SVEUČILIŠTE U ZAGREBU
GRAFIČKI FAKULTET

MARKO MARIČEVIĆ

FORENZIKA DIGITALNOG ZAPISA FOTOGRAFSKE SLIKE

DIPLOMSKI RAD

Zagreb, 2013.

Sveučilište u Zagrebu
Grafički fakultet

MARKO MARIČEVIĆ

FORENZIKA DIGITALNOG ZAPISA FOTOGRAFSKE SLIKE

DIPLOMSKI RAD

Mentor:
v. pred. dr. sc. Miroslav Mikota

Student:
Marko Maričević

Zagreb, 2013.

ABSTRACT

With popularization of digital photography new means of counterfeiting are constantly emerging. Besides that there is a growing need for authenticity verification. Today there is a variety of digital image manipulation applications. Therefore it is more and more easy for counterfeiters to relay altered messages to the viewers. There are methods for detecting these kinds of manipulations even when there are no visual sings of image tampering. However in some cases it is necessary to apply multiple layers of analysis. The topic of this masters thesis are aforementioned methods for the JPEG digital image files analysis. In regard with authenticity verification the main focus will be observing and comparing basic characteristics and file structure of the JPEG format. Theoretical part is based on known forensic methods witch are thoroughly tested in experimental part with suggested models of improvement.

Key words: computer forensics, JPEG, image tampering, authentication

SAŽETAK

Svakodnevnim povećanjem korištenja digitalne fotografije otvaraju se vrata za nove i kreativne načine krivotvorenja fotografije. Uz to javlja se i potreba ocjene autentičnosti fotografije. Velika raznolikost i pristupačnost aplikacija za digitalnu obradu digitalnog zapisa fotografske slike omogućila je vizualno uvjerljiv prikaz krivotvorene fotografije koji na gledatelja ostavlja drugačiji dojam te prenosi drugačiju,odnosno krivotvorenu poruku. Zbog potrebe za dokazivanjem autentičnosti digitalnog zapisa fotografske slike su nastale metode za analizu tog zapisa koje mogu otkriti odstupanja od realnog zapisa i onda kada ne postoje vizualni znakovi obrade fotografije. Međutim, neke tehnike analize ne mogu detektirati određene metode manipulacije nad fotografijom te je potrebno primijeniti više tehnika detekcije i analize digitalne fotografije. Ovaj rad se bavi metodama za analizu i detektiranje krivotvorenja digitalne fotografije s obzirom na digitalni zapis i strukturu JPEG formata. S ciljem dokazivanja autentičnosti u radu će biti predstavljene i opisane metode temeljene na promatranju i usporedbi osnovnih karakteristika JPEG zapisa i poznatim karakteristikama kreiranja digitalnog JPEG zapisa. U teoretskom dijelu su rada analizirana postojeća saznanja uz poznate metode analize, tj. forenzike, digitalnog zapisa fotografije te je u eksperimentalnom dijelu rada ispitana forenzika digitalnog zapisa fotografije i predloženi su modeli unaprijeđena aktualnih metoda.

Ključne riječi: računalna forenzika, JPEG, manipulacija, autentifikacija

SADRŽAJ

1 UVOD

Svakodnevnim korištenjem digitalne fotografije u profesionalne ili amaterske svrhe otvaraju se vrata za nove i kreativne načine krivotvorenja fotografije. Napretkom tehnologije i mogučnošću ugradnje digitalnog fotoaparata u danas skoro svaki elektronički uređaj među kojima su: prijenosno računalo, dlanovnik, mobilni telefon te pristup širokopojasnom pristupu Internetu omogućili su vrlo brzo dijeljenje fotografija i njihovo publiciranje na Internetu. S novim tehnologijama i trendovima nastali su novi, jednostavniji računalni programi za obradu digitalnih fotografija. Zbog tog problema se javlja potreba za dokazivanjem autentičnosti digitalne fotografije. Velika raznolikost i pristupačnost računalnih aplikacija za digitalnu obradu digitalnog zapisa fotografske slike omogućila je vizualno uvjerljiv prikaz krivotvorene fotografije koji na gledatelja ostavlja drugačiji dojam te prenosi drugačiju tj. krivotvorenu poruku. Svaka digitalna fotografija je konačni binarni zapis napravljen nizom matematičkih algoritama. Matematički algoritmi se ponašaju po unaprijed poznatim pravilima te svaka promjena utječe na konačni zapis digitalne fotografije. Upravo je zbog toga moguće analizirati digitalnu fotografiju u potrazi sa nepravilnostima u strukturi digitalnog zapisa i u samoj strukturi digitalne fotografije.

Svaka digitalna fotografija smatra se jedinstvenom te joj na taj način treba pristupati pri analizira. Zbog toga nije moguće napraviti jedinstveni model analize digitalnih fotografija već je potrebno primijeniti niz različitih tehnika kako bi se otkrile potencijalne greške ili manipulacije. Ovaj se rad bavi metodama za analizu i detektiranje krivotvorenja digitalne fotografije s obzirom na digitalni zapis i strukturu JPEG formata. S ciljem dokazivanja autentičnosti u radu će biti predstavljene i opisane metode temeljene na promatranju i usporedbi osnovnih karakteristika JPEG zapisa i poznatim karakteristikama kreiranja digitalnog JPEG zapisa. U teoretskom dijelu su rada analizirana postojeća saznanja uz poznate metode analize, tj. forenzike, digitalnog zapisa fotografije. U

eksperimentalnom dijelu za analizu i dokazivanje autentičnosti uz unaprijed definirani model koristiti će se manipulirane fotografije izrađene u laboratorijskim uvjetima s ciljano napravljenim promjenama te će se uz promatranje rezultata objasniti način na koji se ispravno interpretiraju dobivene informacije. Korištenjem različitih tehnika pri dokazivanju autentičnosti probati će se analizirati široki spektar trenutno poznatih metoda manipulacije, a jedna od najčešćih metoda je dodavanja ili brisanje elemenata digitalne fotografije.

2 TEORIJSKI DIO

2.1 Digitalna fotografija

Oko 1500. g. Leonardo da Vinci konstruirao je kutiju na čijoj je prednjoj strani mali otvor nasuprot kojeg je mutno staklo na kojem se ocrtava slika [1]. Ovakva se kutija naziva kamera opskura (L*at. camera obscura*).

Ranih 1800. godina Joseph Nicephore Niepce uz primjenu kamere opskure i sabirne leće uspijeva dobiti prvu uspješnu sliku preteču fotografiji (tzv. *heliografija*). Time je u biti izumljeni prvi fotografski aparat koji predstavlja temelj u razvoju fotografije.

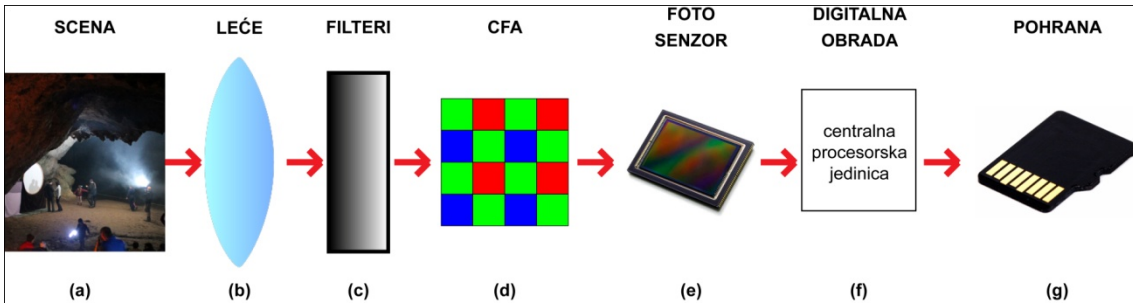
U 20. stoljeću kao najpoznatiji medij za snimanje fotografije se koristio fotografski film [1]. Fotografski film se sastoji od prozirne podloge na koju se nanosi fotoosjetljivi sloj koji je u osnovi srebreni halogenid (najčešće bromid). Osvjetljavanjem fotografskog filma pomoću fotografskog aparata dobiva se nevidljivi zapis objekta snimanja. Srebreni halogenid je kristalne strukture, a veličina svakog pojedinačnog kristala određuje koliko će se detalja zabilježiti u procesu nastajanja fotografije, tj. osvjetljavanja. U fotografskoj se praksi govori o veličini zrna srebrenog bromida, a što je zrno veće to će se manje detalja zabilježiti na fotografskom filmu. Osvjetljenji fotografski film naziva se negativ koji mora proći daljnju obradu da bi se dobila konačna slika tj. pozitiv. Kod negativ zapisa boje su komplementarne, a tonovi obrnuti što znači da su tamna područja prikazana svijetlo i svijeta područja tamno, crvena je prikazana kao cijan, zelena kao magenta te plava kao žuta.

Pronalaskom CCD čipa (Charged Coupled Device) senzora osjetljivog na svjetlo 1969. godine Willard Boyle i George Smith započinju razvoj digitalne fotografije. 1974. godine firma Kodak izrađuje prvi prototip fotografskog aparata

koji umjesto filma koristi CCD senzor kao foto osjetljivi medij. Uz pronalazak CCD senzora za digitalnu fotografiju je bitan bio i razvoj CPU (centralna procesorska jedinica) koja je služila prvotno za određivanje i podešavanje elemenata ekspozicije kao i za automatsko izoštravanje scene. Zadnjih godina, digitalni fotoaparati su napravili veliku razliku u načinu kako fotografi, bilo amateri ili profesionalci, rade fotografije. U prošlom stoljeću 35mm SLR fotoaparat je bio najvažniji izum za ozbiljnog fotografa [2]. Sada, u 21. stoljeću mnogi fotografi koriste digitalnu fotografiju umjesto klasične. Bez obzira na razliku u dobivanju fotografije, većina postavki fotoaparata je ostala ista. U stvarnosti, većina digitalnih fotoaparata je dizajnirana da izgledaju te da se njima koristi kao i na klasičnim SLR fotoaparatima. Napretkom tehnologije digitalni fotoaparati postaju učinkovitiji, jednostavniji za korištenje te jeftiniji, a time na tržištu skoro pa potpuno zamjenjuju klasične fotoaparate.

Krajem 20. stoljeća na tržište dolazi sve više digitalnih fotoaparata, a do 2003. godine je većina proizvođača fotoaparata objavila da je prodaja digitalnih fotoaparata prestigla prodaju klasičnih te time započinje era digitalne fotografije [3]. Digitalno snimanje je proces zapisivanja vidljivog spektra svjetlosti, njegove obrade (pretvaranje svijetla u digitalni zapis) te spremanje tog zapisa na digitalni medij.

Slika 1 prikazuje shematski prikaz digitalne fotografije [3]. Prvo, svjetlo je sa scene (a) fokusirano prema fotoosjetljivom mediju pomoću optičkih leća (b). Optičke leće (objektiv) kontroliraju veličinu scene te količinu svjetla koja se propušta do foto osjetljivog medija. Objektivi se mogu grubo svrstati u tri kategorije: širokokutni, normalni i teleobjektivi. Žarišna duljina objektiva je udaljenost od optičkog centra objektiva do točke u kojoj se skupljaju sve zrake svijetla koje dolaze od nekog beskonačno udaljenog predmeta i paralelno prolaze kroz objektiv. Žarišna duljina je podatak kojimse određuje vidni kut objektiva. Objektivi malih žarišnih duljina (uobičajeno 28 ili 35mm) nazivaju se širokokutni objektivi. Žarišna duljina normalnih objektiva približno odgovara čovjekovom aktivnom kutu gledanja (uobičajeno 50mm). Objektivi većih žarišnih duljina, od 75mm, nazivaju se teleobjektivi (podjela vrijedi za leica format) [1].



Slika 1: Shema procesa nastajanja fotografije

Prije nego dođe do zapisa fokusiranog svjetla, svjetlo prolazi preko niza filtera koji pomažu pri pretvaranju zapisa u digitalni. Prvi filter naziva se *antialiasing* koji malo zamagljuje sliku kako bi spriječio širenje prostorne frekvencije veće od rezolucije samog foto osjetljivog medija, tj. senzora [3]. Kao posljedica na digitalnoj fotografiji mogu nastati distorzije ili umjetne tvorevine koji nisu bile prisutni u orginalnoj sceni. Slijedi infracrveni filter zbog toga što je senzor vrlo osjetljiv na infracrveni spektar svjetlosti. Treći filter je tzv. CFA (*color filter array*) koji je izveden kao mozaik filtera boja. Postavlja se ispred foto osjetljivog medija, a služi za dobivanje informacija potrebnih za kreiranje kolor fotografije.

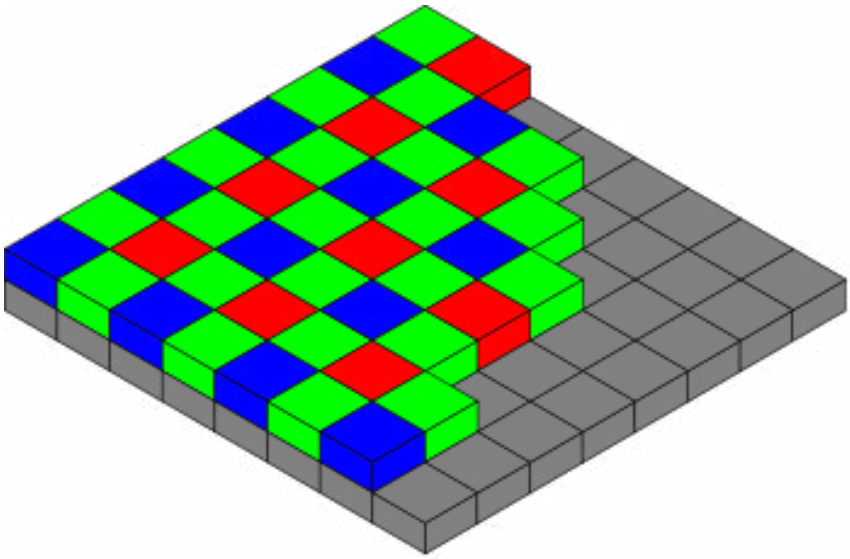
Senzor je najbitnija komponenta digitalnog fotoaparata. Dva najpoznatija tipa senzora su *Charged-Coupled-Device* (CCD) i *Complimentary Metal-Oxide-Semiconductor* (CMOS). CCD i CMOS senzori se bitno tehnološki razlikuju, ali im je primjena ista. Ovi senzori sadrže mnogo fotoosjetljivih ćelija koje se nazivaju *pikseli*, a pretvaraju intenzitet svjetla u električni napon. Svaka ćelija tj. *piksel* može zabilježiti samo intenzitet svjetla, a time se dobiva monokromatska komponenta. Radi toga se koriste CFA filtri koji razdvajaju različite valne duljine svjetla (d).

