razliku između maliciozne i nešškodljive modifikacije.
- Kriptografska autentifikacija ne dozvoljava preciznu lokalizaciju neovlašćenja (Menezes 1998).

Lako je razumeti da se takva evaluacija ne može izvršiti na npr. uobičajne digitalne sadržaje koji se nalaze na internetu (video sa Youtube-a, slika objavljena u elektronskom izdanju novina...). Ovakva vrsta aktivne tehnologije (Blythe 2004) može biti usvojena da upravlja podacima u specifičnom sadržaju aplikacija gde je izvodljivo raspoređivanje dodatnih informacija ali da nisu u mogućnosti da se bave sa otvorenim operativnim okruženjem u kome je moguć samo korak detekcije.

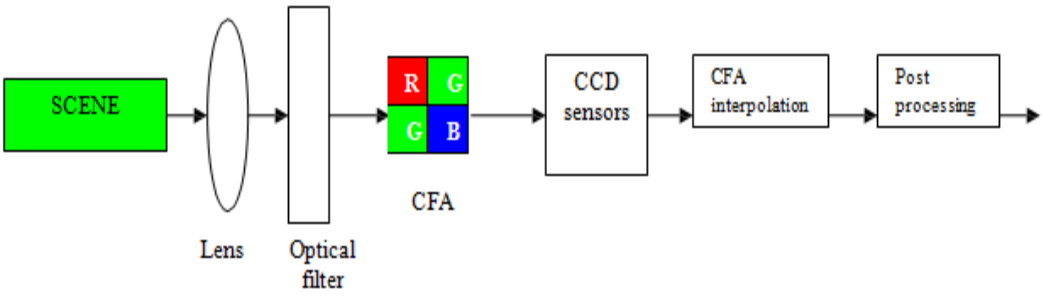
U ovoj situaciji bi najkorisnija bila pasivna metodologija; sa terminom "pasivan" - pristup pokušava da napravi procenu imajući na raspolaganju samo digitalni sadržaj. Jasno je da je ovakva vrsta istrage teža i da mora biti zasnovana na temeljnoj analizi nekih unutrašnjih karakteristika koje su ili nisu bile prisutne i koje su ili nisu prepoznatljive

unutar posmatranih podataka (Popescu 2004). Da bi se razjasnilo, kada je npr. izršena fotomontaža da bi se izmenio sadržaj digitalne slike, neki tragovi ove operacije su istavljeni preko "nove lažne" slike da bi se izmenilo značenje prezentovane scene.Ovi tragovi mogu rezultirati u modifikaciji strukture slike kao što su nekarakteristične vrednosti piksela (sekvencijalne interpolarne vrednosti ili čudne kontinuirane flat vrednosti) ali i u nekonstantnosti unutar samog sadržaja slike kao što su anomalije unutar pravca osvetljenja ili u prisustvu disproporcijalnih objekata na slici.

4.2 Vrste digitalnih dokaza i njihova karakterizacija

Od digitalnih forenzičkih alata se traži da povrate presudne informacije analiziranjem digitalnih dokaza; njihove unutrašnje karakteristike su povezane onako kako su dokumenti stvarani, sačuvani/odlagani i upotrebljavani - to su veoma važni elementi koji se prvi uzimaju u obzir i oni odlučuju koja je metodologija istrage odgovarajuća.

Od svih digitalnih podataka, digitalna forenzika se najviše bavi sa slikama; trokanalne , dvodimenzionalne oblasti (jednodimenzionalne ako je slika na nivou sive boje) je sve iz čega se mogu dati odgovori. Ukoliko je slika nastala digitalnom kamerom koja je uslikala stvarnu scenu "prati" da će njen sadržaj sadržati sve nesavršenosti i izmene načinjene specifičnim senzorom i blokom procesiranja koji generiše krajnji sačuvani fajl. Kao što je dokazano (Slika 4.2), kada je slika nastala u realnom životu, svetlo je fokusirano sočivima senzora kamere koja su 2D CCD/CMOS koji konstituišu elemente slike (piksele). Ti elementi su pogođeni fotonima i konvertovani su u voltažne signale koji su uzorkovani A/D konverterom.



Slika 4.2: Akvizicioni proces unutar kamere

Pre nego što dođu do senzora, zraci sa scene su filtrirani kroz CFA (Color Filter Array) koji je specifični mozaik boja koji dozvoljava svakom pikselu zasebno da odabere boju. Izlaz senzora je uspešno demozaičen kako bi sadržao sve tri boje za svaki piksel a zatim ovaj signal prolazi dodatno procesiranje kao što su balans bele boje, gama korekcije; nakon čega se odlaže u memoriju kamere u specijalnom formatu (iako se kod komercijalnih uređaja preferira JPEG format). Sada je lako razumeti da karakteristike svake operacije i karakteristike svakog elementa, od same scene do završnog fajla slike, utiču na digitalne podatke. Postoje tehnike koje su istraživale prisustvo specifičnog CFA (Swaminathan 2006) unutar teksture slike da bi se vratili na brend kamere koja je napravila tu sliku kao i druge metode koje su predlagale studiranje koeficijenta kvantizacije JPEG-a koje bi trebalo da otkrije da li je slika prošla drugu kompresiju i time otkrila moguće

neovlašćene promene (Lukas 2003). Sa druge strane, mnogi pristupi su bazirani na anomalijama koje je ostavio sam uređaj (izgrebano sočivo, defektni pikseli...). Obraćena je pažnja na šum senzora i, između ostalog, na mračnu struju, šum samog slikanja, toplotni šum; PRNU šum je najinteresantniji za forenzičke aplikacije. Prisustvo PRNU-a je indukovano unutrašnjem diskomfortu u procesu proizvodnje silikooonskih CCD/CMOS-a. Takav šum je sistematski otisak koji karakteriše svaki senzor tako da će dve kamere istog proizvođača ostaviti različite tragove na digitalnim sadržajima koje naprave. To, konkretno, nije nasumični šum zato što je dvodimenzionalnog šablona koji je supernametnut za svaku napravljenu sliku. Međutim slike, kojima je potrebna forenzička analiza, mogu biti deo video nastavka; pod ovakvim okolnostima, podaci koji se kontrolišu imaju privremenu dimenziju i to mora da se uzme u razmatranje iako se većina razmatranja o digitalnim slikama vezanih za prisustvo PRNU-a i CFA poistovećuje sa akvizicionom fazom i može biti prošireno na video (Chen 2007, Mondaini 2007). Bitno je istaći da veliki deo omogućenih podataka može da pretrpi različite vrste manipulacije (sa poštovanjem statičnih), posebno da frejmovi mogu biti preskočeni, modifikovani kako bi se izmenilo značenje, izmenjeni kako bi se izmenilo samo trajanje videa. Video sadržaj, koji dolazi od različitog uređaja ali sličnog sadržaja, može biti dodat videu na način koji "ne nervira" i da tako izmeni čitavu priču. Forenzička analiza mora biti fokusirana na stvari kao što su korelacija PRNU šum unutrašnjeg frejma i MPEG-X re-kodovanje.

Druga vrsta slika koje mogu da konstituišu digitalni dokaz za pregled, kao dodatak onim dobijenim iz digitalnih foroaparata ili kamkodera, dolazi usled skeniranja, To znači da štampani dokument (npr. naslovnica časopisa ili neka slika iz stvarnog života) koji se nalazi u ravni, položen na skener, je osvetljen red po red putem klizećeg jednodimenzionalnog senzora kako bi se stvorio digitalni podatak (Khanna 2007). Finalni format fajla je obično podesiv ali je najčešće JPEG ili PNG. U ovom slučaju, zbog raznolikosti uređaja i digitalnih procesa, drugi elementi (dodajući ih onima vezanim za kamere) mogu biti uzeti u obzir za vreme forenzičke analize kako bi se naglasili mogući tragovi digitalne zloupotrebe. Na primer, prisustvo preko slike 1D obrasca šuma, umesto dvodimenzionalnog, može biti indikator o poreklu slike. Pravac (vertikalni ili horizontalni) takve jednodimenzionalne periodičnosti može biti dokaz putem skenera. Drugi aspekt za kontrolu može biti neki komadić prljavštine koji je ostao na površini ploče, male ogrebotine stakla skeneravkoje su usled skeniranja postale sastavni deo skeniranog fajla.

Treba napomenuti i na još jedan tip slika sa kojima forenzički alati mogu da se sretnu - kompjuterski generisane slike. Većina tih slika napravljena je uz pomoć softvera dok su neke napravljene kamerom (http://area.autodesk.com/index.php/fakeorfoto). Ovi sistemi omogućavaju izgradnju kompletno novih slika ili da omoguće realističnu fotomontažu spajajući sintetički generisane delove u jednu sliku. Da bi izgledalo što realističnije postoje razni korisni instrumenti, a supernametanje šuma je samo jedna od lukavosti koju vrhunski korisnik može da upotrebi u stvaranju svoje lažne slike. Kad se bavimo ovakvom vrstom slika, osnovna ideja koju treba pratiti jeste izvlačenje značajnih karakteristika koje daju indikaciju o samoj realnosti slike.

4.2.1 Unutrašnji digitalni otisak

Iako su forenzičke tehnologije primenjene u različite svrhe, moguće je pokazati kako je uobičajni pristup propraćen sa gotovo svim do sada predstavljenim forenzičkim algoritmima bez obzira na to da li su namenjeni za identifikaciju izvora ili za detekciju neovlašenih promena. Digitalna forenzika je bazirana na ideji da su nerazdvojivi tragovi

(npr. digitalni otisak) ostavljeni u digitalnom mediju za vreme procesa stvaranja i svakog sledećeg procesa (Swaminathan 2008). Pribegavanju isključivo analiziranim podacima, bez ijedne prethodno omogučene informacije (pasivni pristup) i bez znanja o povezanim originalnim podacima (slepa metoda), forenzičke tehnike hvataju unutrašnje informacije sprovedene digitalnim prednostima u smislu različitih metoda analize - statistička, geometrijska...

U obzir za forenzičku analizu uzeto je nekoliko vrsta digitalnih otisaka. Klasifikacija je moguća delivši ih u tri kategorije:

- digitalni tragovi nastali procesima unutar kamere: svaka komponenta unutar digitalnog akvizicionog uređaja modifikuje ulaz i modifikuje unutrašnji otisak u završnom izlazu zbog specifičnog optičkog sistema, senzora boja, softvera kamere; slike, naročito prirodne slike, imaju generalne karakteristike bez obzira na sadržaj - nasledni šum ili ponašanje osvetljenosti, statističke karakteristike koje mogu bti viđene kao inherentni otisak.

- digitalni tragovi ostavljeni u procesima van kamere: svako procesiranje primenjeno na digitalne medije modifikuje njihove karakteristike (statističke, geometrijske...) ostavljajući prema tome čudne tragove na samo procesiranje.

Treba napomenuti da su prethodni otisci nezavisni sa sadržajem analiziranih podataka; trag ostavljen datom kamerom je isti iako su stečeni različiti subjekti.

- otisci koji su u vezi sa karakteristikama frejmovane scene: slika nastala "iz sveta" ima specifične karakteristike u zavisnosti od njenog sadržaja kao što je karakterstika osvetljenosti, koja karakteriše reprodukcionu scenu.

Nakon odabranog otiska procedura je da se odaberu neke od karakteristika otiska koji je uzet u obzir kako bi se istražili relativni parametri i kako bi se napravila odluka koja se zasniva ili na klasifikacionim ili na procedurama procene. U slučaju identifikacije izvora, ovi tragovi su obično izvučeni i upoređeni sa setom podataka mogućih otisaka specifičnih za svaki model/vrstu/brend akvizicionog uređaja, kako bi se digitalni podaci povezali sa odgovarajućim izvorom. Sa druge strane, prema svrsi detektovanja falsifikata, ideja je da se detektuje neuniformnost ili razbijanje takvih otisaka unutar podataka koji su uzeti u obzir; naročito, medij je analiziran po blokovima i za svaki blok je odabran otisak ili, još bolje, njiove karakteristike ili parametri su izvučeni i međusobno upoređeni. Očigledno je da će samo prva kategorija biti uzeta u obzir, dok se za verifikaciju integriteta mogu koristiti sve tri kategorije.