CFA je mozaik filtra boja koji razdvaja valne duljine svjetla i propušta samo određene valne duljine na svaki pojedinačni piksel. Postoje različite izvedbe CFA, a najkorišteniji je Bayer RGB uzorak *(slika 2)* po kojemu na dva *zelena piksela* dolaze po jedan *crveni* i *plavi*. Alternativno rješenje Bayerovom uzorku je Foveon X3 senzor koji koristi svojstvo silicija da u različitim dubinama sloja propušta različite valne duljine što omogućava RGB zapis fotografije

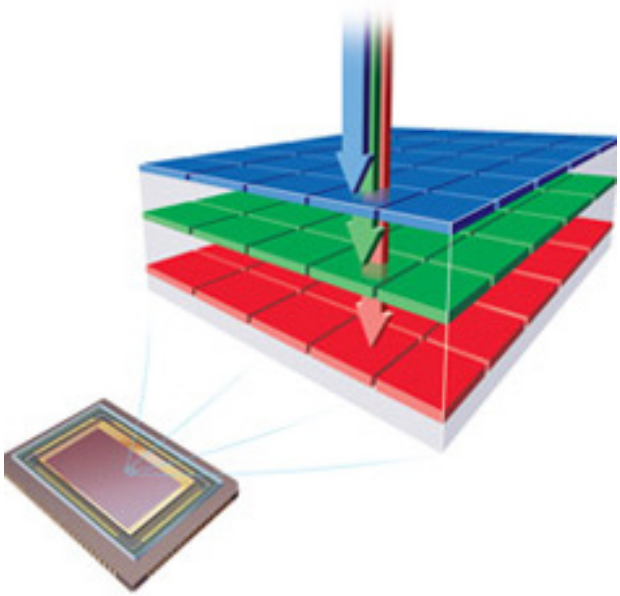
(slika 3). Nakon prolaska svjetla kroz CFA filter svjetlo dolazi na fotoosjetljivi senzor (e). Senzor se može zamisliti kao dvodimenzionalna matrica piksela. Ako se uzme da je jedna os X, a druga Y, rezolucija fotografije je broj piksela po osi X pomnožen s brojem piksela po osi Y. Stvaranje digitalne fotografije temelji se na binarnom sustavu što znači da postoji konačna vrijednost koja opisuje sadržaj scene. Konačna vrijednost je skup pozitivnih brojeva koji prikazuju vrijednost intenziteta svjetla ovisno o tome koliko bitova sadrži sustav. Npr. 8-bit sustav ima mogućnost prikazati intenzitet svjetla u 256 nivoa (od 0 do 255). Vrijednost 0 prikazuje potpuni nedostatak svjetla ili crnu, dok 255 prikazuje maksimalni iznos svjetla ili bijelu boju. Senzor ima zadaću prenijeti intenzitet svjetla u konačnu sliku, a taj se proces naziva kvantizacija. Kvantizacija je proces kojim se dobiveni intenzitet svjetla pretvara u najbliži cijeli broj, a time dolazi do malih gubitaka u slici.

Nakon što je intenzitet svjetla za svaku boju zabilježen uz pomoć senzora, potrebna je dodatna obrada dobivenih informacija kako bi se dobila vrijednost boja za svaku od primarni boja. Proces ima zadaću pretvoriti monokromatsku matricu u kolor fotografiju, a poznat je pod nazivom interpolacija (f). Nakon pretvorbe u RGB sustav boja, dobivaju se tri kolor sloja, crveni, zeleni i plavi. Interpolacija je proces koji je kod svakog proizvođača fotoaparata različiti i također je različiti od modela do modela fotoaparata.

Nakon toga slijedi daljnja obrada informacija koju radi interni procesor, a u toj obradi uključena je gama korekcija i bijeli balans (f). Pri završetku obrade svih informacija fotoaparat izrađuje fotografiju koju je moguće pohraniti u digitalnom obliku na nekom od medija za pohranu podataka (g). Format zapisa može sadržavati sirovi zapis (.raw, .cr2, .nef, itd.), fotografiju bez gubitka pri kompresiji (.tiff), bitmape (.bmp) ili fotografiju sa gubitkom kao JPEG format.



Slika 2: Bayer RGB uzorak (Izvor: http://en.wikipedia.org/wiki/Bayer_filter)



Slika 3: Foveon X3 RGB uzorak

(Izvor: http://www.foveon.com/files/X3_tech_hero.jpg)

Digitalna fotografija pohranjena na medij za pohranu može se dalje duplicirati i prenositi bez ikakvih gubitaka informacija ili kvalitete fotografije. Digitalne datoteke se mogu elektroničkim putem slati na velike udaljenosti u jako kratkom vremenskom intervalu. Fotografiju je zatim moguće dodatno obrađivati pomoću računalnih aplikacija te ih dodatno distribuirati. Dok postoji

mnogo prednosti digitalne fotografije u odnosu na klasičnu, zbog svoje praktičnosti i fleksibilnosti nastaju novi problemi kada se fotografija želi upotrijebiti kao dokaz. Digitalnom fotografijom moguće je vrlo lako i brzo manipulirati uz pomoć raznolikih računalnih aplikacija namijenjenih za obradu fotografije. Kvaliteta manipulacije najviše ovisi o vještini, stručnosti i znanju pojedinca, a kada dođe do potrebe za provjerom autentičnosti potrebno je primijeniti razna pravila, algoritme i modele za takvu analizu. Proces dokazivanja autentičnosti fotografije se uvelike razlikuje u digitalnoj i klasičnoj fotografiji, a s obzirom na problematiku ovaj rad se bavi proučavanjem postojećih algoritama za analizu digitalne fotografije te predlaže nove modele za uspješniju, bržu i efikasniju analizu.

2.2 Analize digitalne fotografije

Umjetnost krivotvorenja i manipulacije fotografijom postoji otkako je izumljeni fotoaparat. Prve manipulacije fotografijom su zapažene početkom 1840. godine kada je Hippolyte Bayard napravio prvu krivotvorinu promjenom naslova na fotografiji kako bi promijenio cijeli kontekst. Tehnike su brzo počele napredovati te su počele sadržavati dvostruke ekspozicije negativa, bojanje negativa te slaganje i spajanje više slika. Ubrzo su manipulaciju fotografija prepoznale vlade, koje su koristile manipulaciju za političku propagandu i širenje netočnih informacija. Vladini dužnosnici, posebice u totalitarnom režimu koristili su tehnike manipulacije fotografijom kako bi izmijenili povijesne činjenice te iskrivljenu sliku prikazali javnosti [3].

U današnje vrijeme, postoji veliki utjecaj krivotvorenja digitalne fotografije koji je javnosti predstavlja putem tiskanih i digitalnih medija (WWW, novine, časopisi) [4, 5]. U par slučajeva objave krivotvorene fotografije u medijima, radi održavanja dobre reputacije, izdavači su kažnjavali fotoreportere za koje se

dokazalo da su izradili krivotvorine. Iako su se mnogi ranije bavili manipulacijom klasične fotografije, zabrinutost oko integriteta i vjerodostojnosti digitalne fotografije raste već od 1988. godine kada su počele prve računalne manipulacije fotografijom [6].

To je bilo vrijeme kada je specijalizirana oprema, tj. digitalni fotoaparati i računala, bila dostupna samo maloj skupini ljudi koji su imali tehnička znanja i vještine za njihovo korištenje.

Napretkom tehnologije izrade te vrlo malom cijenom proizvodnje digitalni fotoaparati su svojom širokom ponudom i raznolikošću preplavili tržište. Digitalne kamere su osim kao zasebni uređaji integrirani u skoro svaki mobilni telefon, prijenosno računalo i tablet. Razni Internet servisi kao *Instagram,Facebook*, *Flickr,* te aplikacije za mobilne telefone koje na jednostavan način omogućuju dijeljenje fotografija putem Interneta postaju trend. Primjerice, na portal Facebook se mjesečno snimi preko tri miliona fotografija [7]. Takav trend potiče i razvoj brojnih računalnih aplikacija za digitalnu obradu fotografija od kojih su mnogi besplatni i dostupni široj javnosti. Korisnici su sada u mogućnosti napraviti velike promjene na fotografijama bez da se vizualno vidi promjena. Kako se sve više fotografija koristi kao dokaz na sudu, vrlo je bitno provjeriti integritet i autentičnost fotografija.

Organizacija SWGIT (*Scientific Working Group Imaging Technology*) je opisala analizu fotografije kao "tumačenje sadržaja slikovnog zapisa i / ili samog slikovnog zapisa primjenom znanosti o slikovnim prikazima i analizi, te stručnošću u dotičnom području" [8]. U SWGIT dokumentu su opisane tri osnove zadaće analize fotografije, a od toga su dvije relevantne za ovaj rad. Prva zadaća *interpretacija* je shvaćanje sadržaja fotografije primjenom znanstvene ekspertize. Uobičajeno se to dobiva kombinacijom statičke analize i kognitivne funkcije. Statička analiza je od velike koristi u provjeriti autentičnosti, ali nije ju moguće primijeniti na sva gledišta fotografije. Stoga, zaključci se donose uz pomoć kognitivne funkcije koja se sastoji od promatranja detalja i objašnjavanjem elemenata fotografije.

Druga zadaća analize fotografije koja je vrlo bitna naziva se *ispitivanje* kojom se dobivaju informacije o značajkama fotografije te njezina struktura. Uglavnom, kvaliteta fotografija koje dolaze na analizu nisu idealne zbog svjetlosnih uvjeta, udaljenost objekta od fotoaparata, rezolucije, fokusa, gubitka u stvaranju fotografije, itd. Radi tog razloga, većina obrade počinje ispitivanjem i traženjem informacija o detaljima i uvjetima nastanka digitalne fotografije. Ova vrsta obrade obično se naziva *pojašnjenje* radi toga što je cilj ovog postupka jasnije i lakše razumjeti sadržaj fotografije te uvjeti u kojima je nastala. Fotogrametrija je tehnika mjerenja kojom se iz jedne ili više uzastopnih fotografija određuje, veličina i oblik snimljenoga predmeta. Fotogrametrija se može koristi i za lociranje promjene na slici, analizom rasvjete, sjena i perspektive pojedinih elemenata [9–11]. Korištenje fotogrametrije za otkrivanje promjena temelji se na izračunima u području fizike, koja je izvan opsega ovoga rada te se o tome neće raspravljati.

Usporedba fotografija je ispitivanje dva ili više objekta na jednoj ili više fotografija, da bi se uočila razlika ili sličnost u svrhu daljnjeg istraživanja. Usporedna analiza, informacije razvrstava na tri klase: opća, ograničeno – opća i jedinstvena. Opća klasa je obilježje koje dijeli veliki broj objekata u skupini. Jedinstvena klasa je obilježje vezano za samo jedan objekt u klasi. Opća i jedinstvena klasa opisuju dva različita karaktera fotografije, ograničeno – opći karakterizira objekt koji nije dovoljno jedinstven da bi bio u toj klasi, a opet nema obilježja koja pripadaju općoj klasi [3].

Analizom sadržaja procjenjuje se način nastanka fotografije, uvjete u kojima je stvorena te s tehničkog aspekta je li fotoaparat uopće mogao stvoriti takvu fotografiju. Autentičnost fotografije osigurava integritet digitalnog zapisa, izvorni zapis koji nije promijenjeni i koji prenosi istinitu informaciju promatraču. U pravosudnom slučaju, autentična fotografija se može koristiti kao dokaz koji ispravno opisuje neko mjesto, situacije ili događaj.

Oprema kojom je stvorena digitalna fotografija u osnovi se sastoji od objektiva, fotoaparata i medija za zapis. Specifikacija fotoaparata razlikuje se između svakog proizvođača i svakog modela. Moguće je uočiti i razlike između

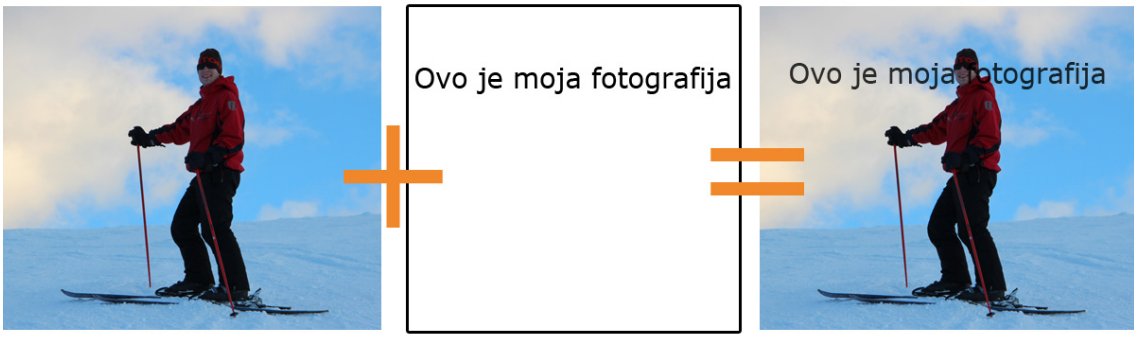
istih modela fotoaparata. Da bi se u takvim slučajevima potvrdila autentičnost fotografije, potrebno je obratiti pozornost na format i strukturu datoteke. Karakteristike na koje treba obratiti pozornost su: rezolucija, dubina boja, format zapisa, veličina datoteke, te informacije integrirane u strukturu zapisa fotografije. Kada su poznate karakteristike nastanka fotografije, fotografiju je moguće koristiti za usporedbu. Također, ako je poznat model fotoaparat, moguće je prema određenim parametrima provjerili mogućnost nastanka fotografije tim fotoaparatom.

Dok RGB sustav boja i konačni broj piksela predstavljaju digitalnu fotografiju, konačni digitalni zapis se određuje pomoću formata zapisa. Poznati formati zapisa su BMP, TIFF i JPEG. Svaki od njih ima prednosti i mane, a time su pogodniji za tisak, razmjenu, Internet ili neku drugu namjenu. Kod stvaranja, formati BMP i TIFF koriste kompresiju bez gubitka pa ne dolazi do gubitka informacija niti kvalitete pri zapisu fotografije. Format JPEG koristi kompresiju s gubitkom time žrtvujući kvalitetu slike u zamjenu za manju veličinu datoteke. Kompresija se računa tako da odbacuje piksele koji mogu biti zamijenjeni susjednim pikselom, a kvaliteta prikaza se određuje uz pomoć faktora kvalitete QF (*quality factor*). Karakteristike svake fotografije, dubina boja, rezolucija, format zapisa stvara osnovu za mogućnost krivotvorenja i manipulacije fotografijom.

2.3 Digitalni vodeni žigovi

Tehnike za analizu digitalnih fotografija nisu kompletne bez predstavljanja metode za zaštitu autorskih prava i vlasništva nad fotografijom. Za tu svrhu postoje digitalni vodeni žigovi. Kod korištenja digitalnih vodenih žigova, fotografija koju se želi zaštititi se spaja sa vodenim žigom u jedinstvenu fotografiju. Digitalni vodeni žigovi mogu i ne moraju biti vidljivi golim okom. Slika

4 prikazuje primjer vidljivog vodenog žiga. U tom slučaju je vodeni žig integriran u sliku te čine cjelinu tj. novu fotografiju. Praktično se primjenjuje kada se želi istaknuti vlasništvo nad fotografijom, a najčešće se može vidjeti na Internetu. Takve fotografije su uglavnom male rezolucije radi bržeg prijenosa.



Slika 4: Vidljivi vodeni žig

U drugoj vrsti vodenog žiga, vodeni žig je integriran u fotografiju ali nije vidljiv golim okom. Ova metoda je korisna kada autor fotografije želi zaštititi svoja autorska prava te onemogućiti krivotvorenje. Na slici 5 prikazan je primjer takve vrste zaštite. Digitalni vodeni žig nije vidljiv golim okom te je za njegovu detekciju potrebno koristiti algoritme koji mogu otkriti i prikazati skrivenu informaciju.

Slika 5: Nevidljivi vodeni žig integriran u fotografiju uz pomoćaplikacija za steganografiju

Svrha aplikacija za digitalne vodene žigove je zaštita autorskih prava, zaštita protiv krivotvorenja, zlouporabe i neovlaštenog kopiranja. Nevidljivi vodeni žigovi imaju još više prednosti jer su potrebni različiti programi za detekciju i prikaz te se radi toga osim u fotografiji koriste i u zaštiti tekstualnih dokumenata, audio i video zapisa.

2.4 Nepoznato porijeklo fotografije

Poznavajući tehnike zaštite može se spriječiti krivotvorenje originala i neovlašteno kopiranje. Obrnuti proces nastaje kada se mora otkriti izvor fotografije te dokazati njezina autentičnost. Potrebe za time ima sve više s obzirom da je upotreba digitalnih fotoaparata prisutna u svakodnevnom životu, a programi za digitalnu obradu fotografije postaju sve moćniji. Manipulacija digitalnom fotografijom postaje sve prisutnija te potreba za dokazivanjem autentičnosti postaje sve važniji faktor pri objavi fotografija.

2.5 Pregled metoda za analizu digitalne fotografije

U današnje vrijeme uz sve više digitalnih uređaja forenzička analiza ne bi bila moguća bez upotrebe računala. Forenzika digitalne fotografije može se podijeliti na dva ključna dijela, a to je identifikacija izvora fotografije i dokaz autentičnosti fotografije. Pronalazak izvora fotografije je bitna procedura jer određuje način nastanka fotografije tj. izvor fotografije (kamera, fotoaparat, mobilni telefon, tablet...). Dokazivanjem autentičnosti koriste se razne metode za provjeru integriteta i pokušaja krivotvorenja fotografije. Pronalaženje izvora

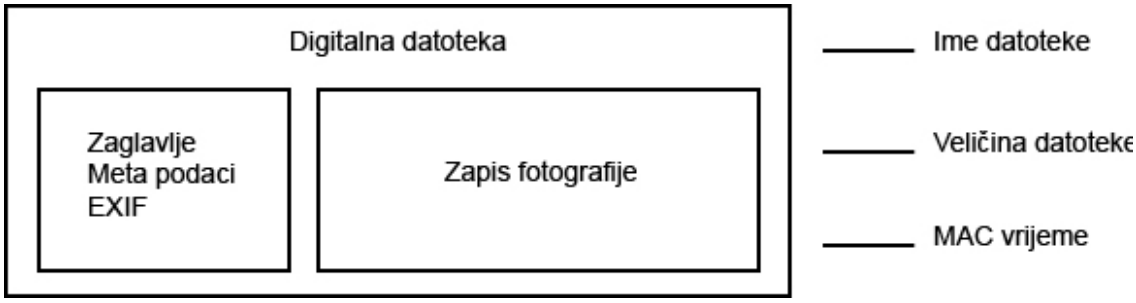
fotografija temelji se na metodama: distorzije optike objektiva, šuma u fotoosjetljivom senzoru, filteru boja (CFA), interpolacije i inherentnim svojstvima fotografije [12–19]. Ovaj rad se neće baviti ovim metodama, nego samo metodama analize digitalne fotografije. Krivotvorenje fotografija, u ovom smislu podrazumijeva svaku promjenu nastalu naknadnom računalnom obradom. Najčešći primjeru su rezanje i lijepljenje dodatnih elemenata, dupliciranje, premještanje, rotacija i mijenjanje osvjetljenja elemenata na fotografiji. Metode za detekciju krivotvorenja i manipulacije analiziraju fotografije, traže nedosljednosti u kromatskoj aberaciji, osvjetljenju, strukturi, JPEG kvantizacijskoj tablici i bikoherenciji [19–22].

2.6 Struktura digitalnog zapisa

Za zapis digitalne fotografije danas se koriste mnogi formati. Svaki od njih ima drugačiju strukturu, svoje prednosti i mane. Binarni zapis, kojim se služe računala svaku informaciju zapisuju uz pomoć brojeva 0 i 1. Konačni binarni zapis predstavlja kodiranu informaciju u kojoj su sadržane informacije o samoj slici, formatu zapisa, zapis o nastanku i modificiranju fotografije, način kodiranja i kompresije, vrijeme modificiranja, nastanka fotografije, itd..

U svrhu forenzičke analize, struktura digitalnog zapisa je vrlo bitna informacija s obzirom da uvidom u nju, dolazi se do informacija bitnih za daljnju analizu i proces dokazivanja autentičnosti. Heksadecimalni zapis, meta podaci, EXIF, struktura formata zapisa i MAC potpis su bitne informacije koje se mogu pročitati iz samog digitalnog zapisa, a nastaju istovremeno s nastankom fotografije.

Cijeli koncept temelji se na tome da digitalna fotografija sadrži puno više informacija nego što ih preglednici fotografija mogu prikazati (slika 6). Digitalni zapis je spremnik koji uz sadržaj koji prikazuje ima i informacije koji detaljno opisuju taj zapis, vrijeme nastajanja i okruženje nastanka zapisa. Zbog toga postoji bitna razlika između autentičnosti digitalne datoteke i autentičnosti digitalne fotografije.



Slika 6: Struktura digitalnog zapisa fotografije

Autentična digitalna datoteka je izvorna datoteka nastala u digitalnom fotoaparatu, dok je autentična fotografija izvorna scena bez ikakvih slučajnih ili namjernih promjena. Promjenom učinjenom na digitalnoj datoteci, sama fotografija može i dalje ostati autentična, ali npr. datum nastanka može biti promijenjen.

2.7 Format zapisa datoteke

Razvojem i napretkom tehnologije u razvoju digitalnih fotoaparata, računalnih aplikacija za obradu fotografija te sve većim trendom razmjene fotografija nastali su mnogi formati za digitalni zapis fotografija. Neki od njih su kroz brojne nadogradnje postali toliko prihvatljivi te tako primjerice na Internetu, odnosno *World Wide Webu* za razmjenu fotografija vladaju formati PNG i JPEG. Svi formati za zapis, imaju standarde i pravila u kojima su opisani načini

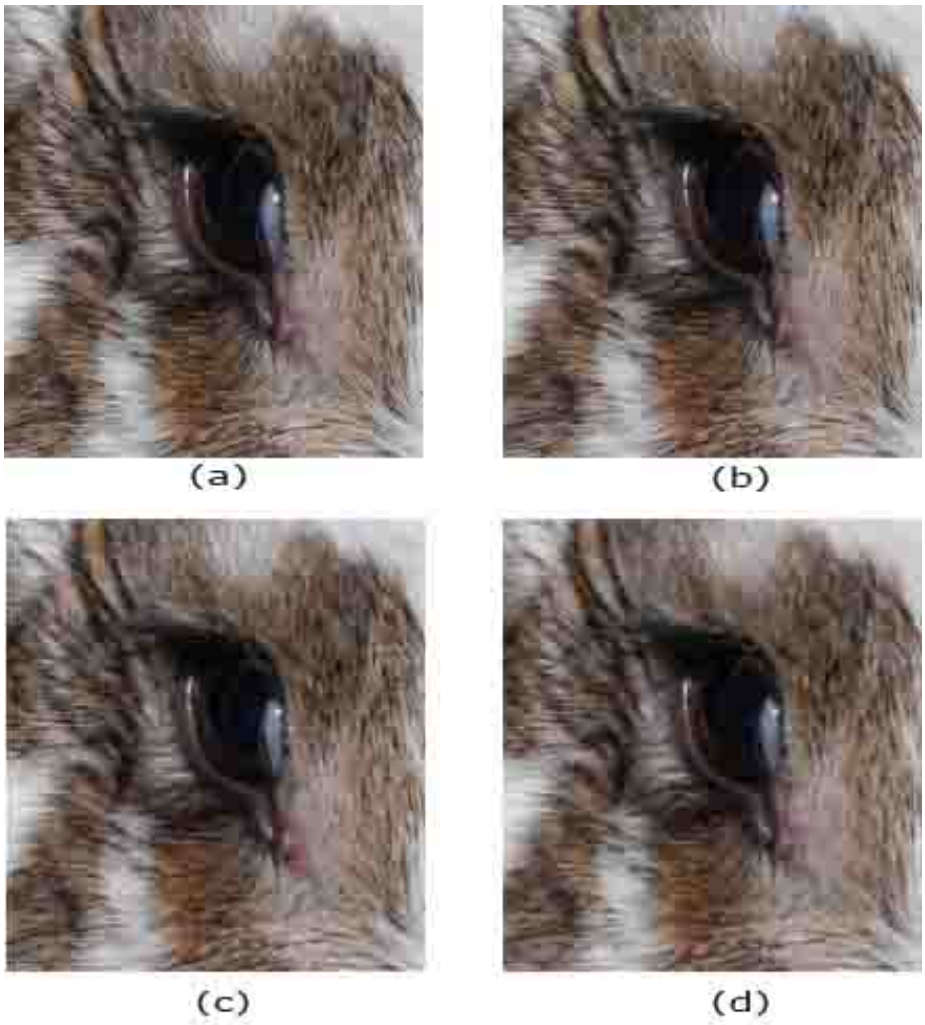
pohrane, pravila kompresije dubina boja, rezolucija, itd. Digitalni zapisi mogu se podijeliti po vrsti kompresije. U tom slučaju postoji kompresija sa gubitkom i kompresija bez gubitka informacija.

Kompresija bez gubitka informacija pri izradi datoteke koristi algoritme koji pri obradi originala i pretvorbi u novu datoteku ne gubi informacije o fotografiji. Takav način kompresije traži optimalni način da spremi sve informacije, a da pritom ne izgubi ni jedan detalj vidljiv na fotografiji. Nedostatak takvog zapisa je količina prostora koju datoteka zauzima te se koriste kada su kvaliteta i detalji važniji od zauzeća prostora. Poznati formati koji se koriste su .BMP i .TIF.

Podskup zapisa bez kompresije su danas aktualni *sirovi zapisi*. To su vlasnički formati koji su stvorile korporacije koje se bave razvojem digitalnih fotoaparata i računalnih aplikacija za obradu fotografija. Takvi formati zapisa se smatraju kao negativom u klasičnoj fotografiji. Jedna od karakteristika im je potreba za posebnim računalnim aplikacijama za njihov pregled i obradu. Najzastupljeniji vlasnički formati su .DNG (Adobe), .CR2 i .CRW (Canon), .NEF (Nikon) i .SRF (Sony).

Formati zapisa koji koriste kompresiju s gubitkom izrađuju datoteke koje zauzimaju manje prostora, ali s gubitkom kvalitete. Faktor kvalitete fotografije ovisi o vrsti zapisa i količini kompresije (slika 7). Algoritmi za kompresiju, analiziraju fotografiju te izračunavaju koji dio informacija se može obrisati, a da fotografija ne gubi detalje. Prevelika kompresija trajno uništava fotografiju te je gubitak kvalitete lako uočljiv. Slika 7 prikazuje vidljive efekte pri različitim nivoima kompresije. GIMPomogućuje spremanje fotografije u JPEG format sa nivoima kvalitete od 0-100, gdje broj 100 označava najmanju kompresiju tj. najveću kvalitetu fotografije. Kvaliteta i način kompresije ovise o algoritmu kompresije stoga, odabirom krivog ili prevelikoga nivoa kompresije fotografija može izgubiti poruku koju želi prenijeti. JPEG standard je trenutno najkorišteniji način kompresije digitalnih fotografija. Kod provjere autentičnosti fotografije, korisno je obratiti pozornost na format zapisa fotografije te mogućnost formata zapisa digitalnog fotoaparata. Neki fotoaparati imaju mogućnost spremanja fotografije u nekompresiranom formatu .TIFF ili nekom sirovom formatu dok

neki imaju mogućnost zapisa samo u JPEG formatu. Također, veličina datoteke sumnjive fotografije može se usporediti sa fotografijama nastalim na istom fotoaparatu pri sličnim osvjetljenju.



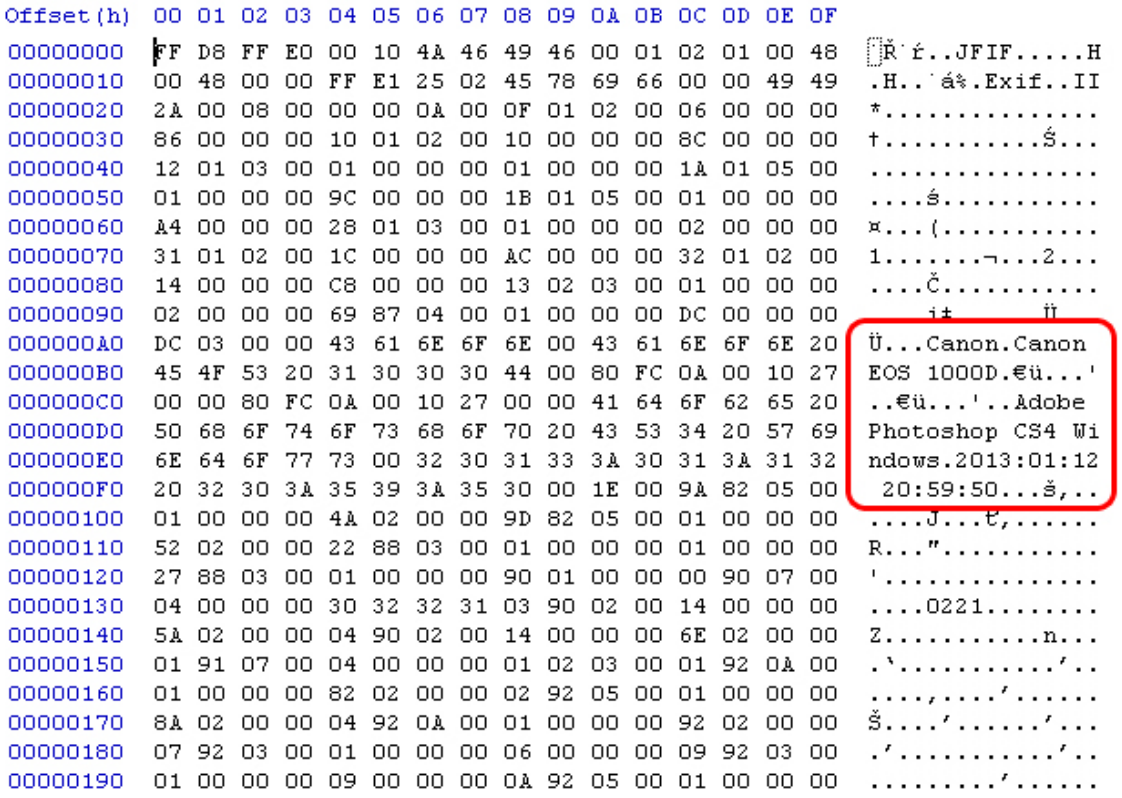
Slika 7: JPEG zapis s gubitkom kvalitete. Na fotografijama su vidljivi gubitci ovisno o kompresiji: nekopresirana fotografija (a), JPEG kvaliteta 70 (b), JPEG kvaliteta 40 (c), JPEG kvaliteta 0 (d)

2.8 Heksadecimalni brojevi

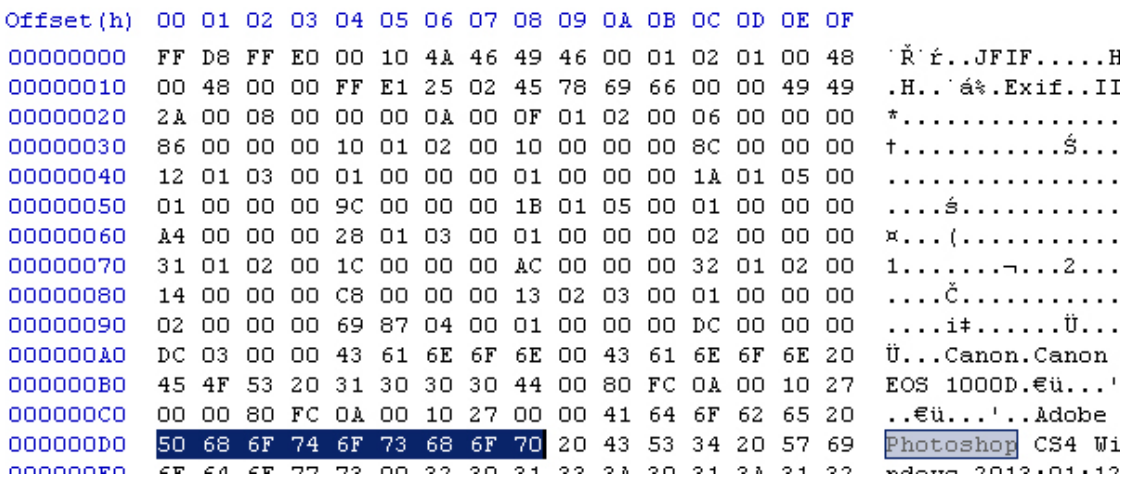
Računala sve informacije obrađuju i zapisuju u binarnom brojevnom sustavu. Bit je naziv binarne znamenke, a vrijednosti mogu biti 0 ili 1. Digitalni podatak je niz bitova koji tvoje cjelinu, a njegova veličina je skoro pa neograničena. Da bi se binarni podatak mogao obraditi, potrebno ih je pravilo interpretirati uz pomoć računalnih programa koji imaju tu zadaću. Binarni brojevni sustav je teško razumljiv čovjeku te se te informacije pretvaraju u heksadecimalni brojevni sustav. Heksadecimalni brojevni sustav se sastoji od 16 znamenki: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E i F. Heksadecimalna znamenka sastoji se od 4 bita, a dvije heksadecimalne znamenke predstavljaju jedan bajt koji ima jednu od 256 vrijednost u rasponu 00 do FF. Svaki heksadecimalni broj tj. bajt predstavlja decimalnu vrijednost, programsku naredbu, matematičku operaciju, slovo ili datoteku u računalnom sustavu. Heksadecimalne vrijednosti datoteke moguće je vidjeti uz pomoć heksadecimalnog preglednika koji dolazi kao računalni program te u tekstualnom obliku prikazuje te informacije. ASCII (American Standard Code for Information Interchange) [23] je jedan od standarda za kodiranje i prikaz svakog pojedinačnog znaka uključujući slova, brojeve te posebne znakove. Kada računalne aplikacije imaju interakciju sa datotekama ostavljaju svoj trag na način da ugrade svoj "potpis" kao heksadecimalnu vrijednost ili kao EXIF zapis. Za primjer, Photoshop ostavlja detaljan zapis o operacijama izvedenim na fotografijama, a ta informacija je integrirana u heksadecimalni zapis datoteke (slika 8). Zbog toga je pri istraživanju fotografije potrebno obratiti pozornost na heksadecimalni zapis te pokušati naći tragove krivotvorenja jer računalni programi za obradu fotografije ostavljaju tragove.