4.3 Tehnike za identifikaciju akvizicionog uređaja

Tehnike za identifikaciju uređaja su fokusirane na proceni porekla digitalnih podataka slike ili videa. Postoje dva glavna aspekta za proučavanje:

- prvi je razumevanje koji digitalni uređaj je napravio te digitalne podatke (skener, mobilni telefon, digitalna kamera, video rekorder, ili je kompjuterski generisana)
- drugi je određivanje specifične kamere ili senzora koji je napravio takav sadržaj, prepoznavši model i brend (Slika 4.3)



Slika 4.3: Problem identifikacije izvora

Digitalne slike mogu biti sačuvane u raznim formatima - JPEG, GIF, PNG, TIFF, i sam format može biti informativan kao sama slika. Npr; JPEG fajlovi sadrže dobro definisan set karakteristika koji uključuje metapodatke, kvantizacione tabele za kompresiju slika i lusi (lossy) komprimovane podatke. Metapodaci opisuju izvor slike, tu obično spadaju podaci o tipu kamere, rezoluciji, podešavanjima fokusa... Pored toga, kada se koristi RAW format, kamera kreira heder fajl koji sadrži sva podešavanja kamere uključujući (u zavisnosti od kamere) nivo izoštrenosti, podešavanje kontrasta i osvetljenosti, temperaturu boja/balans bele boje... Slika nije izmenjena ovim podešavanjima, ona su naprosto tagovana na sirove podatke slike. Iako takvi metapodaci daju ogromnu količinu podataka, postoje neka ograničenja:

- te informacije mogu biti editovane
- mogu biti izbrisane
- mogu biti ubačene lažne informacije o kameri

Zato je neophodno imati pouzdanu identifikaciju izvora bez obzira na tip informacija iz metapodataka.

Ova sekcija će biti posvećena analizi principijelnih rešenja za identifikaciju akvizicionih uređaja slika i videa istražujući generalnu strukturu i sekvence faza cevovoda slike, zasnovanih na fizici i operacijama uređaja koji je pod ispitivanjem. Ove tehnike ciljaju na analiziranje tih operacija sa ciljem da se nađe otisak za taj uređaj (tzv. otisak unutar kamere (in-camera figerprint)) u vidu prisustva identifikujuće tačke zbok interpolacije CFA (Color Filter Array), nesavršenosti senzora i odstupanja sočiva. Tehnike koje će biti istražene bazirane su na izvlačenju, od slika koje pripadaju drugim kategorijama (skenirane slike, video...) sa nekim robustnim unutrašnjim karakteristikama koje su specifične za određene uređaje. Generalno, ove karakteristike mogu biti upotrebljene za treniranje klasifikatora; dok se trening izvršava i bez obzira da li karakteristike odobravaju dobru karakterizaciju, sistem omogućava klasifikaciju digitalnih dobara.

4.4 Odstupanje sočiva

Zbog procesa dizajniranja i izrade, sočiva proizvode različite vrste odstupanja na slikama. Istražene su dve vrste odstupanja kako bi se rešio problem identifikacije izvornog uređaja:

- radijalna distorzija sočiva (Choi 2006)
- hromatsko odstupanje (Lahn 2007)

Radijalna distorzija izaziva prave linije u prostor objekta da se čine kao zakrivljene linije na sanzoru kamere a dešava se kada dođe do promene u poprečnom uveličanju M sa povećanjm distance od optičkih osa. Stepen i redosled kompenzacije takve distorzije varira od proizvođača do proizvođača kao i kod različitih modela kamera istog proizvođača. Kao rezultat, senzori različitih kamera ostavljaju unikatne otiske na "uhvaćenim" slikama. Radijalna distorzija sočiva može biti zapisana kao:

$$r_u = r_d + k_1 r_d + k_2 r_d$$

gde su r_u i r_d nedistorzovani odnosno distorzovani radijusi. Radijus je radijalna distanca $\sqrt{x2 + y2}$ od tačke (x, y) od centra distorzije (centar slike). Cilj ove metode (Choi 2006) jeste da se nađu parametri $k1$ i $k2$ koji konstituišu otisak da identifikuje izvornu kameru prateći Devernejevu metodu prave linije. Međutim, ova metoda je bezuspešna ukoliko na samoj slici nema pravih linija kao i ukoliko se uporede dve kamere istog modela.Takođe je moguće izvršiti korekcije softverom sa ciljem da se isprave radijalne distorzije slike.

Drugi tip istraženog odstupanja u cilju rešavanja identifikacije izvora je hromatsko odstupanje. Hromatsko odstupanje je fenomen gde svetlo različite talasne dužine ne uspeva da se konverguje na istoj poziciji kao i fokalno sočivo. Postoje dve vrste hromatskog odstupanja:

- longitudinalno odstupanje koje izaziva različite talasne dužine da se fokusiraju na različitim distancama od sočiva
- bočna aberacija je pripisana drugačijoj poziciji senzora

U oba slučaja, hromatsko odstupanje vodi do različitih formi nesavršenosti boja unutar slike. Samo bočno hromatsko odstupanje može da se uzme u razmatranje za udentifikaciju izvora (Lahn 2007). Hromatsko odstupanje izaziva neporavnanje između RGB kanala tako da je zadatak procena poremećenih parametara kako bi se kompenzovalo za distorziju maksimovanjem zajednčkih informacija između kanala boja. Zatim su ovi parametri upotrebljeni za identifikaciju izvora mobilnog telefona kroz upotrebu SVM klasifajera.

4.5 Tehnike za procenu integriteta slike

Integritet informacija je fundamentalan na suđenju; presuda mora biti povučena nakon razmatranja seta dokaza i autentičnost tih dokaza treba da bude potvrđena pre donošenja odluke. Sa jedne strane, svedoci i njihove tvrdnje čine jedan tip dokaza; sa druge strane, konkretni dokazi (npr. oružje ili neki drugi konkretni dokazi). U drugu kategoriju spadaju sve informacije sa mesta zločina i takve informacije su obično sačuvane u vidu slika. Ako slike predstavljaju realan svet, onda se one smatraju autentičnim dokazima. Ali, jasno je dolazak digitalnih slika i relativno lakog procesiranja digitalnih slika učinilo da je u današnje vreme autentičnost nesigurna. U ovom scenariju, efikasna procena integriteta digitalne informacije, konkretno digitalne slike, igra ključnu ulogu.

Ali, šta znači integritet? U konkretnom smislu, slika mora biti ishod akvizicije iz realnog sveta, bez nekog daljeg procesiranja; u širem smislu, slika mora da predstavlja

scenu iz realnog sveta i, ukoliko je kasnije došlo do nekog procesiranja slike, njen sadržaj ne sme biti izmenjen. Kad dokaz pređe iz trodimenzionalnog oblika u digitalnu sliku, gubi se poreklo slike i više se ne može verovati u ono u šta se gleda, iako se za sadržaj tvrdi da je istinit. Nekoliko alata za procesiranje slika je lako dostupno i lako za upotrebu za gotovo svakoga; uzeti u obzir Adobe Photoshop - već sada je licenciran za milione korisnika širom sveta. Sa takvim programimaje omogućen veliki broj operacija kako bi se uticalo na digitalne fajlove: osobe mogu biti prebačene u drugi kontekst, objekti mogu biti izbrisani iz scene, konkretni detalji mogu biti klonirani, objekti mogu biti dodati u scenu. Sve ove manipulacije postaju sofisticiranije i sofisticiranije time čineći izmene gotovo neprimetnim; ključ da se digitalna slika koristi kao kritični dokaz jeste da se uspostavi autentifikacija slike.

Digitalna forenzika pretpostavlja da su digitalne slike karakterisane iznutra putem specifičnih obrazaca u procesu proizvodnje kao i bilo kojim drugim procesom nastalim nakon nastanka slike. Kako bi se propisno izdvojile modifikacije, pristup forenzike slike razmatra da su otisci unutar slike različiti i prepoznatljivi zbog različitih primenjenih procesa na samu sliku ili da su originalni tragovi bili izmenjeni zbog neovlašćenog pristupa, time izgubivši uniformnost. Različiti digitalni otisci su uzeti u obzir i proučavanjem njihovih karakteristika moguće je potvrditi da je došlo do neovlašćenog pristupa kao i da se utvrdi na kojim procesima je došlo do izmena. Odnoseći se na širi izraz značenja integriteta (npr. digitalna slika predstavlja podudaranu sliku realnog sveta), dosta procesa koji ne utiču na semantiku (njp. JPEG kompresija ili rekompresija, podešavanje svetljenja, gama korekcije...) mogu biti pogrešno predstavljanje kao pokušaj neovlašćene izmene. Zbog toga, detekcija izmene na slikama ne mora obavezno da dokazuje da je bilo maliciozne izmene na sammoj slici, ali zato postavlja pitanje u vezi sadržaja slike i pomaže u daljoj analizi.

Tehnološki pristupi za potvrdu autentičnosti digitalne slike dele se na tri kategorije:

- otisci unutar kamere
- otisci van kamere
- otisci scene

U prvoj i trećoj kategoriji, forenzičke tehnike neke nekonstantnosti takvih tragova, dok se u drugom slučaju otisci koriste za identifikaciju specifičnih procesa.

4.6 Trendovi budućnosti

Iako su mnoge predložene tehnike digitalne forenzike "svetle" i revolucionarne, nijedna od njih pojedninačno ne može da ponudi rešenje za razmatrani problem (npr. identifikacija izvora i verifikacija integriteta informacije). Intervencija korisnika je često poželjna radi validacije finalnih rezultata; npr. uzeti u obzir procenu maliciozne izmene slike, što je bez intervencije korisnika gotovo nemoguće, pošto, iako se otkrije procesiranje van kamere, često samo ljudski tumač može da odluči da li je došlo do maliciozne izmene ili ne. Validacija digitalnih forenzičkih pristupa za verifikaciju integriteta se ne nalazi učestalog frejmvorka, u pogledu bazu podataka slika i mere performansi kao što su preciznost, robustnost i bezbednost.

Baza podataka slika je fundamentalna za evaluaciju predloženih algoritama; čest set podataka ommogućava ujedinjenu platformu za zajednicu istraživanja kako bi uporedili

razne algoritme. Zapravo, nekoliko setova podataka je slobodno za zajednicu istraživanja (http://www.ee.columbia.edu/ln/dvmm/trustfoto/) ali postoje neka otvorena pitanja koja pozivaju na reper seta podataka. Eksperimenti koji uključuju karakteristike kamere zahtevaju setove podataka slika pribavljenih od različitih modela kamera na različitim pribavljenim podešavanjima. Kako bi se olakšala procedura tehnike detektovanja falsifikovane slike koristeći slike kreirane tehnikama "vrhunski" falsifikovanih slika, neophodan je set podataka ovih slika. Zato je potreban svaki napor za produkciju i standardizovanje dodatnih repera setova podataka.