Prednost korištenja ove tehnike je brzina pretrage traženih kriterija. Svaka fotografija sadrži previše informacija da bi čovjek obratio pozornost na sve detalje u heksadecimalnom zapisu, stoga čovjek zadaje kriterij pretrage, a heksadecimalni preglednici pretražuju sadržaj datoteke. Računala naspram čovjeka mogu u vrlo malom vremenskom intervalu pretražiti veliku količinu

podataka. Ako ima rezultata, heksadecimalni preglednik će ih naći i prikazati (slika 9), a čovjek ce onda provesti daljnje istraživanje i analizu za dokazivanje autentičnosti. Manipulacija heksadecimalnim zapisom je relativno lagana uz poznavanje strukture zapisa. Svaka greška, brisanje bajta, mijenjanje vrijednosti može rezultirati oštećenom datotekom ili nečitljivim zapisom.



Slika 8: Heksadecimalni zapis fotografije kojom se manipuliralo



Slika 9: Pretraga heksadecimalnog zapisa u potrazi za znakovima manipuliranja

2.9 EXIF podaci

U digitalnoj fotografiji *Exchangeable Image File Format* (EXIF) je standard za pohranu informacija o parametrima nastajanja fotografije. Koriste ga svi moderni digitalni fotoaparati od amaterskih do profesionalnih, a informacija je integrirana u sami digitalni zapis fotografije. U EXIF su pohranjeni podaci o modelu fotoaparata, vremenu i datumu nastanka fotografije, otvoru objektiva, ISO osjetljivosti, vremenu eksponiranja, rezoluciji, načinu mjerenja svjetla, fokusu, žarišnoj duljini objektiva, GPS koordinatama te niza ostalih informacija vezanih za fotografiju. EXIF se osim u digitalnim fotoaparatima koristi i u mobilnim telefonima, skenerima i programima za obradu fotografija. U forenzici EXIF je jedan od najbitnijih elemenata istraživanja zbog niza informacija relevantnih za daljnju istragu[24]. EXIF je prvobitno napravljen za .TIFF format zapisa, točnije EXIF meta podaci se počinju koristiti s TIFF revizijom 6.0.

1996. godine JEIDA (*Japan Electronic Industry Development Association*) objavila je "*Digital Still Camera Image File Format Standard*" koji se povezuje na *EXIF Format ISO 12234-1* [25, 26]. 2002. godine JEITA (*Japan Electronics and Information Technology Industries Association* (bivša "JEIDA") objavljuje specifikaciju koja kasnije postaje standard "*Exchangeable image file format for digital still camera: EXIF verzija 2.2*". Uz EXIF postoji i mnogo drugih standarda kao što su *JPEG2000*, *JPEG-LS, SPIFF* o kojima se neće govoriti pošto je EXIF danas rasprostranjeniji i ima najširu primjenu. EXIF uključuje najbolje dijelove JPEG, JFIF, TIFF i DCF formata, uz kompatibilnost s *FlashPix, CIFF* i ostalim vlasničkim formatima. Informacije pohranjene u EXIF uključuje puno standardnih polja kao što su *FileName, FileModDate, Model, DateTime* i ostalo (slika 10).

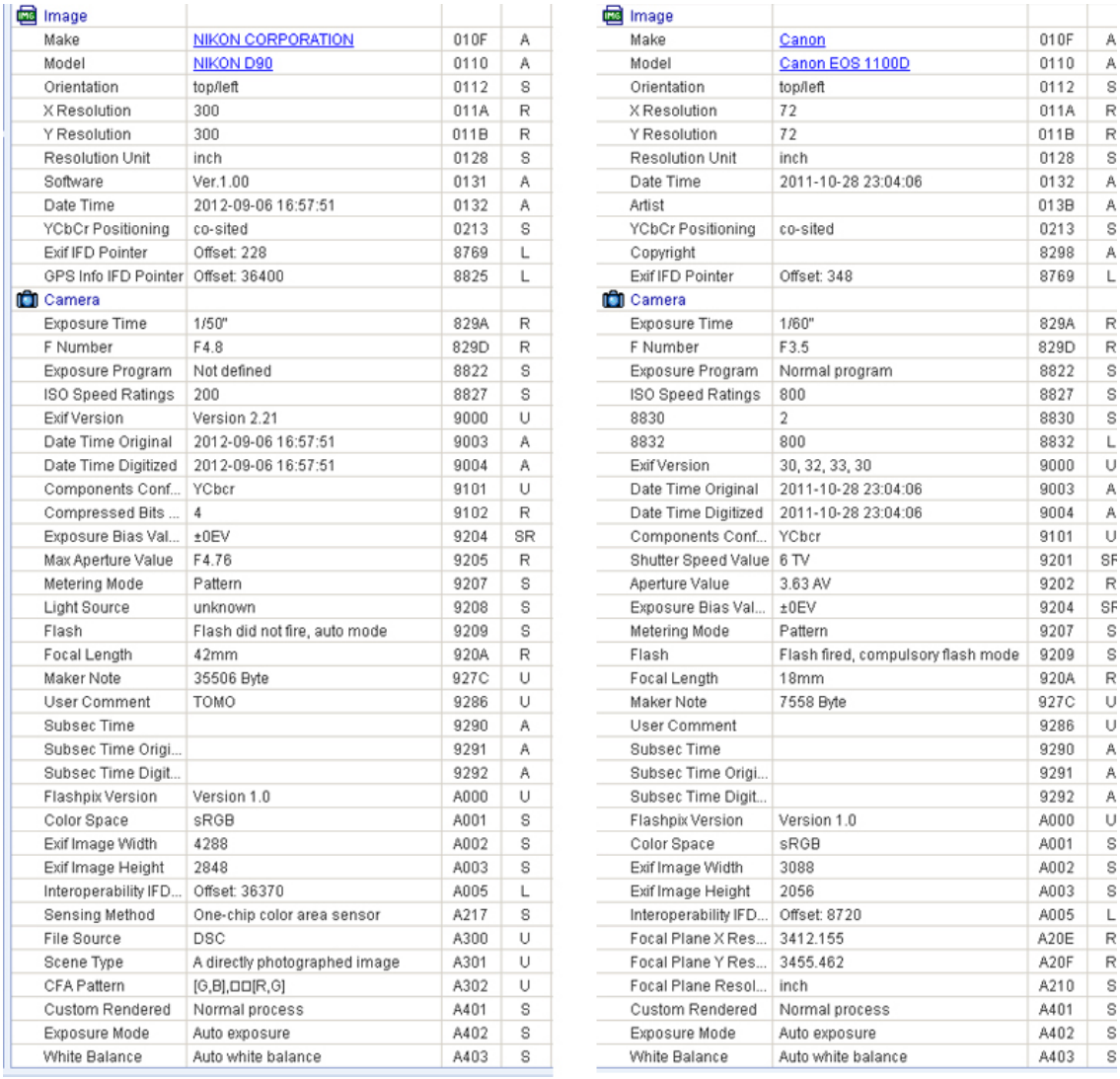


Image			
Make	NIKON CORPORATION	010F	A
Model	NIKON D90	0110	A
Orientation	top/left	0112	S
X Resolution	300	011A	R
Y Resolution	300	011B	R
Resolution Unit	inch	0128	S
Software	Ver.1.00	0131	A
Date Time	2012-09-06 16:57:51	0132	A
YCbCr Positioning	co-sited	0213	S
Exif IFD Pointer	Offset: 228	8769	L
GPS Info IFD Pointer	Offset: 36400	8825	L
Camera			
Exposure Time	1/50"	829A	R
F Number	F4.8	829D	R
Exposure Program	Not defined	8822	S
ISO Speed Ratings	200	8827	S
Exif Version	Version 2.21	9000	U
Date Time Original	2012-09-06 16:57:51	9003	A
Date Time Digitized	2012-09-06 16:57:51	9004	A
Components Conf...	YCbcr	9101	U
Compressed Bits ...	4	9102	R
Exposure Bias Val...	±0EV	9204	SR
Max Aperture Value	F4.76	9205	R
Metering Mode	Pattern	9207	S
Light Source	unknown	9208	S
Flash	Flash did not fire, auto mode	9209	S
Focal Length	42mm	920A	R
Maker Note	35506 Byte	927C	U
User Comment	TOMO	9286	U
Subsec Time		9290	A
Subsec Time Origi...		9291	A
Subsec Time Digit...		9292	A
Flashpix Version	Version 1.0	A000	U
Color Space	sRGB	A001	S
Exif Image Width	4288	A002	S
Exif Image Height	2848	A003	S
Interoperability IFD...	Offset: 36370	A005	L
Sensing Method	One-chip color area sensor	A217	S
File Source	DSC	A300	U
Scene Type	A directly photographed image	A301	U
CFA Pattern	[G,B],□□[R,G]	A302	U
Custom Rendered	Normal process	A401	S
Exposure Mode	Auto exposure	A402	S
White Balance	Auto white balance	A403	S

Image			
Make	Canon	010F	A
Model	Canon EOS 1100D	0110	A
Orientation	top/left	0112	S
X Resolution	72	011A	R
Y Resolution	72	011B	R
Resolution Unit	inch	0128	S
Date Time	2011-10-28 23:04:06	0132	A
Artist		013B	A
YCbCr Positioning	co-sited	0213	S
Copyright		8298	A
Exif IFD Pointer	Offset: 348	8769	L
Camera			
Exposure Time	1/60"	829A	R
F Number	F3.5	829D	R
Exposure Program	Normal program	8822	S
ISO Speed Ratings	800	8827	S
8830	2	8830	S
8832	800	8832	L
Exif Version	30, 32, 33, 30	9000	U
Date Time Original	2011-10-28 23:04:06	9003	A
Date Time Digitized	2011-10-28 23:04:06	9004	A
Components Conf...	YCbcr	9101	U
Shutter Speed Value	6 TV	9201	SF
Aperture Value	3.63 AV	9202	R
Exposure Bias Val...	±0EV	9204	SF
Metering Mode	Pattern	9207	S
Flash	Flash fired, compulsory flash mode	9209	S
Focal Length	18mm	920A	R
Maker Note	7558 Byte	927C	U
User Comment		9286	U
Subsec Time		9290	A
Subsec Time Origi...		9291	A
Subsec Time Digit...		9292	A
Flashpix Version	Version 1.0	A000	U
Color Space	sRGB	A001	S
Exif Image Width	3088	A002	S
Exif Image Height	2056	A003	S
Interoperability IFD...	Offset: 8720	A005	L
Focal Plane X Res...	3412.155	A20E	R
Focal Plane Y Res...	3455.462	A20F	R
Focal Plane Resol...	inch	A210	S
Custom Rendered	Normal process	A401	S
Exposure Mode	Auto exposure	A402	S
White Balance	Auto white balance	A403	S

Slika 10: Primjer EXIF zapisa fotografije nastale u fotoaparatu

Uz sve prednosti EXIF zapisa postoje i neke mane. Velika mana je što se proizvođači nisu mogli dogovoriti oko standardnih polja koje će sadržavati EXIF zapis. Tako primjerice na primjerima iz slike 10, fotoaparati Canon i Nikon nemaju ista polja i ne sadrže iste podatke. Zbog toga, ovisno od proizvođača do proizvođača, EXIF zapis i polja u njemu mogu biti različita. Svaki proizvođač sam određuje koje informacije želi prikazati te prema tome prilagođuje EXIF zapis. Zbog načina kodiranja, a ponekad i kriptiranja podataka, ispravne informacije kao serijski broj, proces obrade i kreiranja JPEG fotografije moguće je vidjeti samo sa proizvođačevim EXIF preglednikom.

Podaci koje sadrži EXIF su jako osjetljivi na promjenu, tako da datoteka može lako postati oštećena i nečitljiva ako se koriste nekompatibilni programi za dodatnu obradu i mijenjanje podataka [26]. Adresa sadržaja EXIF podataka u strukturi datoteke određena je pokazivačima. Podatci mogu biti bilo gdje adresirani u datoteci te pokazivači služe za prikazivanje lokacije računalnim programima. Svako zaglavlje EXIF zapisa po standardu sadrži SOI (*start of image*) *FF D8* zatim slijedi *APP1 FF E1 xx xx 45 78 69 66 00*, a završava sa *FF D9*. *APP1* se pojavljuje na samom početku zapisa, a sadrži *thumbnail* fotografije i ima ograničenje maksimalne veličine koja iznosi 64Kb.

Zbog toga što EXIF zapis može biti zapisani na bilo kojem mjestu u datoteci, neispravno dekodiranje i promjena podataka može dovesti do neispravne datoteke. Slika 11 prikazuje EXIF zapis koji je promijenjen uz pomoć računalnih programa. Kada se uspoređuje sa standardnim EXIF zapisom iz slike 10, primjećuje se nestanak devet polja. Jedan od načina traženja manipulacije nad fotografijom je uspoređivanje načina kreiranja i promjene EXIF zapisa. Analiziranje EXIF zapisa najbolje je napraviti sa sumnjivom fotografijom i novonastalom fotografijom ako je poznata marka proizvođača i model fotoaparata. EXIF zapis u tom slučaju sadrži sva polja s vrijednostima karakterističnim za tu fotografiju (vrijeme, datum, otvor objektiva, vrijeme eksponiranja, ISO osjetljivost).

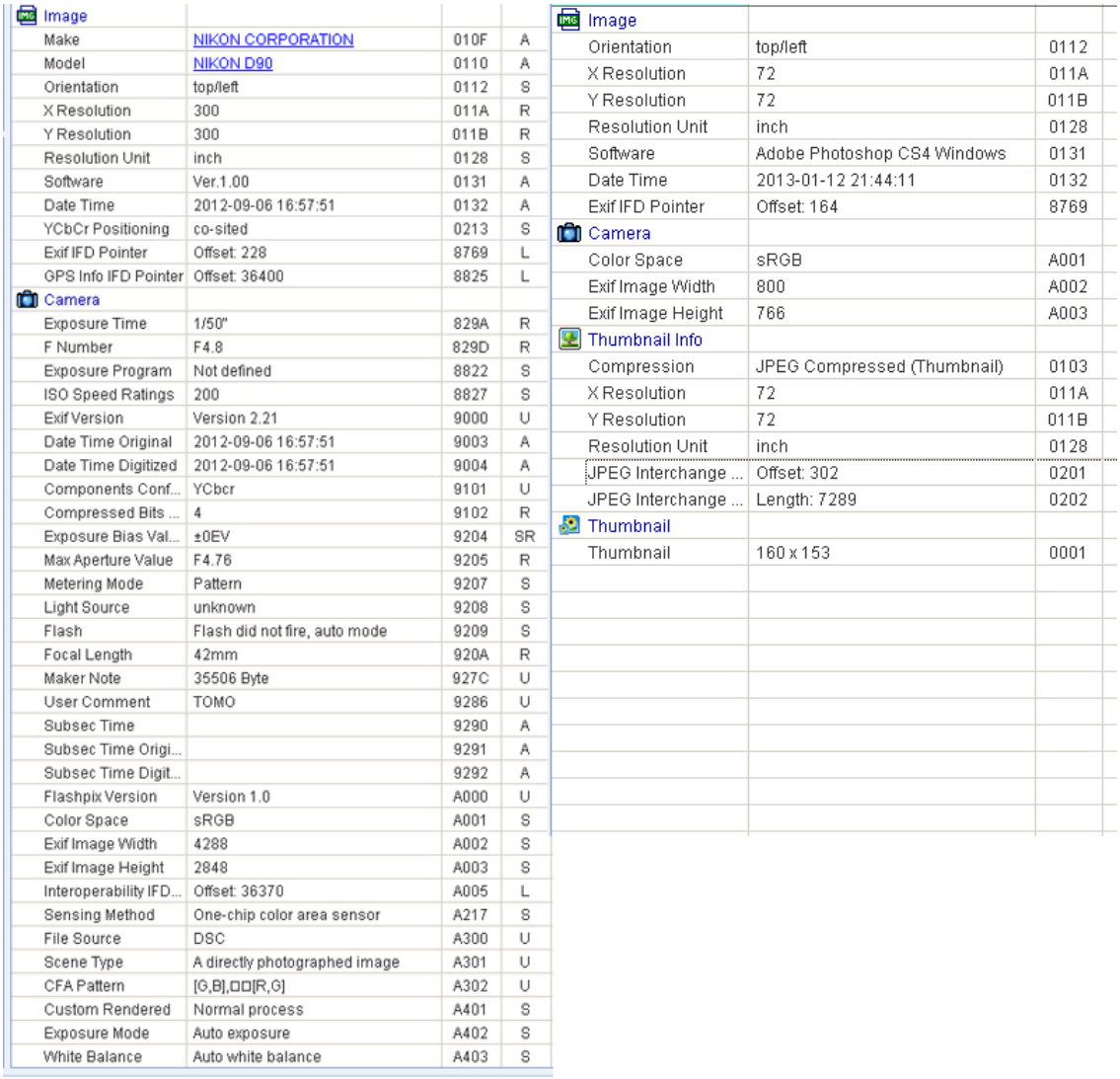


Image			
Make	NIKON CORPORATION	010F	A
Model	NIKON D90	0110	A
Orientation	top/left	0112	S
X Resolution	300	011A	R
Y Resolution	300	011B	R
Resolution Unit	inch	0128	S
Software	Ver.1.00	0131	A
Date Time	2012-09-06 16:57:51	0132	A
YCbCr Positioning	co-sited	0213	S
Exif IFD Pointer	Offset: 228	8769	L
GPS Info IFD Pointer	Offset: 36400	8825	L
Camera			
Exposure Time	1/50"	829A	R
F Number	F4.8	829D	R
Exposure Program	Not defined	8822	S
ISO Speed Ratings	200	8827	S
Exif Version	Version 2.21	9000	U
Date Time Original	2012-09-06 16:57:51	9003	A
Date Time Digitized	2012-09-06 16:57:51	9004	A
Components Conf...	YCbcr	9101	U
Compressed Bits ...	4	9102	R
Exposure Bias Val...	±0EV	9204	SR
Max Aperture Value	F4.76	9205	R
Metering Mode	Pattern	9207	S
Light Source	unknown	9208	S
Flash	Flash did not fire, auto mode	9209	S
Focal Length	42mm	920A	R
Maker Note	35506 Byte	927C	U
User Comment	TOMO	9286	U
Subsec Time		9290	A
Subsec Time Origi...		9291	A
Subsec Time Digit...		9292	A
Flashpix Version	Version 1.0	A000	U
Color Space	sRGB	A001	S
Exif Image Width	4288	A002	S
Exif Image Height	2848	A003	S
Interoperability IFD...	Offset: 36370	A005	L
Sensing Method	One-chip color area sensor	A217	S
File Source	DSC	A300	U
Scene Type	A directly photographed image	A301	U
CFA Pattern	[G,B],□□[R,G]	A302	U
Custom Rendered	Normal process	A401	S
Exposure Mode	Auto exposure	A402	S
White Balance	Auto white balance	A403	S

Image		
Orientation	top/left	0112
X Resolution	72	011A
Y Resolution	72	011B
Resolution Unit	inch	0128
Software	Adobe Photoshop CS4 Windows	0131
Date Time	2013-01-12 21:44:11	0132
Exif IFD Pointer	Offset: 164	8769
Camera		
Color Space	sRGB	A001
Exif Image Width	800	A002
Exif Image Height	766	A003
Thumbnail Info		
Compression	JPEG Compressed (Thumbnail)	0103
X Resolution	72	011A
Y Resolution	72	011B
Resolution Unit	inch	0128
JPEG Interchange ...	Offset: 302	0201
JPEG Interchange ...	Length: 7289	0202
Thumbnail		
Thumbnail	160 x 153	0001

Slika 11: Primjer ispravnog i manipuliranog EXIF zapisa

S obzirom na ograničenja ovakve analize, prije donošenja zaključka o integritetu fotografije potrebno je voditi brigu o drugim činjenicama. EXIF je integriran u sami digitalni zapis fotografije, odnosno datoteku te ga je moguće mijenjati uz pomoć heksadecimalnih ili EXIF tekstualnih uređivača. Drugi je problem što su neki parametri EXIF podataka određeni od strane korisnika fotoaparata, npr. vrijeme i datum. Pri donošenju zaključka uz EXIF analizu potrebna je daljnja obrada i analiza kako bi se sa sigurnošću mogao potvrditi integritet i autentičnost fotografije.

2.10 MAC vremena

MAC vremena su dijelovi meta podataka datotečnog sustava koji bilježe sve promjene nad digitalnim datotekama. MAC je skraćenica za *Modified, Access i Create* (izmjena, pristup i nastanak), a odatle dolaze i akronimi *mtime, atime* i *ctime*. Zbog tih podataka, MAC vrijeme je često korišten alat u računalnoj forenzici.

2.10.1 Vrijeme izmjene (mtime)

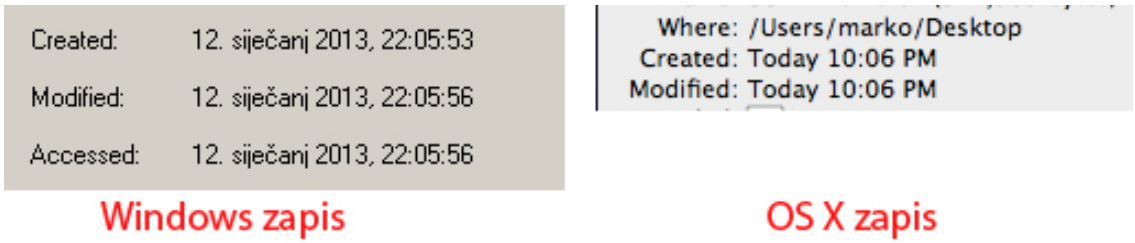
Vrijeme izmjene opisuje zadnje vrijeme promjene sadržaja datoteke. Većina datotečnih sustava nema mogućnost usporedbe novog i postojećeg sadržaja datoteke pa u slučaju izmjene podataka istim podacima, vrijeme izmjene će se promijeniti.

2.10.2 Vrijeme pristupa (atime)

Vrijeme pristupa prikazuje zadnje vrijeme pristupa datoteci. Kada neki program pristupa datoteci, samo pri otvaranju se mijenja vrijeme pristupa. Zbog toga program još uvijek može imati otvorenu datoteku, ali vrijeme pristupa se ne mijenja.

2.10.3 Vrijeme nastanka (ctime)

Ovisno o operativnom sustavu i datotečnom sustavu vrijeme nastanka se drugačije interpretira.Unix, Linux, OS X operativni sustavi zapisuju ovaj podatak kada dolazi do promjene meta podataka datoteke, a ne njezinog sadržaja. Primjer toga je promjena ovlasti pristupa datoteci.Windows operativni sustav koristi vrijeme nastanka za zapis vremena nastanka digitalne datoteke. Zbog tih je razlika mogući nesporazumi nejasnoća dobivenih informacija (kada datoteku nastalu u Windows okruženju otvaramo u Unix okruženju i obrnuto) (slika 12).



Slika 12: Primjer MAC zapisa na drugačijim operativnom sustavima

2.11 Analiza globalne strukture digitalnog zapisa

Zapis digitalne fotografije se može promatrati kao spremnik koji sadrži različite informacije. Dok se u prijašnjim poglavljima pričalo o analizi tih informacija, u ovom poglavlju će se opisati koje sve informacije sadrži fotografija. Da bi se manipuliralo nekom fotografijom, potrebno ju je otvoriti, obraditi i ponovo spremiti. Taj proces stvara malu promjenu u odnosu na original. *Primarna fotografija* je termin koji se koristi za opis fotografije koja nastaje u fotoaparatu [16]. Drugim riječima, fotografija nastaje kako fotoaparat pretvara svjetlost u digitalni zapis uz pomoć CFA, bijelog balansa, gama korekcije, JPEG kompresije sve do zapisa na medij za pohranjivanje. Kod

provjere autentičnosti, prvo je potrebno uvjeriti se da je sumnjivi fotoaparat u mogućnosti napraviti fotografiju provjerom formata datoteke i rezolucije. Ako se sumnja u mogućnost nastanka fotografije, potrebno je napraviti par primjeraka fotografije sa sumnjivim fotoaparatom. Nove primjere fotografije potrebno je usporediti sa primjerom kojemu se dokazuje integritet i autentičnost.

2.11.1 JPEG kompresija

Format zapisa sa ekstenzijom .jpg je danas najkorišteniji format zapisa digitalne fotografije, a označava JPEG zapis – metodu zapisa sa gubitkom u kompresiji koji iskorištava mane ljudskog oka. 1983. godine ISO (*International Organization for Standardization*) počinje tražiti metode kako zapisati digitalne fotografije s velikom rezolucijom. Tri godine kasnije, osnovana je grupa JPEG *(Joint Photographic Experts Group*) od strane CCITT (*International Telegraph and Telephone Consultative Committee*) i ISO sa svrhom definiranja standarda za kodiranje crno – bijelih i kolor fotografija. JPEG objavljuje "*Information Technology – Digital Compression and Coding of Continuoustone Still Images – Requirements and guidelines*" poznat još pod nazivom JPEG specifikacije za kodiranje i dekodiranje komprimirane fotografije (ISO 10918-1).

Eric Hamilton 1992. godine objavljuje format JFIF (JPEG File Interchange Format) koji omogućuje zapis meta podataka izvan samih informacija o slici. To je omogućilo JPEG zapisu da bude prepoznat među svim računalnim preglednicima fotografija.

Algoritmi za kompresiju JPEG zapisa nude povoljan omjer kvalitete i veličine fotografije. Zbog upotrebe JPEG zapisa i mogućnosti najučinkovitije kompresije sa gubitkom danas svaki digitalni fotoaparat ima mogućnost JPEG zapisa.

Standard JPEG podržava 8 ili 12 bitnu dubinu boja po RGB kanalu. Osam bitna dubina boje je postala prihvaćenija u praksi te se primjenjuje u digitalnom fotoaparatu iu računalnim programima za obradu fotografija. Za svaki kanal boje (R,G,B) u 8 bitnom sustavu, intenzitet svjetla se može izraziti sa 256 konačnih vrijednosti (0-255) za svaki piksel. Efikasnost kompresije JPEG zapisa temelji se na DCT (*Discrete Cosine Transform*) [27]. DCT algoritam ne stvara gubitak u kvaliteti fotografije, jer umjesto prostorne kompresije pretvara prostornu domenu u frekvencijsku domenu, a tek onda započinje proces kodiranja.

Koraci za kodiranje trokanalne kolor fotografije koristeći JPEG standard kompresijesu [28]:

1. Fotografija se pretvara iz RGB sustava boja u Luminance / Chrominance (YCbCr) sustav boja.
2. Fotografija je podijeljena u zasebna polja piksela dimenzije 8x8.
3. Vrijednost polja pretvaraju se iz cijelih brojeva (0 – 255) u cijele brojeve (-128 – 127).
4. Svako polje pretvara se iz prostorne domene u frekvencijsku domenu pomoću DCT algoritma.
5. Dobivene vrijednosti se kvantiziraju.
6. DCT koeficijent se tada kodira bez gubitaka.
7. Dodaje se zaglavlje u rezultat dobiven kodiranjem.

Pretvaranje RGB u YCbCr sustav boja je prvi korak u procesu stvaranja JPEG zapisa[29]. U ovom procesu se fotografija razdvaja u jednu luminacijsku komponentu i dvije kromatske. Ovaj proces se radi jer je ljudsko oko osjetljivije na svjetlije tonove, a manje osjetljivo na promjenu boju [30]. Zbog tromosti i

osjetljivosti ljudskog oka, informacije koje se nalaze u kromatskoj komponenti mogu se mnogo smanjiti bez vidljivih gubitaka u kvaliteti fotografije.

U drugom koraku fotografija se dijeli u zasebna polja 8x8 piksela (slika 13a). Treći korak pretvara vrijednosti cijelih brojeva u brojeve s predznakom. U četvrtkom koraku svaki blok se pojedinačno obrađuje DCT algoritmom i pretvara iz prostorne u frekvencijsku domenu. Područja koja imaju blagu izmjenu tonova, pripadaju u niži spektar frekvencija. Područja intenzivnih kontrasta i izmjena boja pripadaju u visoki spektar frekvencija. Rezultat dobiven DCT algoritmom je skup od 64 amplitude signala tzv. *DCT koeficijentom*. U kolor fotografiji, svaki kolor sloj se obrađuje zasebno kao neovisna slika.