Većina predloženih tehnika ne omogućava čiste mere ostvarivih performansi u smislu preciznosti i lažnog alarma. Često se nailazi na manjak rigoroznih teoretskih pozadina i eksperimentalnih koncepata. Kako bi se u budučnosti ove metode rafinisale, analitički rezultati moraju biti čistije definisani, sagrađeni, deljeni i moraju biti dizajnirani odgovarajući testovi i evaluacije setova podataka. Robustnost na razne učestale i maliciozne operacije procesiranja slika je najizazovniji problem sa kojim mora da se suoči svaki forenzički algoritam slike. Predložene metode su često dizajnirane i testirane kako bi radile pod limitiranim a ne generalnim uslovima. Većinu tehnika je moguće zaobići osnovnim softverima za procesiranje slika. Prebrođavanje ovih izazova zahteva razvoj nekoliko novih metodologija i temeljnu evaluaciju njihovih ograničenja kroz generalna i praktična ppodešavanja. Pored robustnosti, različita analiza performansi forenzičkih algoritama dolazi iz polja bezbednosti. Sa povećanjem broja rešenja za detektovanje falsifikata, loši ljudi ciljaju na modifikaciju digitalnog sadržaja kako bi povećali pažnju za izbegavanje detekcije malicioznih izmena. Analiza forenzičkih algoritama sa stanovišta bezbednosti bila bi interesantan otvoreni problem sa kojim se treba pozabaviti u budućnosti. [4]

5. Forenzička klasifikacija kamera: Vreifikacija senzora putem šuma

Napredak u tehnologiji digitalnih slika je doveo do razvoja jeftinih skenera i kamera visoke rezolucije. Digitalne slike stvorene putem raznih izvora nalaze široku primenu - od medicine i organa reda do banaka i društvenih mreža. Zajedno sa umnožavanjem digitalnog sadržaja raste i potreba za softverom za editovanje time omogućivši čak i amaterima određenu vrstu manipulacije slike. Pod ovim okolnostima digitalna slika može imati legalnu upotrebu samo ako može biti autentifikovana. Za to su neophodni forenzički alati kojim će forenzičar otkriti poreklo, autentičnost i vlasništvo nad tom slikom. Zato je potreban objektivan i autentičan način da se izvrši autentifikacija slike.

Postoje mnogi nivoi na kojima može da se adresira problem autentifikacije slike. Neko može da zahteva nalaženje konkretnog uređaja (digitalne kamere ili skenera) koji su generisali sliku ili samo da se sazna proizvođač i model uređaja. Za identifikaciju izvora kamere bilo je ponuđeno nekoliko robustnih metoda:

- Bayram 2005
- Farid and Popescu 2005
- Gerads 2001
- Kharazzi 2004
- Lucas 2005
- Lucas 2006

U Khanna 2007 je prezentovana nova metoda klasifikovanja slika na osnovu njihovog izvora.

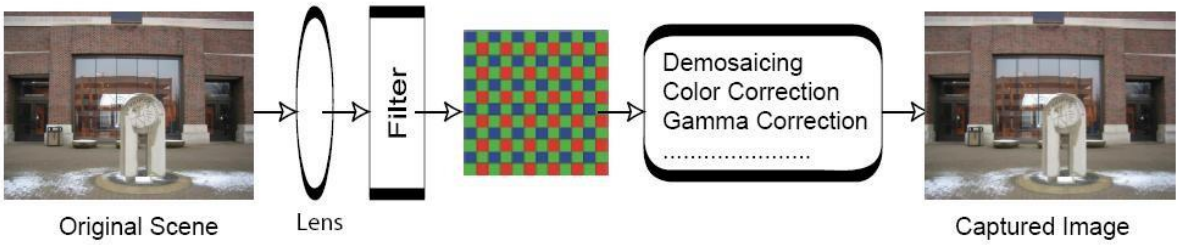
Jedan prostup za identifikaciju digitalnih kamera je zasnovan na karakterizaciji senzora kamere u uređaju. U Geradts 2001 je prikazano da defektni piksel može biti iskorišćen za pouzdanu identifikaciju kamere čak i ukoliko je slika loše kompresovana. Ova vrsta šuma (generisana "vrućim" ili mrtvim pikseom) se češće javlja kod kamera nižeg kvaliteta i može se prikazati vizuelno umnožavanjem slika napravljenih istom kamerom. Ove greške mogu biti vidljive čak i nakom kompresije slike. Problem je u tome što mnoge kamere nakon samog slikanja "obrađuju" nastale slike i uklanjaju tu vrstu šuma tako da ova tehnika nije uvek efektivna.

Lukas je odradio pionirski posao u razvoju metoda za identifikaciju izvora kamere koristeći šematski šum senzora (Lukas 2005, 2006). Identifikacija je zasnovana na neravnomernosti šuma piksela što je jedinstvena karakteristika CCD (charged coupled device) i CMOS (complementary metal oxide semiconductor) senzora. Pouzdana identifikacija je moguća čak i kada je slika kompresovana u JPEG format. Šematski šum je prouzrokovan od strane nekoliko faktora kao što su neravnomernost piksela, tačkice prašine na optici, optičke smetnje i mračna struja (Holst 1988 i Janesick 2001). Visokofrekventni deo šematskog šuma je procenjen na osnovu oduzimanja rašumljene verzije slike od originala. To se izvršava upotrebom filtera za rašumljavanje zasnovanog na vejvletu (Mihcak 1999). Referentna šema kamere je određena prosekom šema šuma iz više slika nastalih iz iste kamere. Referentna šema služi kao potpis kamere. Da bi se identifikovala izvorna kamera (source camera), šema šuma je u korelaciji sa poznatim referentnim šemama dobijenim iz setov kamera. Kamera koja se najviše podudara sa referentnom šemom i daje maksimalnu korelaciju je odabrana da kao izvorna kamera. Ova

šema je proširena u Lukas 2006 za detektovanje falsifikata slika nastalih od digitalnih kamera. Chen 2007, 2008 donosi poboljšanu metodu za identifikaciju izvorne kamere zasnovanu na zajedničkoj proceni i detekciji PRNU-a (photoresponse non-uniformity) kamere u slikama. U ovom radu, implementirane metode koriste proste metode proseka (Lukas 2005) i zbog toga dalja poboljšanja rezultata mogu biti viđena korišćenjem poboljšane metode za procenu šuma senzora (Chen2007, 2008).

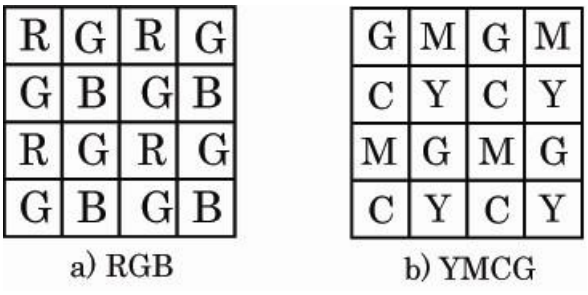
Rezultati prezentovani Lukas 2005 metodom su verifikovani korišćenjem različitih setova kamera.

5.1 Pregled digitalne kamere: proces kreiranja slike



Slika 5.1: Cevovod kreiranja slike kod digitalnih kamera

Na slici 5.1 su prikazani osnovni elementi digitalne kamere. Iako se tačni dizajn i algoritmi razlikuju od proizvođača do proizvođača, osnovna struktura cevovoda kamere ostaje ista. Prvo, svetlo sa predmeta ulazi u kameru kroz sočiva i prolazi kroz set filtera (uključujući anti-aliasing). Zatim, senzor "hvata" svetlost. Ovi senzori (standardni CCD ili CMOS) su slepi na boje u smislu da svaki piksel hvata samo informacije o intenzitetu svetlosti koja ga pogađa. Da bi se uhvatila informacija o boji, svetlost prvo mora da prođe kroz poredak filtera boja (CFA - color filter array) koji svakom pikselu dodele 3 ili 4 boje na uzorkovanje. Na slici 5.2 su prikazani CFA paterni koji koriste RGB i YMCG boje za piksele formata 4x4. Individualne boje su ispunjene interpolacijom koristeći uzorkovane vrednosti piksela koristeći određeni broj različitih algoritama interpolacije u zavisnosti od proizvođača.



Slika 5.2: CFA šeme

Zatim slede operacije kamere kao što su bela tačka, korekcije i gama korekcije- Na kraju, slika je zapisana u memoriji uređaja u formatu odabranom od strane korisnika (RAW, TIFF, JPEG...).

Iako su ove operacije i stadijumi standardni u cevovdu digitalnih kamera, tačni detalji procesiranja variraju od proizvođača do proizvođača kao i od modela do modela kamere istog proizvođača. Ove varijacije od jednog modela kamere do drugog mogu biti upotrebljene u određivanju tipa kamere korišćene u kreiranju specifične slike.

5.2 Šum senzora

Proizvodni proces senzora slika predstavlja različite defekte koji kreiraju šum i vrednostima piksela (Holst 1998, Janesick 2001). Ovi šumovi mogu biti klasifikovani u 3 tipa bazirana na njihovom poreklu i efektima.

Prvi tip jeste nasumični šum koji je prisutan u svakom izlaganju. Ovaj šum se ne koristi za identifikaciju kamera zato što se njegova vrednost razlikuje od frejma do frejma.

Drugi tip šuma je šematski šum. Odnosi se na bilo koji prostorni obrazac koji se značajno ne menja od slike do slike. Glavni izvori šematskog šuma su defekti tačke, popravljeni šematski šum (FPN) i fotoodgovorna neuniformnost (PRNU). Defekti tačke (vrući ili mrtvi pikseli) su kompenzovani od strane kamere nakon procesiranja. FPN je dodatni šum izazvan zalutalim strujama podloge senzora i još je poznat kao mračna struja (dark current).vMračna struja je fnkcija detektora veličine, gustine, strane materije zarobljene za vreme izrade i nezavistan je id intenziteta incidentnog svetla. PRNU je varijacija u osetljivosti piksela izazvane varijacijama između piksela kao što su veličina detektora, odziv spektra, debljini naslaga i drugim nesavršenostima nastalim u toku procesa proizvodnje. Ove varijacije mogu biti modelovane kao po-pikselu multiplikativni faktori. FPN i PRNU ostaju isti preko više frejmova ali se razlikuju preko različitih senzora.

Treći tip šuma je šum "iščitavanja" (readout noise) i javlja se pri iščitavanju podataka iz senzora. Najvidljiviji je sa visokim ISO ili kada je slika izuzetno osvetljena.

Dok se za buku smatralo da je dodati izraz, kao što je to slučaj sa FPN, PRNU je multiplikativni faktor. Ovaj prikaz šuma je dobro utvrđen u literaturi senzora slike i ista literatura je upotrebljena u ovom radu. Prosekovanje frejmova će redukovati izvore šuma osim kod FPN i PRNU. Iako su FPN i PRNU različiti, poznati su kao šum scene (scene noise), šum piksela, neunifrmnost piksela ili šematski šum.

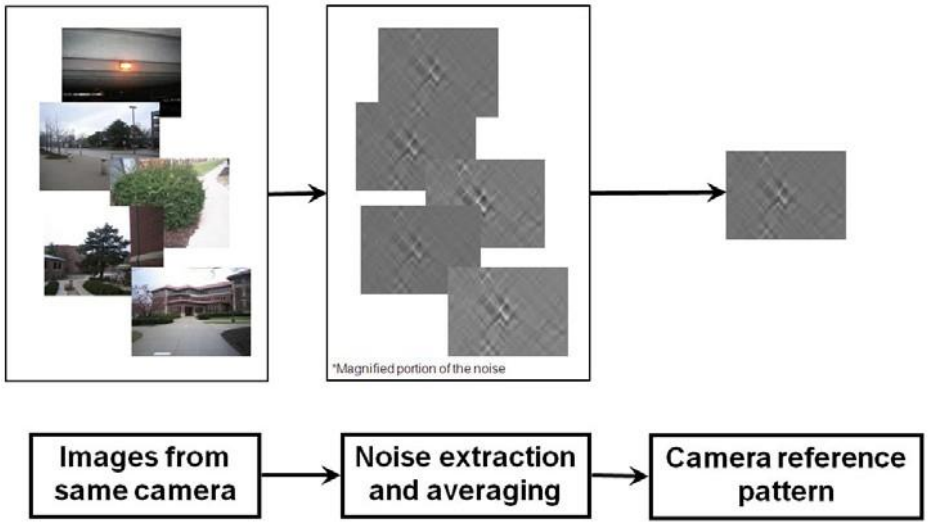
Fokus je na korišćenju šematskog šuma za identifikaciju kamere. Međutim, izuzetno je teško dobiti šematski šum direktnim metodama ili flat-fealding-om (tehnikom za poboljšanje kvaliteta digialne slike). To je zbog činjenice da su u mnogim kamerama opšte namene sirovi podaci senzora nedostupni. Određeni broj algoritama za linearno procesiranje slike je primenjen da transformiše voltažu detektovanu senzorom slike za finalne JPEG ili TIFF podatke. Zato su, u nedostatku direktnih metoda, upotrebljene indirektne metode za procenu šuma senzora. U Lukas-u 2005 uspešno je korišćena metoda za identifikaciju šuma senzora. Ova metoda koristi vejvlet filter (Mihcak 1999) u kombinaciji sa prosekom frejmova za procenjivanje šematskog šuma u slici.