139	144	149	153	155	155	155	155
144	151	153	156	159	156	156	156
150	155	160	163	158	156	156	156
159	161	162	160	160	159	159	159
159	160	161	162	162	155	155	155
161	161	161	161	160	157	157	157
162	162	161	163	162	157	157	157
162	162	161	161	163	158	158	158

(a) Uzorak izvorne fotografije

236	-1	-12	-5.2	2.1	-1.7	-2.7	1.3
-23	-18	-6.2	-3.2	-2.9	-0.1	0.4	-1.2
-11	-9.3	-1.6	1.5	0.2	-0.9	-0.6	-0.1
-7.1	-1.9	0.2	1.5	0.9	-0.1	0	0.3
-0.6	-0.8	1.5	1.6	-0.1	-0.7	0.6	1.3
1.8	-0.2	1.6	-0.3	-0.8	1.5	1	-1
-1.3	-0.4	-0.3	-1.5	-0.5	1,7	1.1	-0.8
-2.6	1.6	-3.8	-1.8	1.9	1.2	-0.6	-0.4

(b) DCT koeficijetni

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

(c) Kvantizacijska tablica

15	0	-1	0	0	0	0	0
-2	-1	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(d) Kvantizacijski koeficijenti

240	0	-10	0	0	0	0	0
-24	-12	0	0	0	0	0	0
-14	-13	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

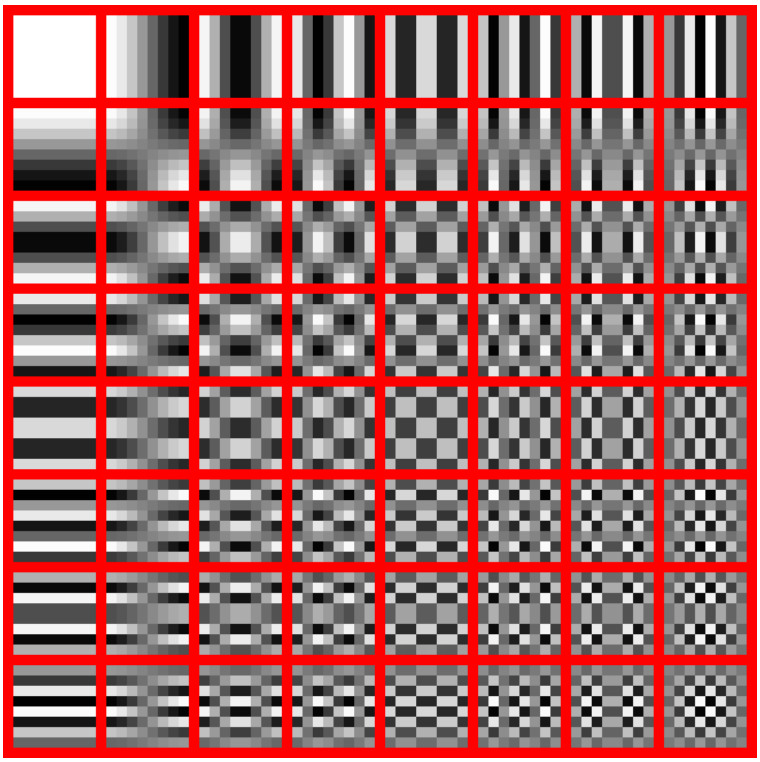
(e) Inverzni kvantizacijski koeficijenti

144	146	149	152	154	156	156	156
148	150	152	154	156	156	156	156
155	156	157	158	158	157	156	155
160	161	161	162	161	159	157	155
163	163	164	163	162	160	158	156
163	164	164	164	162	160	158	157
160	161	162	162	162	161	159	158
158	159	161	161	162	161	159	158

(f) Rekonstuirana fotografija

Slika 13: Primjeri DCT koeficijenata i kvantizacijskih tablica

DCT koeficijent dijeli se u dvije komponente, AC i DC. DC komponenta odnosi se na valnu dužinu svjetla i predstavlja prosjek ulaznih uzoraka. Komponenta DC predstavlja jedan od 64 uzorka, a to znači da broj AC komponenti iznosi 63 (slika 14).



Slika 14: AC i DC komponente DCT koeficijenta
(Izvor:https://www.projectrhea.org/rhea/images/9/98/Dct.png)

U petom koraku, rezultat DCT algoritma, tj. svaki koeficijent se dijeli sa 64 elementa kvantizacijske tablice koje su drugačije za kromatski kanal i za luminacijski kanal. Dodatno, svaki piksel u svakom kanalu se obrađuje istom kvantizacijskom tablicom (slika 13c). Niže vrijednosti u tablici prikazuju veću kvalitetu fotografije dok visoke vrijednosti označavaju manju kvalitetu fotografije. Iznos svakog element nakon procesa kvantizacije se zaokružuje na najbliži cijeli broj (slika 13d). Zaokruživanje je glavni uzrok gubitaka informacija u DCT kodiranju, a naziva se *kvantizacijska greška* koja je odgovorna za male promjene vrijednosti piksela između originala i komprimirane fotografije.

U šestom koraku, nakon kvantizacije, nastavlja se kodiranje slike algoritmima baziranim na statističkim karakteristikama. Kako se može vidjeti na slici 13d u procesu kvantizacije dobiva se puno znamenki 0. U zadnjem koraku, JPEG zaglavlje se spaja sa kodiranim nizom podataka koji čine cjelinu, tj. JPEG zapis fotografije.

Proces dekodiranja fotografije koristi iste korake kao i kodiranje, samo u suprotnom smjeru. Podaci se dohvaćaju iz kodiranog JPEG zapisa, nakon toga se uz pomoć kvantizacijskih tablica množe kako bi se dobili ispravni nekvantizirani DCT koeficijenti. U tom se procesu javljaju greške zbog zaokruživanja brojeva. Nekvantizirani koeficijenti pretvaraju se iz frekvencijskog područja u prostorno područje koristeći inverzni DCT algoritam. Konačno, tako dobivena fotografija se pretvara iz YCbCr prostora boja u RGB prostor boja.

Koristeći se JPEG kompresijom, u prosjeku, efikasno se može smanjiti veličina zapisa na 10% veličine originalne datoteke sa jako malim i skoro nevidljivim gubicima u kvaliteti. Uz veću je kompresiju moguće postići još manju veličinu ali sa većim i oku vidljivim gubicima. Uz te gubitke treba voditi računa o tome da kompresija JPEG zapisa stvara trajni i nepovratni gubitak kvalitete fotografije.

2.12 Analiza interpolacije

Interpolacija je proces približavanja vrijednosti ili funkcija između dvije definirane točke. Kada se mijenja veličina digitalne fotografije, u tom procesu se dodaju novi ili oduzimaju postojeći pikseli. Zbog toga se koriste mnogi algoritmi u obradi fotografija, a u ovom radu bit će predstavljena bilinearna interpolacija. Bilinearna interpolacija izvršava se dvosmjerno kako bi postigla najbolju aproksimaciju za nepoznate vrijednosti piksela, baziranih na vrijednostima susjednih piksela.

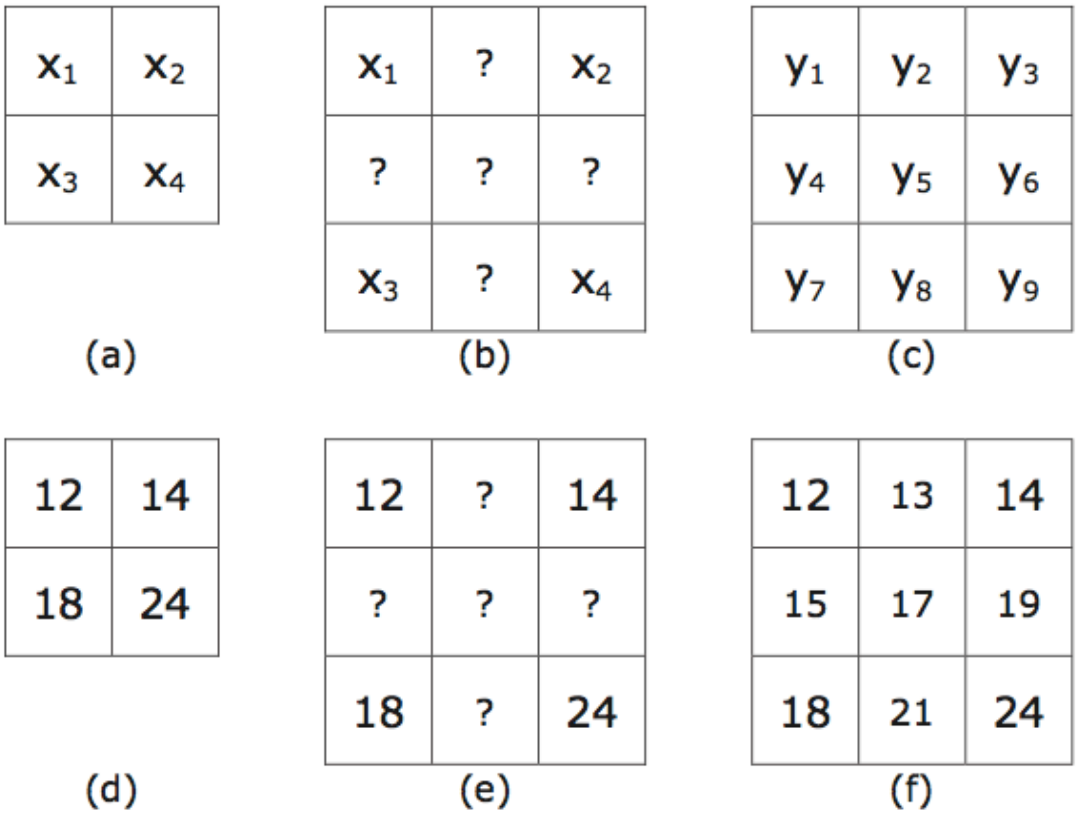
Na slici 15 je prikazana jednostavna 2D rešetka kojoj su dodani novi pikseli. Novi pikseli su razmjestili stare piksele slika 15b, e. Nepoznate vrijednosti novih piksela aproksimiraju se usporedbom sa vrijednostima poznatih piksela. Na slici 15c, foriginalne vrijednosti nalaze se na rubovima fotografija, a vrijednosti su im: y1 = x1, y3 = x2, y7=x3, y9=x4. Koristeći se bilinearnom interpolacijom, vrijednosti koje nedostaju na rubovima mogu se aproksimirati iz ostalih poznatih vrijednosti:

$$\begin{aligned} y_2 &= 0.5y_1 + 0.5y_3 \\ y_4 &= 0.5y_1 + 0.5y_7 \\ y_6 &= 0.5y_3 + 0.5y_9 \\ y_8 &= 0.5y_7 + 0.5y_9 \end{aligned} \tag{1}$$

Dok je centralna vrijednost aproksimizirana iz sve četiri poznate vrijednosti:

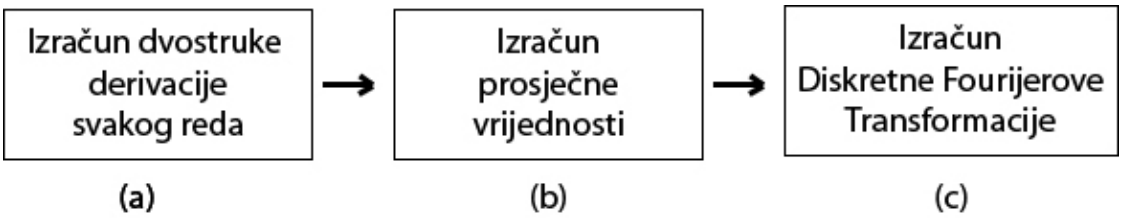
$$y_5 = 0.25y_1 + 0.5y_3 + 0.25y_7 + 0.5y_9 \tag{2}$$

Andrew C. Gallagher u svom radu opisuje korištenje metode dvostrukog deriviranja kako bi pronašao periodičnost u fotografiji [31]. Ova metoda može se primijeniti u JPEG kompresiji za analizu i identifikaciju koliko je puta fotografija bila komprimirana. Tragovi periodičnosti, tražeći uzorke u dvostrukoj derivaciji mogu identificirati je li fotografija originalna ili je više puta komprimirana te da li je došlo do promjene veličine.



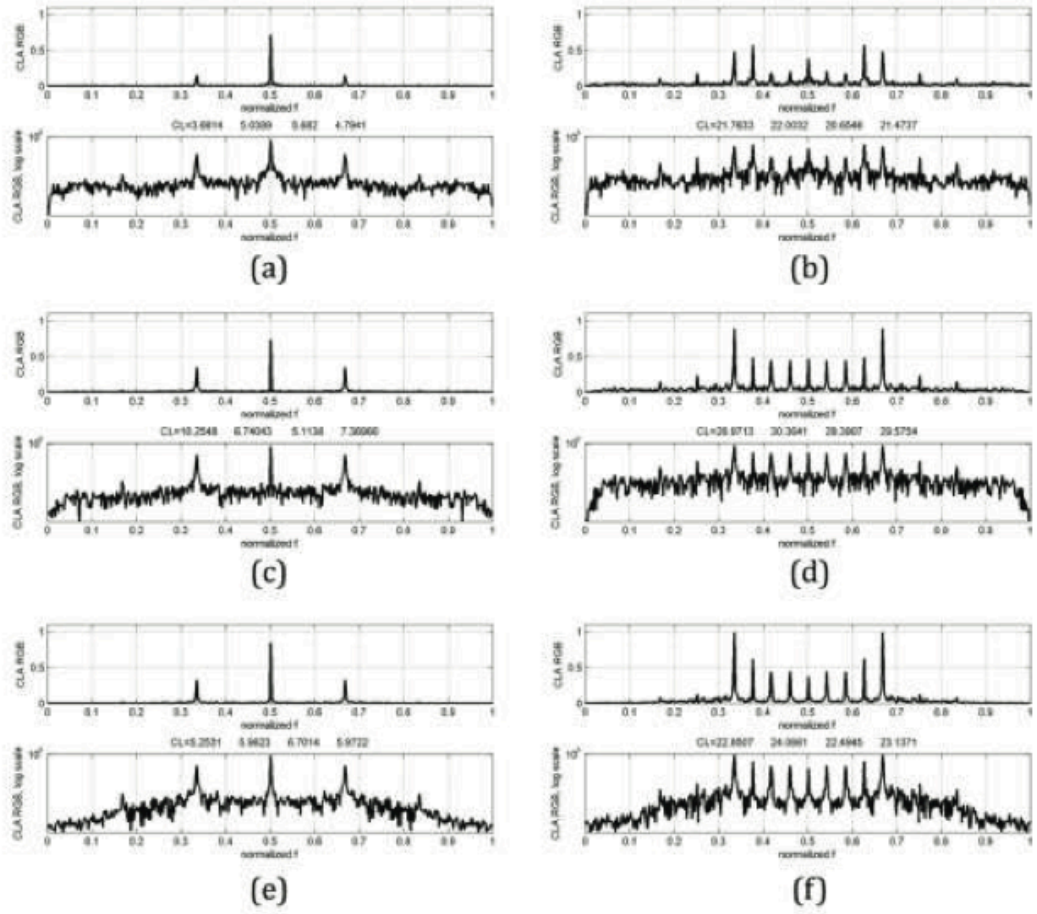
Slika 15: Primjer bilinearne interpolacije

Analizom i izračunom dvostruke derivacije je moguće detektirati tragove interpolacije na fotografiji. Algoritam za detekciju interpolacije prvo radi izračun dvostruke derivacije svakog reda matrice fotografije. Prosječna vrijednost je prosjek svih okolnih vrijednosti, na koju se primjenjuje *Diskretna Fourijerova Transformacija* (DFT) u potrazi za vršnim vrijednostima deriviranog signala (slika 16).



Slika 16: Blok dijagram algoritma za detekciju interpolacije

Rezultati ovog algoritma su vidljivi na slici 17 gdje su vidljive vršne vrijednost dvostruko deriviranog signala na istoj točci grafa (slika 17 a, b, c). Signal je relativno gladak u logaritamskoj skali. U slučaju kada je fotografije više puta komprimirana, pojavljuje se više vršnih vrijednosti, a centralni se smanjuje (slika 17 b, d, f).



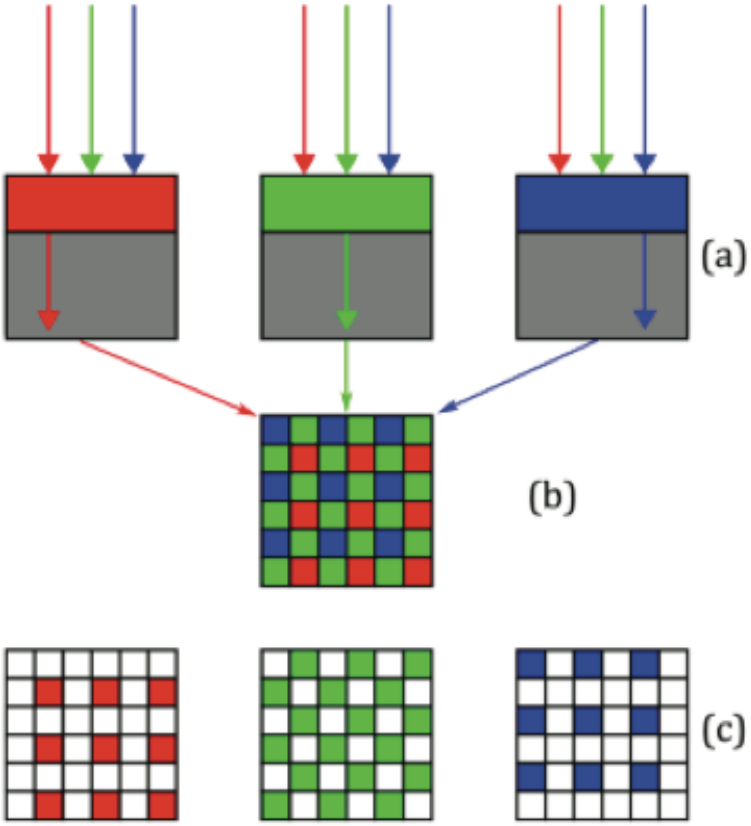
Slika 17: Analiza interpolacije primarne fotografije [3]

Interpolacija piksela se također može dijagnosticirati ako je fotografija komprimirana više puta, skalirana ili rotirana. Alin Popescu i Hany Farid su objavili tehniku za identifikaciju interpolacije koristeći algoritam *očekivanje / maksimalnost* [32]. U biti, algoritam koristi učestale procese da bi otkrio nepoznate parametre. Algoritam se koristi za provjeru sličnosti susjednih piksela uz periodičke uzorke. Kod primjene algoritma na ne komprimiranim fotografijama, lažna detekcija manja je od 1% za rotacije veće od 1 stupanj.