5.3 Pristupi bazirani na korelaciji

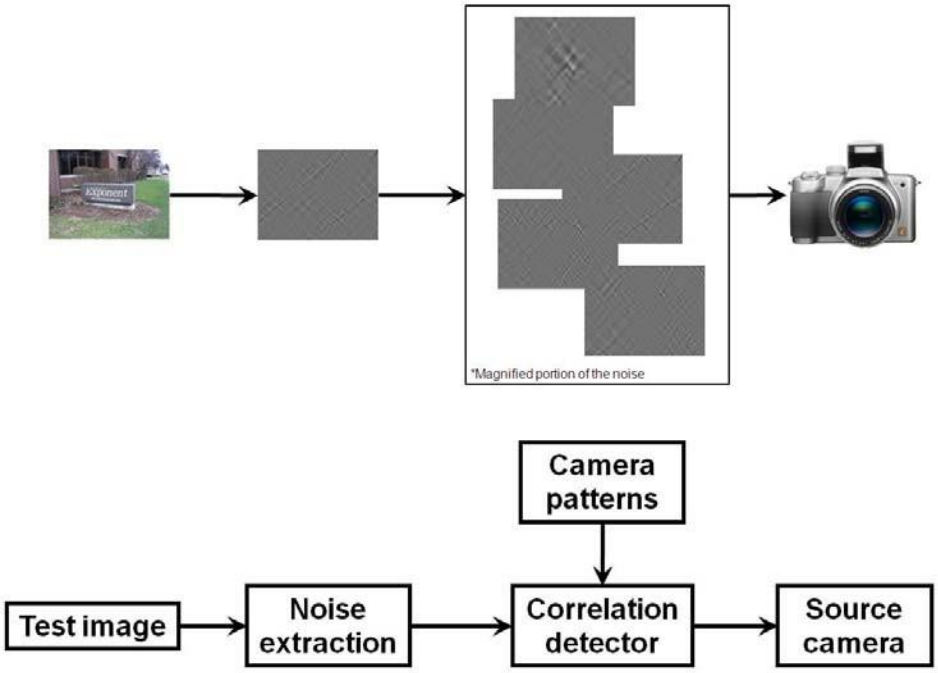
Digitalna kamera uglavnom koristi CCD/CMOS senzore slike. Šematski šum senzora slike se sa uspehom koristi za identifikaciju kamera. Visokofrekventni deo šematskog šuma je procenjen tako što se od originalne slike oduzima rašumljena verzija slike.

Filter za rašumljavanje baziran na vejvletima se koristi za rašumljavanje slika. Referentni obrazac kamere je određen vađenjem proseka šematskog šuma iz više slika uslikanih istom kamerom. Ovaj referentni obrazac služi kao unutrašnji potpis kamere (Slika 5.3). Koraci sa Slike 5.3 su nezavisno primenjeni na sve kamere u ovom trenažnom procesu. Slika 5.4 prikazuje korake u identifikaciji izvorne kamere sa nepoznate slike. Prvi korak je procena šuma senzora u test-slici koristeći filter za rašumljavanje. Zatim, šematski šum je u korelaciji sa referentnim obrascima kamere. Na kraju, kamera koresponduje referentnom obrascu tako što je najveća korelacija odabrana da bude izvorna kamera (Lukas 2005).

Postoje poboljšanja u metodologiji baziranoj na šumu senzora prezentovana u Lukas 2005. Ova poboljšanja prikazuju bolju procenu referentnih obrazaca kamere koristeći manje trenažne setove i poboljšanu klasifikaciju. U Chen-u 2007, 2008, prezentovana je poboljšana metoda identifikacije izvorne kamere zasnovana na zajedničkoj proceni i detekciji PRNU-a. Operacije nakon procesiranja primenjene na procenjene referentne obrasce redukuju pozitivnu korelaciju između referentnih obrazaca kamera istog modela i proizvođača i vov dalje redukuje lažne alarmne stope u razlikovanju kamera istog proizvođača i modela. Metode implementirane u sadašnjij studiji koriste proste metode proseka što dovodi do toga da analiza greške pokazuje niske netačne alarmne stope (do toga se došlo korišćenjem poboljšane metode za procenu senzora šuma predstavljenu u Chen 2007, 2008). Još jedno poboljšanje je dobijeno zamenom korelacije sa unakrsnom korelacijom i "vrha" (peak) za energiju korelacije (PCE) kao deo kriterijuma za donošenje odlka (Goljan and Fridrich 2008). Ovo eliminiše probleme sa nalaženjem eksperimentalnih pragova za korelacione vrednosti i umesto toga koristi Neyman-Pearson hipotezu - računanje pragova zasnovanih na izabranim lažnim alarmin stopama. Identifikacija izvorne kamere koristeći senzor šuma je proširena u Lukas 2006 (za detekciju falsifikata u slikama iz digitalnih kamera).



Slika 5.3: Prostup zasnovan na korelaciji



Slika 5.4: Identifikacija skenera koristeći šemu zasnovanoj na korelaciji

5.4 Eksperimentalni rezultati

U Tabeli 6.1 nalazi se lista digitalnih kamera korišćenih u eksperimentu. Svaka od ovih kamera je korišćena da napravi sliku u različitoj rezoluciji i kvalitetu slike dok su sva ostala podešavanja ostala na podrazumevana (auto fokus, ispravka crvenog oka, balans bele boje). Slike napravljene ovim kamerama imaju kako sličan tako i različit sadržaj. Slika 5.5 pokazuje uzorak slika korišćenih u eksperimentu.

	Device Brand	CCD Sensor	Sensor Resolution	Max. Picture Size	Image Format
c1	Canon PowerShot SD200-1	1/2.5 inch	3.2 MP	2048 x 1536	JPEG
c2	Canon PowerShot SD200-2	1/2.5 inch	3.2 MP	2048 x 1536	JPEG
c3	Nikon Coolpix 7600	1/1.8 inch	7.1 MP	3072 x 2304	JPEG
c4	Panasonic DMC-FZ20	1/2.5 inch	5 MP	2560 x 1920	JPEG/TIFF
c5	Nikon Coolpix 4100	1/2.5 inch	4 MP	2288 x 1712	JPEG
c6	Nokia 6630(3G smartphone)			1280 x 960	JPEG
c7	Olympus E-10	2/3 inch	4 MP	2240 x 1680	JPEG/TIFF
c8	Olympus D-360L			1280 x 960	JPEG/TIFF
c9	Panasonic Lumix DMC-FZ4-1	1/2.5 inch	4 MP	2304 x 1728	JPEG/TIFF
c10	Panasonic Lumix DMC-FZ4-2	1/2.5 inch	4 MP	2304 x 1728	JPEG/TIFF

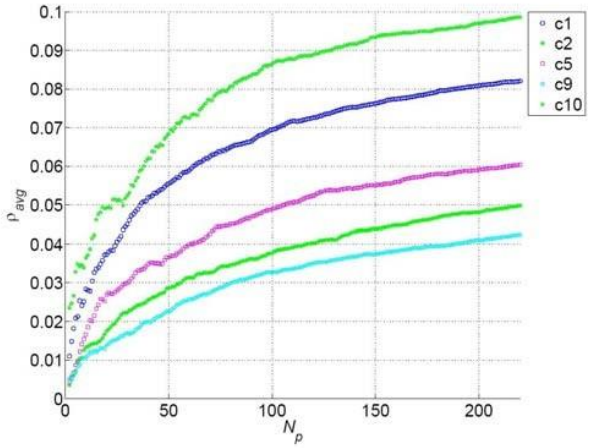
Tabela 5.1: Digitalne kamere korišćene u eksperimentu



Slika 5.5: Uzorci

5.5 Referentni obrasci kamere

Referentni obrasci kamere su dobijeni izvlačenjem proseka šuma izvučenog iz više slika napravljenih jednom kamerom. Nije neophodno da kamere imamo u svom posedu kao ni da posedujemo parametre dizajna već samo slike. Da bi se odredio broj neophodnih slika potrebnih za generisanje referentnog obrasca kamere, 20 nasumično odabranih slika se koriste kao slike za testiranje i prosečna korelacija (ρavg) između referentnog obrasca kamere generisanih iz Np trenažnih slika nacrtane su na Slici 5.6.

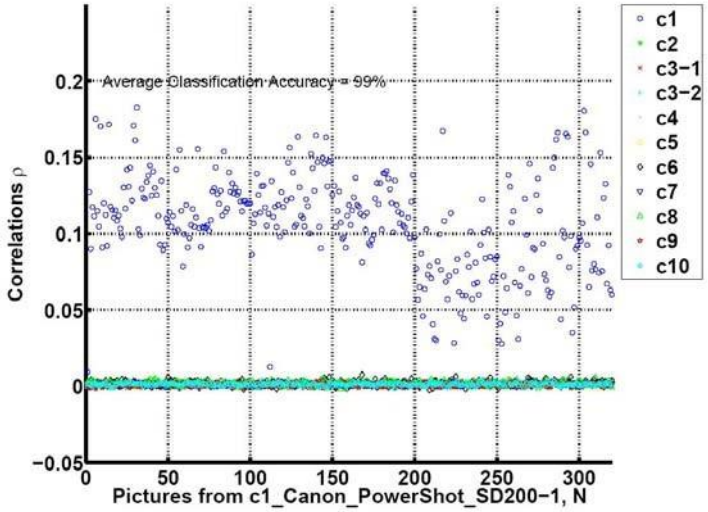


Slika 5.6: Prosečna korelacija kao funkcija broja lika korišćenih za kalkulaciju referentnog obrasca

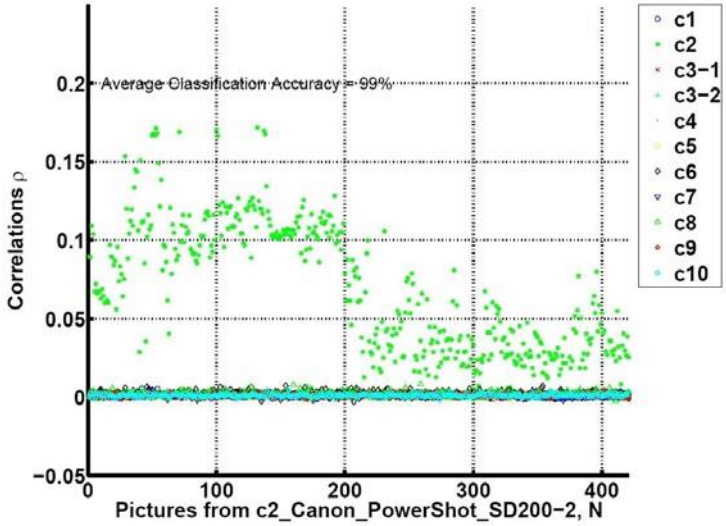
5.6 Identifikacija slike iz neprocesirane slike

U eksperimentu o identifikaciji izvorne kamere koristeći slike nepoznatog porekla, referentni obrasci kamere su procenjeni na osnovu 200 nasumično odabranih slika. Slike 6.7,6.8, 6.9, 6.10 i 6.11 prikazuju korelacione vrednosti za različite slike sa kamere sa referentnim obrascima svih ostalih kamera. Korišćeno je 11 referentnih obrazaca koji odgovaraju na 10 uzetih izvornih kamera. Za C3 kameru korišćena su dva referentna obrasca, jedan sa slike pri rezoluciji 3072x2304 i drugi sa slike pri rezoluciji 2048x1536. Ovo je urađeno da bi se videle razlike referentnih obrazaca na identifikaciju izvorne kamere. U ovim eksperimentima, za računanje korelacije između obrazaca šuma različitih

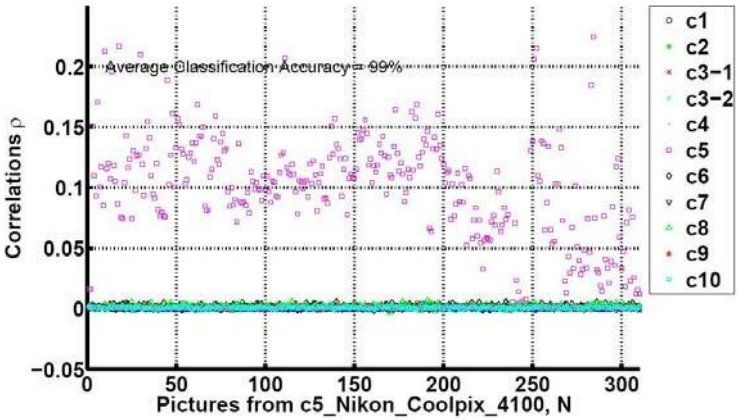
veličina, veća od dve je uvek kropovana od gornjeg levog ugla kako bi se izjednačila sa veličinom manje slike. Ekspeimenti su izvršeni tako što bi došlo do promene veličine slike pre rašumljavanja kako bi se izjednačila veličina referentnih obrazaca. Izvorna kamera je bazirana na referentnom obrascu dajući najveću korelacionu vrednost. U svim slučajevima preciznost klasifikacije je bila veća od 98%. Prvih 200 slika je odgovaralo onim namenjenim za procenu referentnog obrasca a ostale su korišćene za testiranje. Treba napomenuti da iako je korelacija između šeme šuma sa test slika i tačnog referentnog obrasca u poređenju manja nego korelacija između šeme šuma iz trenažnih slika i tačnog referentnog obrasca, korelaciona vrednost sa tačnim referentnim obrascem je mnogo veća nego ona sa netačnim referentnim obrascem. Korelacija sa tačnim referentnim obrascem je mnogo manja za slike na kojima je noć ili na onima dobijenim kad se zatvori zaštita sočiva kamere. Ova obzervacija je ostaje ista kod svih kamera.



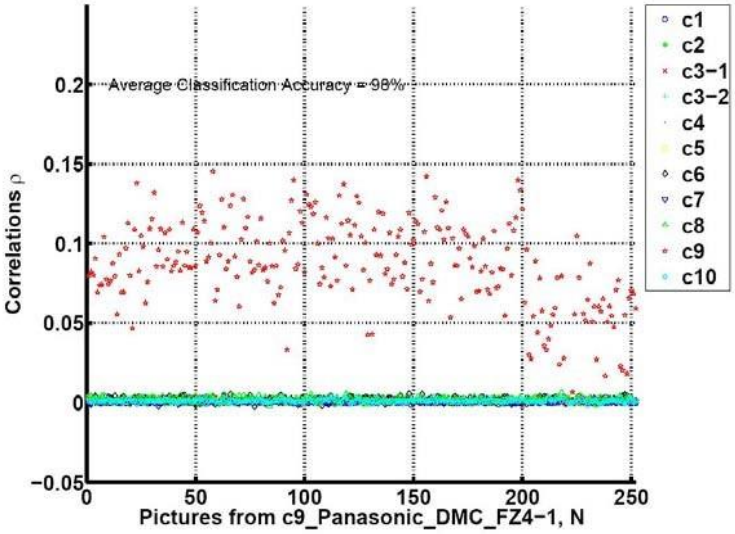
Slika 5.7: Korelacija šuma od C1 sa 11 referentnih obrazaca



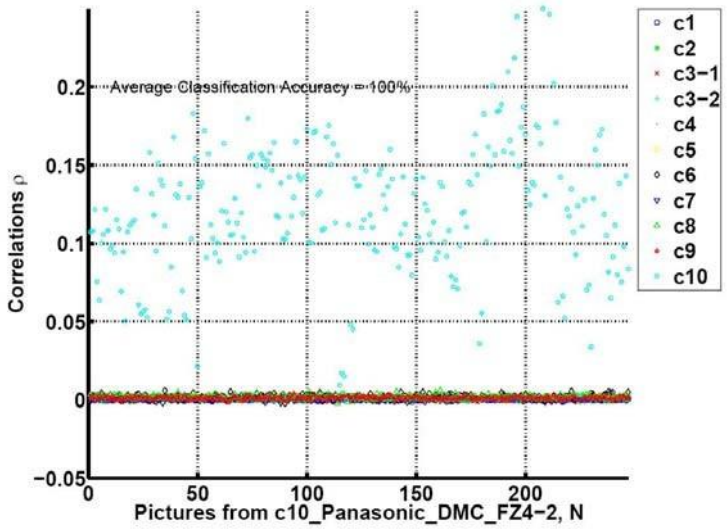
Slika 5.8: Korelacija šuma od C2 sa 11 referentnih obrazaca



Slika 5.9: Korelacija šuma od C5 sa 11 referentnih obrazaca



Slika 5.10: Korelacija šuma od C9 sa 11 referentnih obrazaca

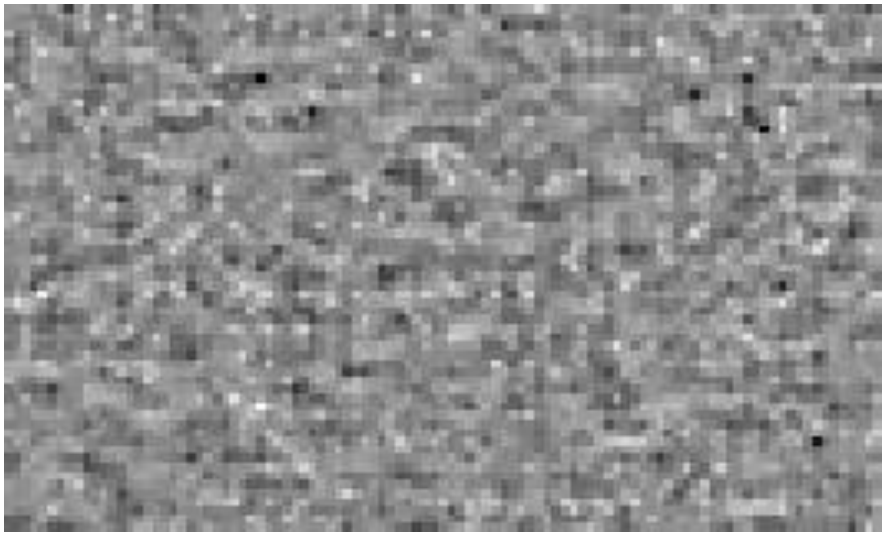


Slika 5.11: Korelacija šuma od C10 sa 11 referentnih obrazacaš [5]

5.7 Forenzika slike zasnovana na šumu senzora

Postoje dva tipa senzora slike koja se često nalaze u kamerama, kamkorderima i skenerima - CCD (Charge-Coupled Device) i CMOS (Complementary Metal-Oxide Device). Oba sadrže veliki broj foto detektora, takozvanih piksela. Pikseli su napravljeni do silikona i "hvataju" svetlo konvertujući fotone u elektrone koristeći fotoelektrični efekat. Akumulirani napon je prenešen do senzora, pojačan, a zatim konvertovan u digitalni signal u AD (analogno digitalnom) konverteru i dalje procesiran pre nego što se podaci sačuvaju u nekom od formata slike, kao što je JPEG.

Pikseli su obično pravougaoni, nekoliko mikrona popreko. Broj elektrona generisanih svetlošću unutar piksela zavisi od fizičkih dimenzija oblasti fotoosetljivih piksela kao i od homogenosti silikona. Fizičke dimenzije piksela malo variraju zbog nesavršenosti u procesu proizvodnje. Takođe, nehomogenost koja je prirodno prisutna unutar silikona doprinosi u varijacijama u kvantnoj efikasnosti među pikselima (sposobnost da konvertuje fotone u elektrone). Razlike u pikselima mogu biti "uhvaćene" matricom *K* koja je istih dimenzija kao senzor. Kada je senzor slike osvetljen sa idealno uniformnom svetlošću intenziteta *Y*, u odsustvu drugih izvora šumova, senzor registruje signal nalik šumu *Y+YK*. Termin *YK* se obično odnosi na neunifirmnost piksela do piksela (PRNU). Matrica *K* je odgovorna za veći deo onoga što nazivamo otiskom kamere. Otisak može biti eksperimentalno procenjen, npr. pravljenjem mnogo slika ravnomerno osvetljene površine i pravljenjem proseka tih slika kako bi se izolovale sistematske komponente svih slika. Istovremeno, vađenje proseka potiskuje komponente nasumičnog šuma kao što je šum samog uslikavanja (nasumične varijacije u broju fotona koji dospevaju do piksela izazvan kvantnim karakteristikama svetlosti) ili "pročitani" (readout) šum (nasumični šum predstavljen za vreme iščitavanja senzora)... Slika 5.12 prikazuje uveličan deo otiska sa Canon G2 4Mpix kamere koja sadrži porsečno 120 8-bitnih crno-belih (grayscale) slika . Svetle tačke odgovaraju pikselima koji konstantnije generišu više elektrona, dok tamne tačke odgovaraju pikselima koji proizvode manje elektrona. Varijacije u vrednostima piksela iz slike proseka (pre podešavanja raspona za vizuelizaciju) je 0,5 ili 21dB. Otisak senzora je obično slab signal (iako jačina signala značajno varira od modela kamera).

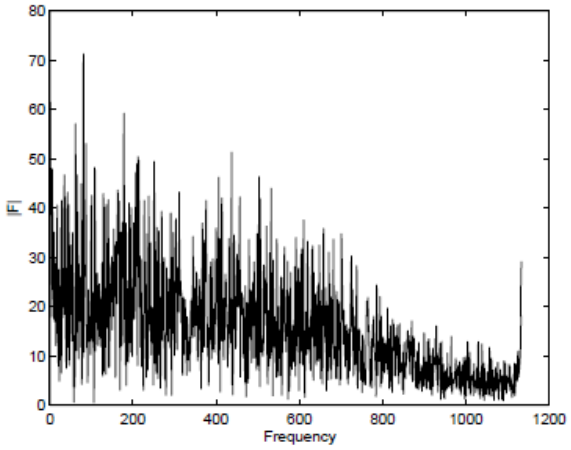


Slika 5.12: Uvećani deo otiska senzora dobijen iz uređaja Canon G2

Slika 5.13 prikazuje veličinu Furier transformacije jednog reda piksela u slici proseka. Signal je sličan belom šumu sa atenuiranom visokom frekvencijom.

Pored PRNU-a, otisak kamere sadrži sve sistematske defekte senzora uključujući mrtve i vruće piksele (piksele koji konstantno proizvode niske i visoke izlaze nezavisno od osvetljenja) kao i tzv. mračnu struju (obrazac nalik šumu koji bi kamera "uhvatila" dok je objektiv prekriven). Najvažnija komponenta otiska je PRNU. PRNU-ov izraz *YK* je jedva prisutan u mračnim oblastima gde je $Y \approx 0$. Takođe, kompletno zasićene oblasti slike, gde su pikseli ispunjeni do punog kapaciteta, proizvode konstantan signal, ne nose nikakve tragove PRNU-a ili bilo koje druge vrste šuma.

Treba naglasiti da su svi senzori slike (CCD, CMOS, JFET, or CMOS-Foveon™ X3) izrađeni od poluprovodnika i da su njihovi procesi proizvodnje slični. Zbog toga će ovi senzori verovatno izlagati otiske sličnih karakteristika.



Slika 5.13: Veličina Furier transformacije jednog reda otiska senzora

Iako je izraz PRNU po pririodi stohastičan, relativno je stabilna komponenta senzora za vreme svog životnog veka. Faktor *K* je zbog toga veoma koristan forenzički kvantitet odgovoran za jedinstven otisak sa sledećim važnim karakteristikama:

- **dimenzionalnost** - otisak je po prirodi stohastičan i ima visok sadržaj informacija, što ga čini jedinstvenim za svaki senzor
- **univerzalnost** - svi senzori slike izlažu PRNU
- **generalnost** - otisak je prisutan u svakoj slici nezavisno od optike kamere, podešavanje kamere ili sadržaja scene, sa izuzetkom kompletno mračnih slika
- **stabilnost** - stabilan je kroz vreme i pod uticajem raznih meteoroloških uslova (temperatura, vlažnost...)
- **robustnost** - preživljava gubitak kompresije, filtriranje, gama korekcije...