Osim velike pouzdanosti rezultata, ova tehnika se koristi i za otkrivanje skaliranja ili rotacije pojedinih elemenata fotografije.

2.13 Polje kolor filtera (CFA)

Pikseli fotoosjetljivih senzora (CMOS, CCD) osjetljivi su samo na intenzitet svjetla te ne razlikuju spektar valnih duljina svjetla. Jedina iznimka među senzorima je Foveon X3, koji ima mogućnost snimanja informacija o boji svjetla na svakom pojedinom pikselu [33]. Da bi se zaobišle ove mane CMOS i CCD senzora, ispred samog foto osjetljivog senzora stavlja se CFA (*Color Filter Array)* filter. Tada, svaki piksel snima intenzitet svjetla samo odredene valne duljine. Postoji puno izvedbi polja kolor filtra, a najkorišteniji je *Bayer uzorak* (slika 2). Budući da je ljudsko oko osjetljivije na zelenu boju nego na crvenu i plavu, *Bayer CFA* filter sadrži duplo više zelenih filtra od crvenih i plavih. Fotoosjetljivi senzor skuplja intenzitet zelenog, crvenog i plavog svjetla, ovisno o rasporedu filtera (slika 18b). Fotografija se sastoji od tri nivoa boja: crvena, zelena i plava. Sirovi zapis dobiven uz pomoć fotoosjetljivog senzora razdvaja se u zasebni nivo za svaki boju. Kako je vidljivo na (slici 18c) 50% informacija u zelenom spektru nedostaje, dok u crvenom i plavom području nedostaje 75% informacija. Za izradu fotografije iz mozaika filtera boja se koriste različiti algoritmi. Algoritmi se mogu podijeliti u dvije skupine. Prva skupina svaki nivo boja smatra zasebnom slikom. Ti algoritmi uključuju bilinearne, susjedne piksele i bi-kubične interpolacije. Uglavnom, takvi algoritmi rade dobro na glatkim prijelazima fotografije ali mogu prouzročiti oštećenja na rubovima i u zonama visokih detalja. Druga je klasa algoritama bazirana na činjenicama da su sva tri kanala boja ovisne jedne o drugima. Matematički izračun takvih fotografija je kompleksniji, ali kao rezultat daju bolju kvalitetu fotografije u rubnim dijelovima i zonama visokih detalja.



Slika 18: Primjena CFA filtera za stvaranje tri novoa boja

Primjenom bilo kojeg algoritma, cilj ostaje isti [34]. Stvaranje fotografije iz informacija o intenzitetu svjetla u RGB zapis. Interpolacijski algoritmi variraju od proizvođača do proizvođača, čak i od modela do modela istog proizvođača. Zbog različitosti algoritma za demozaik to se može iskoristiti za dokazivanje porijekla fotografije, tj. pronalaženje izvora fotografije [29].

2.14 Kvantizacijske tablice

Svrha kvantizacijskih tablica je kontrola količine kompresije primijenjene na fotografiju pri nastanku JPEG formata. Nakon što je blok od 8 x 8 piksela pretvoren u frekvencijsku domenu DCT metodom, kvantizacijska tablica ima rezultat od 64 DCT koeficijenta. Ovaj se proces naziva *kvantizacija* te se ovdje vizualno može primijetiti smanjenje informacija potrebnih za prikaz fotografije. U ovom dijelu se gubi najviše informacija pri stvaranju JPEG zapisa. Količina informacija koja se briše određena je psihovizualnim karakteristikama ljudskog oka, koje vrlo dobro uočava razlike svjetlosti, ali lošije prepoznaje zasićenje boja. Informacije koje se brišu nalaze se u visokofrekventnom području, tj. u području visokih detalja.

Svaka vrijednost DCT koeficijenta može imati vrijednost između 1 i 255, a na njih se primjenjuju određeni faktori skaliranja (slika 19). Vrijednost 1 označava vrlo malu kompresiju, što znači da dolazi do jako malog gubitka kvalitete. Vrijednost 100 označava vrlo visoki stupanj kompresije, a samim time i veliki gubitak kvalitete fotografije.

1	1	1	1	2	3	4	5
1	1	1	2	2	5	5	4
1	1	1	2	3	5	6	4
1	1	2	2	4	7	6	5
1	2	3	4	5	9	8	6
2	3	4	5	6	8	9	7
4	5	6	7	8	10	10	8
6	7	8	8	9	8	8	8

(a)

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

(b)

Slika 19: Primjer kvantizacijskih tablica

JPEG kompresiju je moguće postići u fotoaparatu radi prisutnosti mikroprocesorske jedinice zadužene za računanje. Neki fotoaparati imaju kvantizacijske tablice objavljene na Internacionalnoj Jpeg Grupi standarda (slika 20**).**

Ovakva kvantizacijska tablica može imati mogućnost skaliranja ovisna o faktoru *Q* koristeći sljedeću formulu:

$$S = \begin{cases} za(Q \le 50)\text{K} \ \dfrac{5000}{Q} \\ za(Q > 50)\text{K} \ 200 - 2Q \end{cases} \tag{3}$$

$$T_s[i] = \left\lfloor \frac{S * T_b[i] + 50}{100} \right\rfloor \tag{4}$$

gdje je:

Q – faktor kvalitete

S – faktor skaliranja

Tb – temeljna tablica

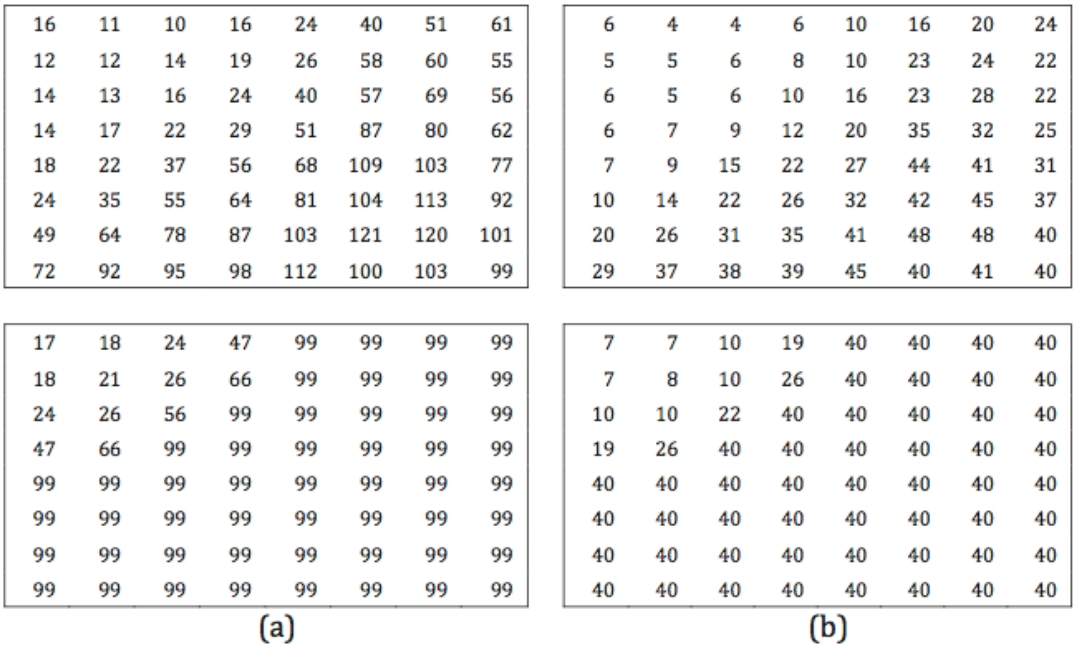
Ts – skalirana tablica.

Faktor kvalitete *Q*, može imati vrijednost 0 – 100, a koristi se kako bi se dobio faktor skaliranja *S*. Svaki element *i* u skaliranoj tablici nastao je računanjem varijable *i* s temeljne tablice. Što je veća vrijednost *Q* faktora, kompresija je manja, a samim time i kvaliteta fotografije veća.

Korisnik uvijek ima izbor između kvalitete ili kompresije, dok proizvođači fotoaparata u svoje uređaje ugrađuju preddefinirane kvantizacijske tablice. U stvarnosti, kvantizacijske tablice mogu biti različite među modelima istog proizvođača. Hany Farid objavio je kvantizacijske tablice od 204 digitalna fotaparata [35]. U tom radu, u prosjeku, kvantizacijske tablice jednog digitalnog fotoaparata imaju sličnosti sa 1.43 drugih fotoaparata.

Kvantizacijske tablice se dijele u četiri kategorije [36]. *Standardne tablice* su definirane skalarnim vrijednostima kvantizacijskih tablica objavljenje od Internacionalne JPEG grupe [36]. Fotografije sa standardnim tablicama imaju dva seta podataka, jedan set za luminaciju i jedan za kromatski kanal. Standardne kvantizacijske tablice imaju vrijednost faktora kvalitete *Q* između 1

– 99 (slika 20). Produžene *standardne tablice* su vrlo slične standardnim, ali s dodatnom, trećom kvantizacijskom tablicom.



16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

(a)

7	7	10	19	40	40	40	40
7	8	10	26	40	40	40	40
10	10	22	40	40	40	40	40
19	26	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40

(b)

Slika 20: Standardne kvantizacijske tablice

Preddefinirane tablice za faktor kvalitete Q = 80, gornje tablice koriste se za luminacijski, a doljne za kromatski kanal.

Definirane fiksne tablice su preddefinirane tablice od strane proizvođača, a namijenjene su upotrebi samo u njihovim proizvodima. Ovakve tablice imaju ograničenu mogućnost odabira postavki kompresije. Kao primjer se može navesti aplikacija za manipulaciju fotografija *Adobe Photoshop* koji ima mogućnost odabira nivoa kompresije između 0 – 12, a za svaku vrijednost kompresije primjenjuje se jedinstvena kvantizacijska tablica. *Adobe Photoshop* od verzije 3 do sada aktualne verzije *CS 6* ima iste preddefinirane kvantizacijske tablice [35].

Definirane prilagodljive tablice nisu u skladu sa JPEG standardom jer su različite za svaku fotografiju nasalu istim digitalnim fotoaparatom. Ove tablice se koriste u fotoaparatima novije generacije, u kojima se kvantizacijske tablice prilagođavaju sceni i rezoluciji digitalne fotografije. Analizom ovih tablica nije moguće otkriti izvor, model fotoaparata ili aplikacije za obradu, ali je moguće

suziti izbor. Zato analizi ovih vrsta kvantizacijskih tablica treba pristupiti s oprezom jer je ovo dugotrajan i mukotrpan proces.

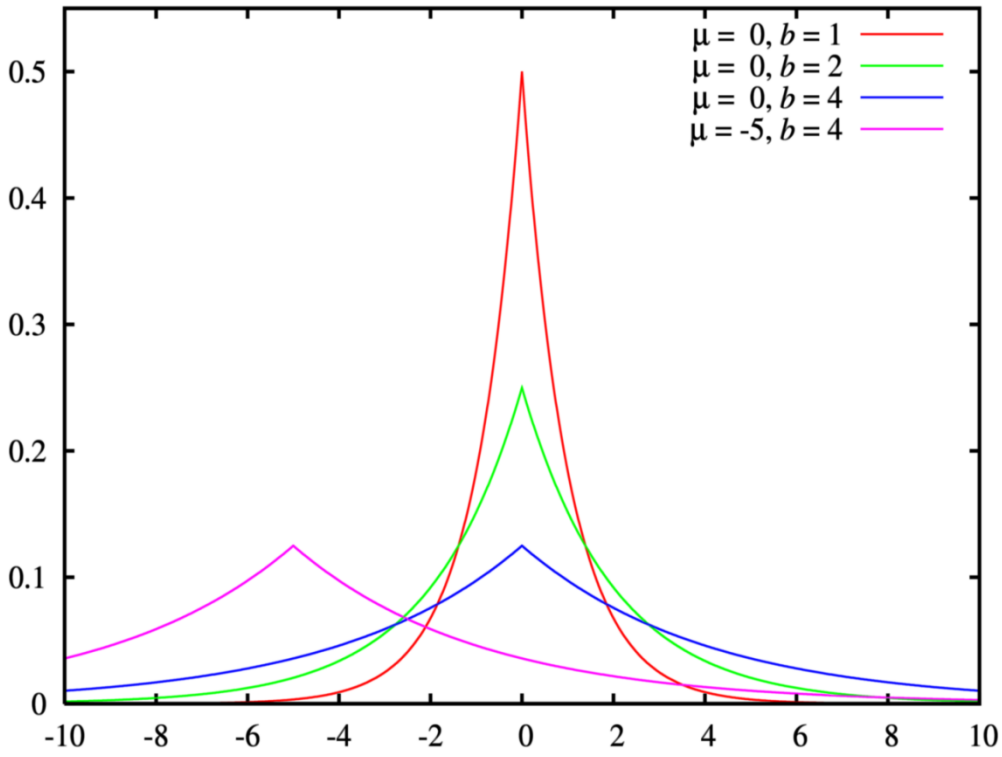
2.15 Analiza DCT koeficijenta

Analizom DCT koeficijenta je moguće ustanoviti mogućnosti višestruke kompresije fotografije. Kod nastanka fotografije, kompresija se vrši samo jedan put, u fotoaparatu. Ako se fotografijom manipulira u računalnim aplikacijama potrebno je ponovno spremiti fotografiju. U tom se slučaju JPEG kompresija ponovo provodi, a samim time u digitalnom zapisu ostaje trag [37].

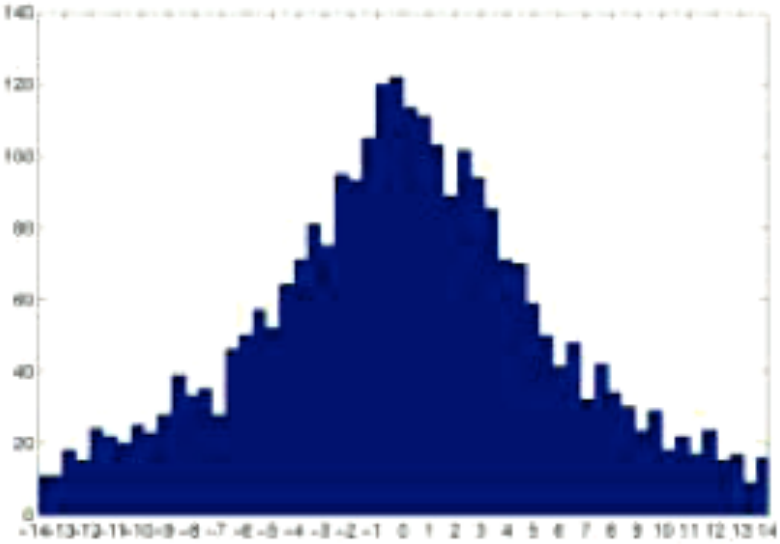
Analizu DCT koeficijenta je moguće provesti samo na fotografijama gdje je primijenjena JPEG kompresija. DCT pretvara prostornu domenu fotografije u frekvencijsku domenu (slika 14).