Otisak može biti iskorišćen za mnoge forenzičke zadatke:

- Testiranjem prisustva specifičnog otiska unutar slike, može se postići pouzdana identifikacija uređaja (dokazivanje da je određena kamera napravila određenu sliku). Prisustvo otiska kamere govori o poreklu slike - nastala je prirodnim putem a ne kao kompjuterski render.
- Ukoliko se ustanovi da otisak fali sa delova slike, moguće je otkriti maliciozne izmene na slici (verifikacija integriteta).

- Detektovanjem jačine ili forme otiska moguće je rekonstruisati deo istorije procesiranja. Npr. neko može da koristi otisak kao šablon za procenu geometrijskog procesiranja kao što je skaliranje, kropovanje ili rotacija. Negeometrijske operacije takođe mogu da utiču na jačinu otiska unutar slike i to potencijalno može biti otkriveno.
- Spektralne i prostorne karakteristike otiska mogu biti upotrebljene za identifikaciju modela kamere ili za pravljenje razlike između skenirane i uslikane slike. [6]

6. Studije slučajeva

U ovom poglavlju biće opisane sledeće studije slučajeva kao i analiza istih:

1. **Varez fabrika:** Slučaj nelegalnog umnožavanja CD-ova. Analizom slike potrebno je utvrditi lokaciju i vreme nastanka slike.
2. **Hodanje po Mesecu (Moonwalk):** Slučaj u kome treba utvrditi da li je slika astronauta Baz Oldrina autentična ili nije.
3. **Vojnik:** Slučaj britanskog vojnika. Sliku sa ratišta svojoj izdavačkoj kući LA Times dostavio fotograf Brajan Valski čije je uredništvo zaključilo da je reč o falsifikatu zbog toga što su primetili dupliranje ljudi iz mase.
4. **Dr. Ajman al Zavahiri:** Al-Kaida je jedna od najvećih terorističkih organizacija na svetu. S' vremena na vreme u etar puštaju video sadržaje sa ciljem zastrašivanja ili regrutovanja novih članova. Većina tih videa je editovana sa ciljem da se oda što je moguće manje informacija.

6.1 Studija slučaja 1: Varez Fabrika

Slika neovlašćenog CD umnožavanje objekta (slika 6.1) je nedavno predstavljena na forumu posvećenom Varezu. Na slici je prikazan CD duplikator, Inkpad za lepljenje "autentičnih" oznaka, pa čak i poklopce za CD. Međutim, nejasno je koliko dugo ova slika kruži internetom. Pitanje: kada i gde je ova slika nastala?

Jedini različiti tekst u sobi potiče sa Tarzan i Džejn filmskog postera i boce izopropil alkohol. Izoštravanjem ove slike i unapređenjem kontrasat, tekst postaje čitljiv (slika 6.2 i slika 6.3). Konkretno, tekst je na španskom, tako da je lokacija verovatno Meksiko, Venecuela, Argentina ili bilo koja druga zemlja španskog govornog područja. Boca alkohola uključuje tekst "Madrileno" (Madrid), što ukazuje na Španiju. Filmski poster za Tarzan i Džejn označava izdavanje tog DVD-a na dan 26. mart, ali se godina ne precizira. Film je pušten na DVD-u u Španiji 26. marta 2003. Imajući u vidu da se DVD promotivni posteri obično puštaju nekoliko meseci pre nego što video postaje dostupan i da je teško naći stavke odmah nakon izdavanja, Photo datum opseg može Procenjuje smože se proceniti datum nastanka slike: januar - maj 2003. Iako su na slici mnogi predmeti, ni jedan predmet se ne može identifikovati sa godinom izvan 2003. godine.

Pored datuma i lokacije, karakteristike prostorije su prepoznatljive, na primer telefonski priključak. Ovo govori da ta prostorija prvobitno nije bila namenjena za ovu prostoriju. Pošto soba nije bila opremljena sa standardnim RJ45 priključkom, dolazi se do zaključka da je taj deo dodat isključivo zbog ovih kompjutera. [3]



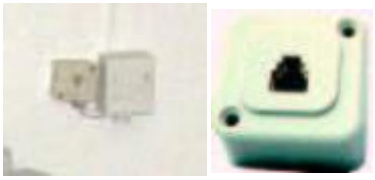
Slika 6.1. neovlašćeno fabrika CD-dupliranje. [7]



Slika 6.2. Tarzan & Jane plakat najavljujući DVD izdanje (mart 26). Ova slika je bila izoštrena.



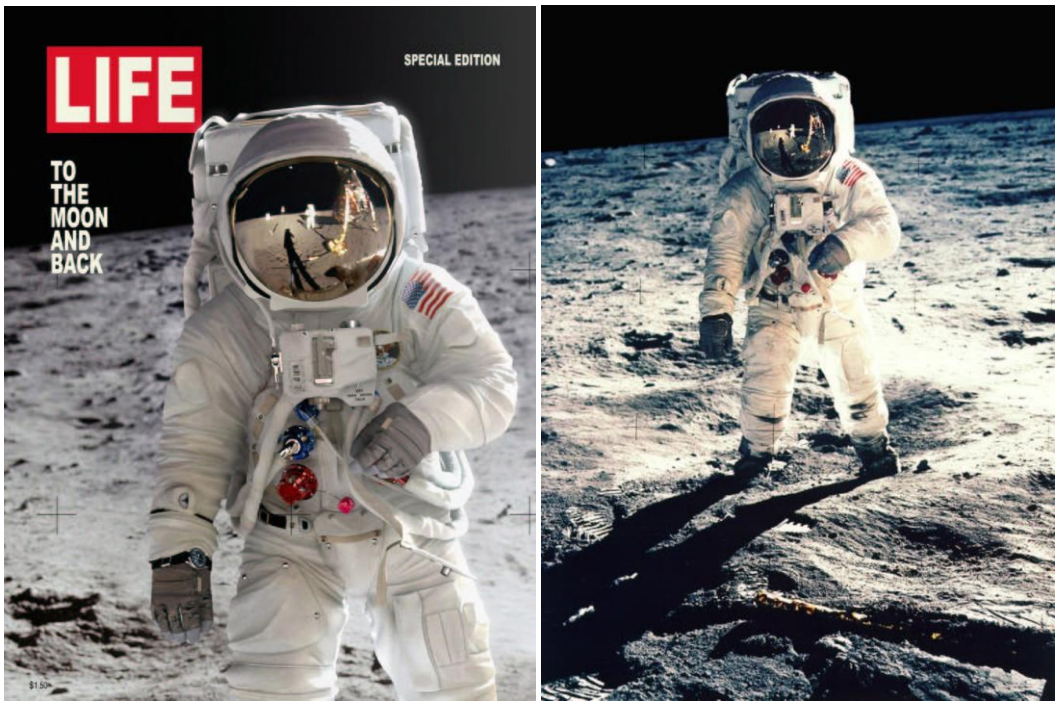
Slika 6.3. Izopropil alkohol bočica sa španskom oznaka. Ova slika je bila smanjena, izoštrena i promenjen joj je kontrast



Slika 6.4. Telefonska utičnica [8]

6.2 Studija slučaja 2: Moonwalk

U 2006. godini, Andrea Bertaccini je bio nagrađen "CG Izbor Nagrada" od strane CG društva za pružanje čuvenog Buzz Aldrinovog Mesečevog hoda (Slika 6.5). Prema umetniku, slika je bila zasnovana na originalnoj NASA fotografiji. Međutim, detalji unutar slike ukazuju na dodatne resurse. [3]



Slika 6.5. Slika Andrea Bertaccini i originalnog NASA foto (Desno).[9]

Poređenje dve fotografije ukazuje na značajan broj razlika. Dok je nedostatak mesečeve prašine na slici umetnika očekivan, ostale razlike su zanimljive:

- **Pufnasto.** CG svemirsko odelo deluje "izduvano" dok je pravo odelo naborano.
- **Vlakna.** Pravo odelo ima različite vlakna vidljiva na rukama, slična vunenom džemperu. CG slici fale ta vlakna.
- **Zavrtanj za uzemljenje.** Kutija na torzou (slika 8.6) u originalu pokazuje zavrtanj za uzemljenje u tamnoj boji u centru. Međutim, umetnik koristi zavrtanj svetle boje.
- **Konektori.** Crveni i plavi konektori na torzou kod umetničke slike pokazuju šest vrlo reflektnih zavrtanja. Ovi zavrtnji nisu vidljivi na pravoj

fotografiji.. Pravo odelo je malo ove zavrtnje ali oni nisu emitovali refleksiju.

- **Pojas.** Umetnikov pojas ima metalne kopče. NASA-ina fotografija pokazuje da nema metalne kopče na pojasu.

Ova odstupanja mogu biti posledica izvora slike. Umetnikova slika je objavljena u 2006. U 2005. godini, IMAKS proizvodi film pod nazivom Magnificent Desolation u kojem nanovo urađen čuveni Mesečev hod. Zakulisna slika iz ovogj film (Slika 6.7) pokazuje odelo slično Bertaccinijevoj slici: odelo deluje izduvano a ne naborano, nema vidljivih vlakna na rukama, zavrtanj za uzemljenje je svetle boje, konektori na torzou imaju šest zavrtnja koji emituju refleksiju, a pojas ima metalnu kopču. Dok je pozicioniranje Bertaccinija zasnovano na NASA-inoj fotografiji, svemirsko odelo je izgleda zasnovano na osnovu IMAKS rekreacija.



Slika 6.6: Close-up detalja torzo na rekreaciju i originala slika



Slika 6.7. Iza kulisa fotografija iz IMAKS filma Veličanstvena Pustoš.

6.3 Studija slučaja 3: Vojnik

Izmenjene slike često se pojavljuju na onlajn forumima, televiziji, filmovima i oglasima bez mnogo zabrinutost. Međutim, postoji stigma kada se pojave u masovnim medijima i novinskim kućama. Pošto izveštači treba da izveštavaju o činjenicama, pojačane ili modifikovane slike mogu lako pogrešno da predstave realne situacije ili da obmanjuju čitaoce.

U 2003. godini, fotograf Brajan Valski poslalao je fotografiju jednog britanskog vojnika u Basri. Ova slika je identifikovana kao lažna nakon što su urednici primetili dupliranje u masi ljudi - što je dovelo do otpuštanja Valskog je iz Los Anđeles Tajmsa. Veruje se da je slika, zapravo, kombinacija dve starije slike koje je napravio Valski. (Slika 6.8).



Slika 6.8: Slike 1 i 2 su originali koji su iskombinovane da bi se dobio falsifikat (slika 3). Slika 4 pokazuke pokušaj ponovnog kreiranja falsifikata "nalepljivanjem" originala koristeći Gimp.

Dve originalne slike se mogu kombinovati da bi se ponovilo falsifikovanje i otkrije kako je verovatno napravljena. Posmatranjem slike nagoveštava se da je veći deo falsifikata nastao iz prvog originala - sve desno od vojnika je sačuvano. Druga originalna slika je bila isečena, ostavljen je samo vojnik i ljudi sa njegov leve strane. Drugi original je uvećan i iskombinovan je sa drugom slikom. Naposletku, kombinacija je bila značajno prefarbana i nebo je bilo modifikovanp.

Međutim, originalni izvori su uglavnom nepoznati. Koristeći tehnike pokrivene u ovom radu, lažna slika može da se analizira bez pomoći originalnih slika (Slika 6.9).

- **Posmatranje.** U kombinovanoj slici, čovek u belom koji čuči (dole levo, iza vojnikovih nogu) je dupliran (ispred kolena vojnika). Međutim, kopije nisu identične; jedan ili oba su, izgleda, bili smanjeni.
- **Meta informacije.** JPEG ne sadrži informacije kamere. Međutim, to ne uključuje Adobe- specifične meta podatke, što ukazuje da je izmenjeno pomoću Adobe alata.

- **Analiza kvantizacionih tabela.** Kvantizaciona matrica je nepoznata, ali kvalitet je približno 72%.
- **ELA.** Analiza nivoa greške pokazuje da je nebo na jednom nivou greške, ali svi ljudi su na različitom nivou greške. Ovo je zapravo zbog ponovnog farbanja slika (recoloring), ali ELA identifikuje samo promenu.
- **PCA.** PC1 pokazuje da je nebo sačuvavano mnogo puta. Vojnik i ljudi sa njegove leve strane su bili sačuvani nekoliko puta. Drugi ljudi u grupi nisu bili sačuvani mnogo puta. PC1 sumira sliku u tri regije: nebo, vojnik i ljudi sa njegove leve strane i ljudi sa njegove desne strane.
- **Vejvlveti.** Na 8% od vejvleta, vojnik se pojavljuje hrskav ali sa mnogim područjima prelaza oštre boje. Ovo sugeriše da je veličina njegove slika bila izmenjena da bi odgovarala slici. Čovek u kariranoj košulji (desno) ima hrskavo lice, "rešeno" je na oko 2% od raspoloživih vejvleta. Međutim, čovek u belom iza njega i dete ispred njega oba imaju mutna lica, što ukazuje na tri različita sloja. Puna analiza vejvleta sugeriše da ljudi mogu da formiraju do devet različitih slojeva.

Procenjujući ELA, PCA, primećeno dupliranje i različite procente renderovanih vejvleta, jasno je da je slika izmanipulisana. Međutim, detalji manipulacije su neubedljivi. Značajan recoloring, mala veličina i niska rezolucija povećavaju lažno-pozitivan rezultati u analizi. Ako se ova pitanja ignorišu, onda slika izgleda da uključuje jedanaest ili više različitih slojeva koji su kombinovani da formiraju sliku. Međutim, ova slika je znatno izmenjena. Analiza pokazuje da može da sadrži tri sloja: vojnik i ljudi sa njegove leve strane, zemlja i ljudi desno od vojnika i nebo.

Najveća nedoslednost u analizi dolazi iz PCA i vejvlet analize. (Za ostale slike, druge metode analize mogu dati nekonstantne rezultate.) U ovom slučaju, vejvleti pokazuju da se čovek kariranoj košulji brzo"razlaže". Ovo je zbog harmonične frekvencije a ne zbog manipulacije. Ni jedan od originala ne pokazuje nepravilnost sa čovekom u kariranom, ali pokušaj rekreacije pokazuje iste karakteristike vejvleta.

Sintija Baron je ponudila sledeći predlog za utvrđivanje harmonično sastavljenih regiona: vejvlet analiza koristi simetrične veličine slike (npr. 512x512 ili 1024x1024) i obrađuje jedan pravac pre nego što pređe na drugi (npr. horizontalno pre vertikalnog). Rotiranje slike pre obavljanja vejvlet analize može pomeriti ili ukloniti lokacija bilo kakvog harmoničnog sastavljanja. U tom slučaju, okretanjem falsifikovane slike uklonjena je "hrskavost" čoveka u kariranoj košulji i smanjena je oštrina u licu.



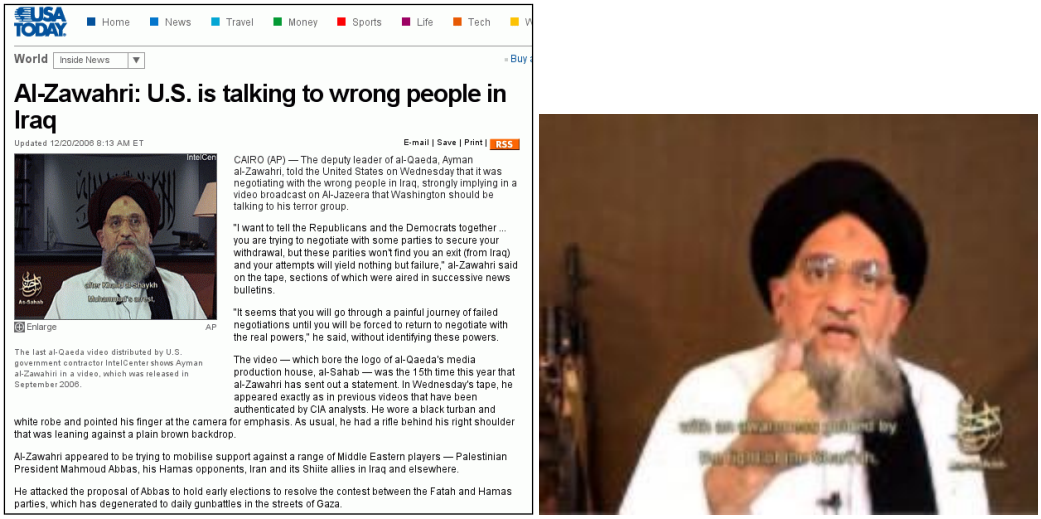
Slika 6.9: 1: Modifikovana slika Brajana Valskog; 2:ELA; 3:PCA; 4: render koristeći 8% slobodnih vejvleta

6.4 Studija slučaja 4: Dr. Ajman al Zavahiri

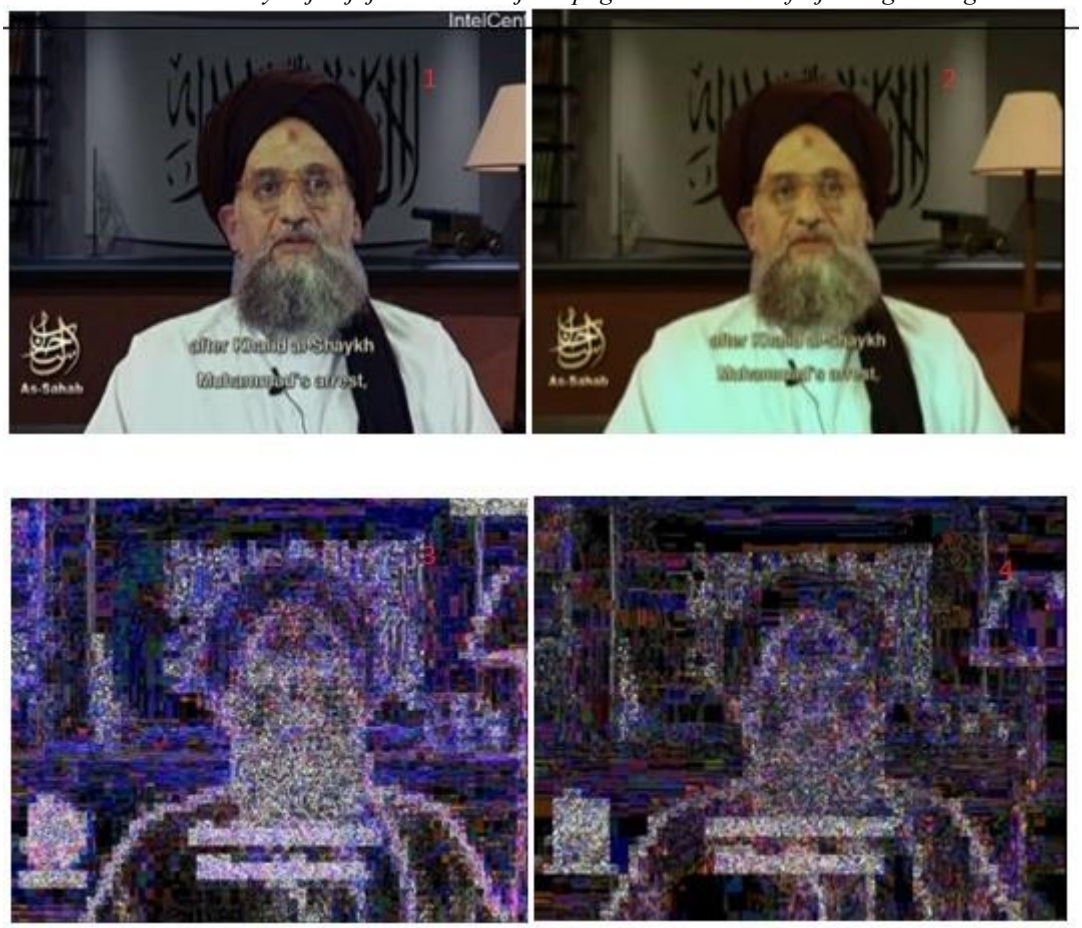
As-Sahab je ogranak video proizvodnje Al Kaide. Oni povremeno pustite video dizajniran da podseti ljude na postojanje Al Kaide, izdavanje pretnji, regrutovanje novih članova i potencijalno deluje kao tajni kanal za aktiviranje terorističkih ćelija. Mnogi od videa AS-Sahaba su manipulisani.

20.12.2006, Dr. Ajman al Zavahiri (drugi čovek Al Kaide) objavio je video snimak. USA Today je pokrio taj video sa naslovom pričom (Slika 6.10). Opis videa kaže: "On je nosio crni turban i belu odeću. Imao je pušku iza njegovog desnog ramena koja je naslonjena na običnoj braon pozadini. " Iako je ovo je validan opis As-Sahabovog videa, na slici koju koristi USA Today nisu pokazali tu sliku. Umesto toga, SAD danas koristi sliku iz drugog videa, od 28.92006. Ovo je primer zamene slika.

Slika koju je USA Today odlučio da upotrebi uključuje mnoge druge zanimljive karakteristike. Prvo, dobijena je od IntelCenter-a (www.intelcenter.com) - organizacije koja prati terorističke aktivnosti. IntelCenter je postavio njihov logo u gornjem desnom uglu videa. Međutim, ime kompanije je jasno izrezano - verovatno od strane USA Today. Poređenje sa istim kadrovima iz originalnog video pokazuje mnoge druge vidljive razlike. Konkretno, IntelCenter je promenio boju i oštrinu slike (Slika 6.11).



Slika 6.10. USA Today najavljuje video izdanje sa pogrešnom slikom i frejm originalnog videa.



Slika 6.11 1: Slika dobijena od IntelCenter-a i prezentovana od strane USA Today-a; 2: Pravi frejm iz videa; 3, 4: 95% ELA za svaku sliku

Posmatranje u kombinaciji sa 95% ELA pokazuje redosled modifikacija. Promene, počevši od najnovije i rad unazad:

- **Kropovanje.** Poslednja promena je bila da slika bude kropovana (isečena).
- **IntelCenter.** IntelCenter je dodao njihov logo.
- **Bojenje.** Slika je nanovo obojena i izoštrena, modifikujući stopu greške duž slike.
- **As-Sahab.** As-Sahabov logo i podnaslov teksta su dodati.

- **Al Zavahiri**. Zavahiri je dodat u slici. ELA jasno pokazuje jasnu promenu nivoa grešaka između njega i pozadine. Ova vrsta "oreol" greške je uobičajena za chroma-key (zeleni ekran) slike. Posebno, postoji prepoznatljiv nivo greške generisan chroma-key zamenama: pošto je većina chroma-key algoritama zamene bazirano na nijansama i ne zasićenju ili osvetljenju, drugačije boje duž šava su u različitim nivoima grešaka.
- **Baner.** Baš kao što tekst može biti dodat na prazan znak, izgleda da je neko dodao tekst u baner iza Zavahirija.

PC1 i vejvlet analize za ovu sliku takođe podržavaju ove zaključke. Pozadina kancelarije izgleda da je zasnovana na sloju koji je bio sačuvan više puta. Tekst banera je bio verovatno dodat u isto vreme kada je dodat i Zavahiribio, dok su logo As-Sahab-a i prevodi dodati poslednji.

Drugi Al Zavahirijev video

Video od 28.9.2006 nije bio samo izmanipulisani video. U stvari, mnogi od Al-Zavaharijevih videa koji su bili ispitani bili su pozitivni na chroma-key maskiranje. Uzevši u obzir video izdat 27.7.2006 (slika 6.12), na videu se prikazuje Al Zavahiri kako sedi u video studiju.

Kada je ovaj video izašao, mnogi Amerikanci su postali besni na američku vladu. Glavni razlog za razdor je bio u jednom argumentu: ako Al Zavahiri sedi u studiju snimajući video, zašto ne možemo da ga uhvatimo? Odgovor je jednostavan: nije u studiju.

- **Posmatranje.** Pozadina studija pokazuje refleksije iznad skele. Ipak, ne postoje senke ispod skele.
- **ELA.** ELA na 95% pokazuje chroma-key oreol oko Zavahirija. As-Sahabov logo je dodat poslednji. Pozadina pokazuje obrazac koji se ponavlja što ukazuje na čvrstu podlogu boja pozadine. Pošto digitalna kamera dodaje šum na slikama, boaj pozadine nije iz digitalnog fotoaparata - nacrtana je.
- **PCA PC1.** Linija izgrađena od PC1 pokazuje da je pozadina više puta sačuvana, tri slike iza Zavahirija imaju tri različita nivoa sačuvavanja, Zavahiri ima različit nivo i As-Sahabov logo ne prikazuje JPEG artefakte. Ovo ukazuje da je slika napravljena pomoću najmanje šest slojeva.
- **PCA PC3.** Udaljenost od treće linije glavne komponente kao i oblast prve glavne komponente naglašava osvetljenje u sobi. Veliki prsten osvetljenja se može posmatrati na Zavahiriju kao i pozadini. Pošto je osvetljeni deo iza Zavaharija neznatno veći nego svetlo na njemu samom, ekran iza njega je od njega udaljen od 30cm do 60cm. Osvetljenje pruža osećaj da je u pitanju veliki studio.
- **Vejvleti.** Na 5% vejvleta pokazuje se šest različitih slojeva. Mohammad Alef (levo u pozadini) veoma mutan, Svetski trgovinski centar je mutan, Muhamed Ata (desno u pozadini) je skoro oštar, Zavahiri je oštar i As-Sahabov logo je veoma oštar i pokazuje oštre boje prelaza.

Pošto je pozadina crtana i uključuje drugi slike, pitanje postaje: odakle dolaze druge slike? Slika od Mohameda Ate (pozadina desno) izgleda da je iz fotografije nađene u izveštaju Komisije 9/11. Ova slika je smanjene veličine i iskrivljena je tako da se uklapa u

pozadinu. Slika Mohammada Alefa (pozadina-levo) može biti iz videa nastalog na venčanju između njegove ćerke i sina Osame bin Ladena sina.



Slika 6.12: 1: slika iz 28.6.2006; 2:ELA na 95%; 3:PC1; 4: PC3; 5: Vejvlet na 5%; 6: Muhamed Ata iz vladinog 9/11 izveštaja

U većini videa Muhamed Alef nosi belu majicu. Slika sa venčanja ukazuje na to da je nosio majicu sličnu ovoj sa slike.

Tvrdeći da je postojala chroma-key pozadina nije isto što i da je stvarno vidimo. 22.01.2007 institut SITE (www.siteinstitute.org) - organizacija koja prati terorističke aktivnosti - je objavio da su presreli Al Kaidin video pre nego što je bio javno objavljen. SITE ga je pustio. Tri dana kasnije, As-Sahab takođe je objavio video.

Video (Slika 6.13) pokazuje Al Zavahirija ispred crne zavese. Zavesa nije pravilno centrirana prema kameri - postoji klin stvarne pozadine u gornjem desnom uglu. Promena osvetljenosti slike pokazuju da je zavesa okačena o šipku. Iako ovo može biti obična crna tkanina, izgleda da imaj jedinstvenu boju. Tkanina može da bude vrsta chroma-key pozadine koja se zove "Chroma-key sheet". Normalno, chroma-key pozadine su postavljene na zid kako bi se smanjila mogućnost pojave nejednakog osvetljenja. Međutim, chroma-key sheet je nakačen na metalni okvir (Slika 6.14) i može se pokazati nabor usled vešanja.



Slika 6.13: Kadar od 25.1.2005 As-Sahabov video (levo) i poboljšanje boja (desno).



Slika 6.14: Chroma-key sheet.

Drugi videi Al Kaide

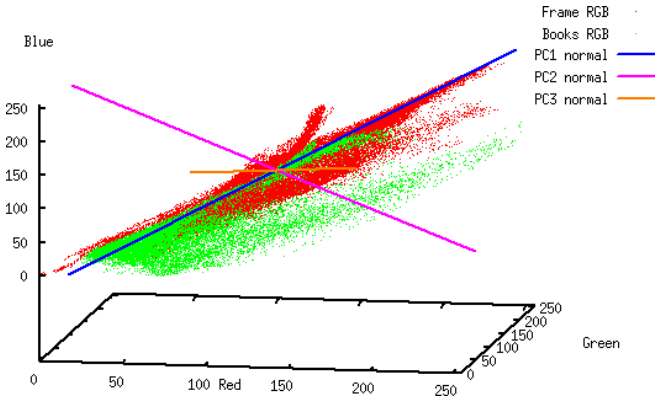
Videi sa Al Zavahirijem nisu jedini As-Sahabovi videi. 2.9.2006. godine, Azzam al-Amriki prikazan je u video snimku (Slika 6.15). Video ga prikazuje u beloj sobi sa radnim stolom, kompjuterom i nekim knjigama. Međutim, 95% ELA ukazuje na to da knjige ne postoje u sobi. Dok su računar, zidovi, sto i Azzam u jednom nivou greška, knjige,titlovi i As-Sahabov logo pojavljuju se na različitim nivoima greške. PC1 pokazuje da se raspon boja knjiga veoma razlikuje od ostatka na slici,kao i da one dolaze iz alternativnog izvora. [3]



Slika 6.15: 1: Azzam al-Amriki sa videa iz 2.9.2006; 2:ELA 95%; 3: PC1; 4:PC1 sa povećanim kontrastom

PC1 sa podešenim kontrastom pokazuje obrazac horizontalnih linija. Ovo je medijski artefakt; originalni video Azzama koristio je isprepleteni video izvor koji je identifikovan od prve glavne komponente. Međutim, dok su horizontalne linije veoma vidljive na pozadini i blago vidljive na Azzamu, nisu vidljive na knjigama ili As-Sahabovom logou. To sugeriše da ovaj video nije stigao iz idprepletanog video izvora.

Rasturanje zemljišta boja koje su korišćene u al-Amrikijevom videu prikazuje tri različite boje regiona (slika 6.16). Glavna gusta oblast sadrži boje nađene preko većeg dela slike: Azzam, zidovi, sto i računar. Mali vrh u centru sastoji se od boja se nalaze u As-Sahabovom logou i prevodu. Ove boje ne pojavljuju nigde drugo u slici i one formiraju nezavistan klastera. Izvan glavnog spektra slike su boje nađene u knjigama. Spektar boja knjiga je izrazito izvan glavnog kolorita slike. Ovo implicira da knjige verovatno nisu iz istog snimka kao i al-Amriki.



Slika 6.16: 1. "Rasejanje zemljišta" Azzam al-Amrikijevog videa. Knjige su zelene boje.

7. Zaključak

U ovom delu rada govorićemo o ostvarenim doprinosima u ovom master radu. Pored teorijskih doprinosa važno je istaći da postoje i značajni praktični doprinosi u vidu prikazanih studija slučaja. Takođe, navešćemo smernice u budućem radi i istraživanju u ovoj oblasti digitalne forenzike.

7.1 Ostvareni doprinosi

Jedna od najvećih prednosti života u dobu visoke tehnologije i socijalnih mreža jeste dostupnost podataka. Kao jedan od najuticajnijih vidova socijalne kulture danas jeste razmena slika. Usled široke dostupnosti softvera namenjenih za editovanje slika, svaka slika koja se nalazi "na mreži" postaje meta ljudi koji imaju za cilj njenu zloupotrebu. Slike su lako podložne manipulaciji i nevešto i neiskusno ljudsko oko u stanju je da poveruje u ono što vidi iako to nije tačno, što je značajno ukoliko ni u pitanju bile osobe od uticaja. Ovim radom smo kroz primere i duboku analizu, objasnim važnost forenzike slike. Predstavljeno je nekoliko načina analiza slike i može se izvući zaključak da je forenzika slike izuzetno važna grana digitalne forenzike čije metode analize daju rezultate ali i da pojedine metode zbog svojih nesavršenosti nisu podobne za sudstvo i na njima se zahteva dodatan rad i usavršavanje.

Navešćemo neke od najvažnijih doprinosa ostvarenih ovim radom:

- dat je teorijski pregled metoda koji su danas u upotrebi za analizu slike;
- dati su načini preko kojih se detektuje kompjuterski generisana slika, osnovna razlika između ovih i drugih vrsta digitalnih slika kao i otkrivanje da li je došlo do izmena u analiziranoj slici u odnosu na njeno prvobitno stanje;
- opisana je tehnika identifikacije uređaja i važnost takve analize;
- objašnjena je vremenska forenzika i zbog čega je značajna kao i koji su ciljevi kontra-forenzike;
- rad "pokriva" neke česte i neke ne tako česte forenzičke metode za vađenje podataka iz digitalnih slika;
- opisuje metode za razlikovanje prave slike od kompjuterski generisanih, i identifikuje kako je slika digitalno izmanipulisana;
- predstavlja principe i motive digitalne forenzike (sa fokusom na sliku i video) kao i opisivanje dva glavna načina pristupa u rešavanju dva osnovna pitanja: koji je izvor digitalnog sadržaja i da li je taj digitalni sadržaj autentičan ili nije?;
- dat je pregled dostupnih alata kojim će forenzičar otkriti poreklo, autentičnost i vlasništvo nad slikom;
- prikazano je nekoliko studija slučajeva kao i forenzički pristupi za analizu;

7.2 Predlog budućeg rada

U ovom diplomskom radu analizirane su metode za digitalnu analizu slike – forenzika slike. Za potrebe daljih istraživanja i budućeg rada razmotrićemo još neke metode koje nisu obuhvaćene ovim istraživanjem, a koje mogu dodatno da doprinesu postizanju boljih rezultata. Kao krajnji cilj, nameće se razvoj jednog forenzičkog alata za forenziku digitalnih slika.

Literatura:

[1] Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko, „Comprehensive Study on Cybercrime 2013, United Nations office on drugs and crime“, New York, Februar 2013.

[2] Roberto Caldelli, Irene Amerini, Francesco Picchioni, Alessia De Rosa and Francesca Uccheddu, „Multimedia forensics tehniques for aquisition device identification and digital image autentification“, Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions., 2010.

[3] Matthias Kirchner, „Notes on digital image forensics and counter forensics“, tekst preuzet iz doktorske disertacije, septembar 2012.

[4] Nitin Khanna, Aravind K. Mikkilineni and Edward J. Delp, Forensic Camera Classification: Verification of Sensor Pattern Noise Approach (2009), in: Forensic Science Communications, 11:1.

[5] Nitin Khanna, Aravind K. Mikkilineni and Edward J. Delp, Scanner Identification Using Feature-Based Processing and Analysis (2009), in: IEEE Transactions on Information Forensics and Security, 4:1(123-139)

[6] Jessica Fridrich, „Digital image forensics using sensor noise“, IEEE Signal Processing Magazine, vol. 26, no. 2, March 2009, pp. 26-37.

[7] Digital Camera Identification from Sensor Noise, with J. Lukas and M. Goljan, IEEE Transactions on Information Security and Forensics, 1(2), pp. 205-214, June 2006.

[8] Sensor Defects in Digital Image Forensics, Chapter in an edited book "Digital Image Forensics: There is More to a Picture than Meets the Eye", editors H. T. Sencar and N. Memon, Springer, May 2012. ISBN: 978-1-4614-0756-0.

[9] www.hackerfactor.com

[10] www.bork.ca/pics/?incoming/varez_factori.jpg

[11] www.phonecoinc.com

[12] www.tredistudio.com

[13] www.nasa.com