Koeficijenti DCT su podijeljeni u dvije komponente, *AC* i *DC*. DC koeficijent predstavlja prosječnu vrijednost valne dužine ulaznog signala. Za svaki JPEG blok dimenzija 8 x 8 piksela, postoji samo jedna DC komponenta. Ostale 63 komponente pripadaju u AC koeficijent.

Prije procesa kvantiziranja, vrijednost DCT koeficijenta prilagođava se *Laplacianovoj distribuciji* koja ima karakterističan vrh u sredini (slika 21). Primjenom kvantizacijskih tablica i zaokruživanja na najbliži cijeli broj, krivulja postaje poremećena (slika 22). DCT histogram za svaku AC vrijednost pri prvoj JPEG kompresiji prikazuje periodične vršne vrijednosti .



Slika 21: Prikaz grafa Laplacianove distribucije (Izvor: http://upload.wikimedia.org/wikipedia/commons/8/89/Laplace_distribution_pdf.png)

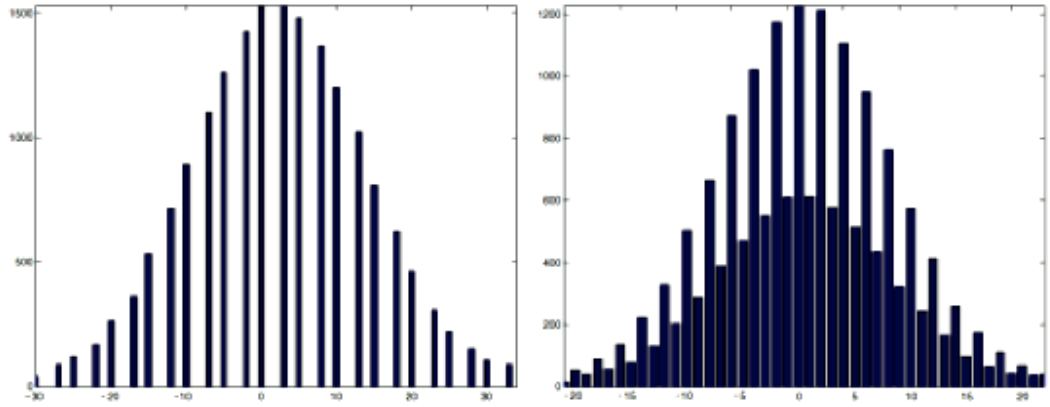


Slika 22: Distribucija AC koeficijenta za sve blokove piksela prije kvantizacije

Kada se drugi put provodi kompresija JPEG fotografije, DCT koeficijent podilazi budućim transformacijama i dvostrukoj kvantizaciji. Pri blagoj kompresiji, drugi kvantizacijski korak ostaviti će manje promjene na fotografiji. Povećanjem kompresije ostati će veći tragovi na konačnoj fotografiji. Uz to, potrebno je voditi računa da su kvantizacijske tablice za luminaciju i chrominance kanale različite.

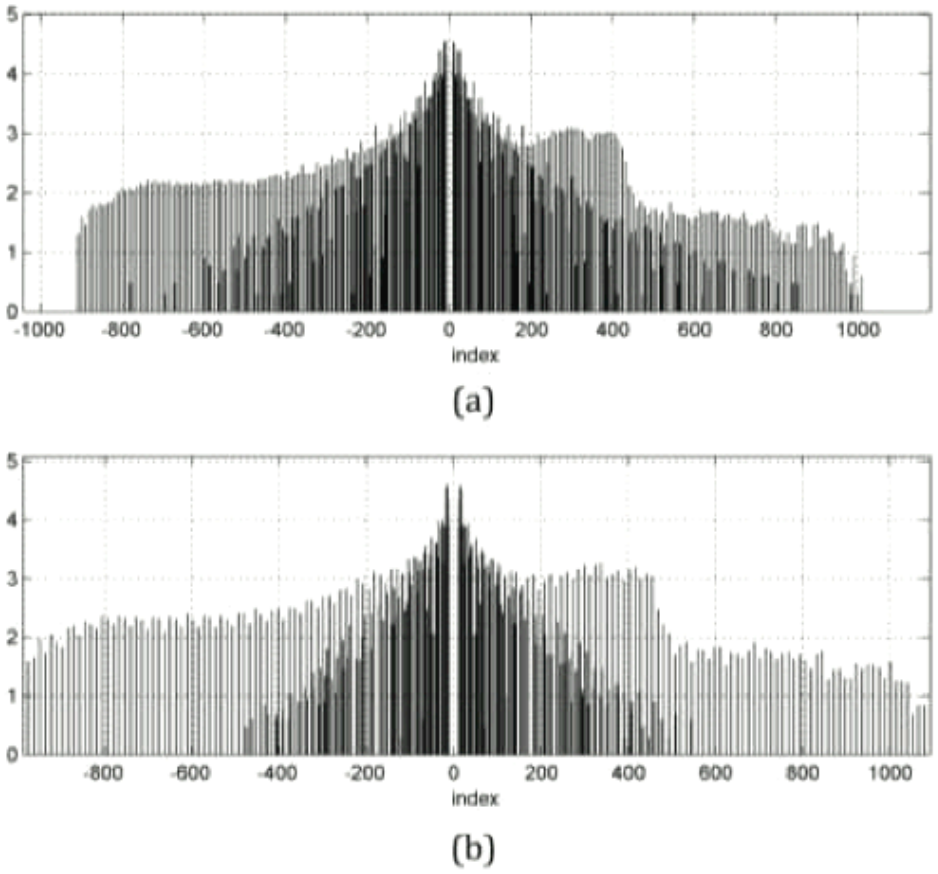
Kod druge JPEG kompresije postoje tri tijeka razvoja događaja. U prvom slučaju, druga kvantizacija *Q2* je manja od prve, primarnke kvantizacije *Q1*, *Q2* < *Q1*. U drugom slučaju, druga kvantizacija je veća od primarne, *Q2* > *Q1.* U trećem slučaju, obje kvantizacije su jednake, *Q2* = *Q1*. Vrijednosti kvatnizacijskih tablica imaju različiti rezultat na distribuciju DCT koeficijenta.

Ako je druga kvantizacija manja od primarne, u DCT histogramu će nedostajati neke vršne vrijednosti (slika 23). Kada je druga kvantizacija veća od primarne, DCT histogram prikazivat će veliku razliku između vršnih vrijednosti.



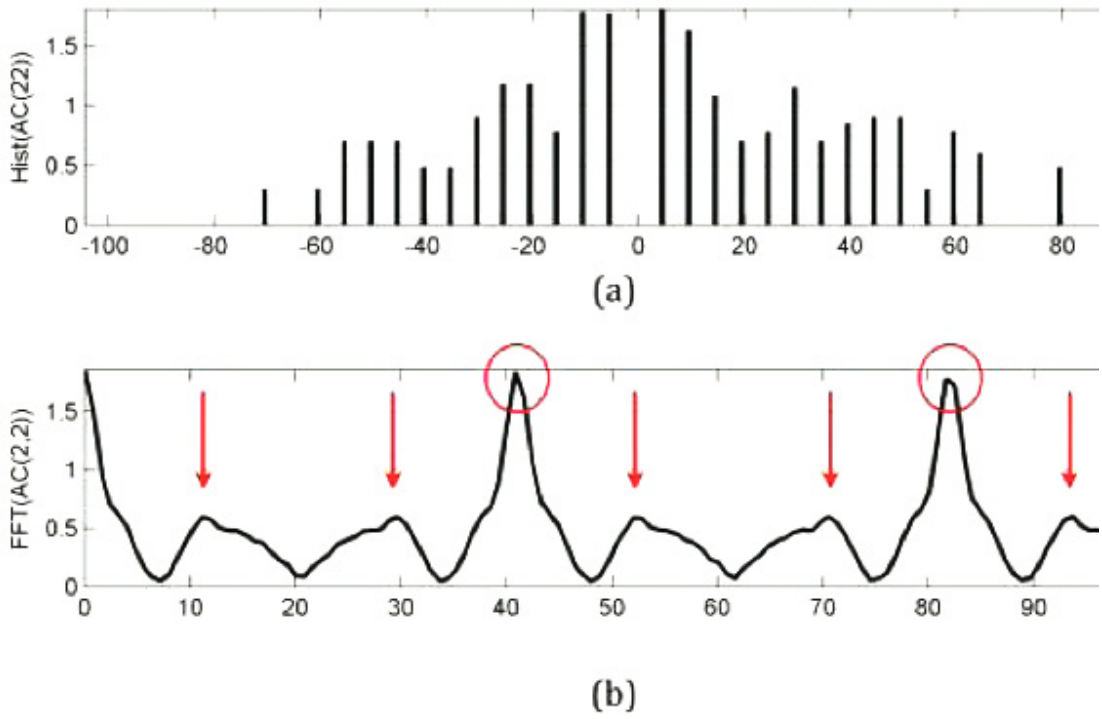
Slika 23: Prikaz vršnih vrijednosti kod dvostruke kvantizacije

Ova tri scenarija su predstavljala jednostavne slučajeve sa pojednostavljenim grafičkim prikazom. U stvarnim slučajevima grafički prikaz je puno kompleksniji (slika 24) jer vrijednost svakog DCT koeficijenta može biti između (0 – 255). U originalnim fotografijama nastalih u fotoaparatu ne postoje preklapanja vršnih vrijednosti jer dolazi samo jednom do procesa kvantizacije.



Slika 24: DCT histogram DC komponente
Histogram realne JPEG fotografije (a)
Histogram manipulirane fotografije te dvostruko kompresirane (b)

Kao dodatak histogramima, periodičnost DCT koeficijenta moguće je prikazati uz računanje *Fourijerovih transformacija* DCT histograma [38]. Anomalije, tj. nestandardne vršne vrijednosti u Fourijerovoj domeni su prikazane kao visoke frekvencije. Na (slici 25a) prikazan je histogram AC koeficijenta dvostruko komprimiranom JPEG zapisa. Kada se na vrijednosti AC koeficijenta primjeni Fourijerova transformacija, dobiva se novi graf koji jasno prikazuje odstupanja (slika 25b).



Slika 25: Prikaz Fourijerove transformacije DCT koeficijenta
Graf vrijednosti AC koeficijenta nakon dvostruke kompresije (a)
Fourijerova transformacija AC koeficijenta (b)

Matthew C. Stamm u svojem radu otkriva slabosti DCT analize pri dvostrukoj kompresiji JPEG fotografija [39]. Dodavanjem male količine šuma među ispravne DCT koeficijente uklanja greške koje nastaju kvantiziranjem. Rezultat su DCT koeficijenti koji su raspoređeni kao kod ne komprimiranih fotografija. Prikazivanje ovakve vrste tragova manipulacije, moguće je postići analizom visokofrekventnih elemenata fotografije [40].

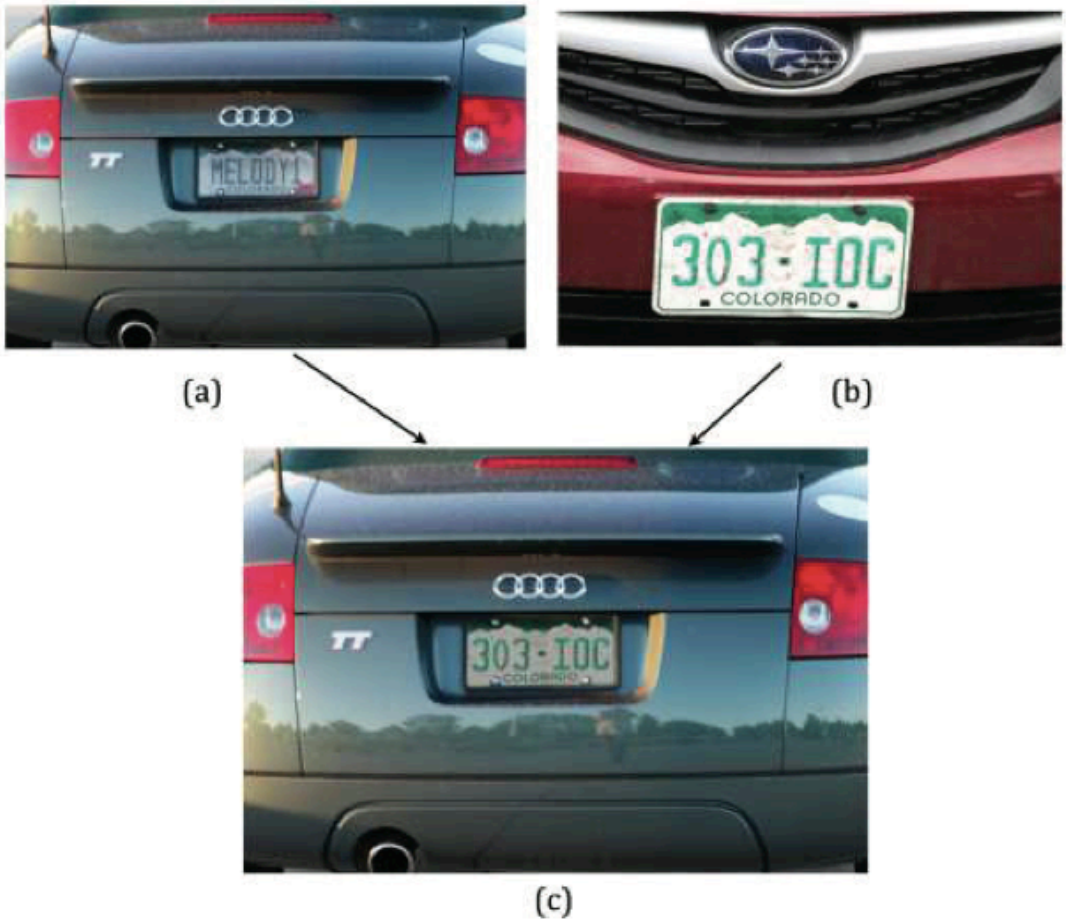
2.16 Analize lokalne strukture fotografije

Globalnom analizom strukture fotografije je moguće ustanoviti da li je fotografija mijenjanja, ali nije moguće ustanoviti područje koje je promijenjeno. Tako je primjerice globalnom analizom moguće ustanoviti da je fotografija smanjena, ali nije moguće ustanoviti da li je još nešto promijenjeno. Na primjer: ako se fotografija želi poslati putem Internata , ali zbog veličine i brzine slanja fotografija se mora smanjiti. Takva fotografija nije krivotvorena već je optimizirana za neku namjenu. Također, umjetničko izražavanje nad fotografijom se ne smatra krivotvornjem.

Lokalna analiza strukture se bavi detekcijom područja fotografije koje je manipulirano. Prilagođavanje svjetline i kontrasta kako bi naglasili dio fotografije mijenja se i vrijednost originalnih piksela, ali ovakve promjene ne mijenjaju sadržaj fotografije. Fotografija se smatra podeksponiranom ako fotografijom prevladavaju tamni tonovi zbog krivog izbora elemenata ekspozicije. Kako bi se ta greška prepravila, naknadno u programu za obradu fotografija se korigira svjetlost. Takva promjena ne mijenja sadržaj fotografije pa se ne bi trebala smatra krivotvorenjem (slika 26).

Slika 26: Primjer korigiranja svjetline na fotografiji

"Nedopuštene manipulacije" fotografijom se mogu opisati sve radnje kojima se stvara iluzija ili prevara na fotografiji (slika 27**)**. Zbog toga postoje algoritmi koji mogu detektirati područje fotografije koje je promijenjeno, a u ovom poglavlju biti će opisani samo algoritmi koji se najviše koriste.



Slika 27: Primjer "nedozvoljene manipulacije" fotografije (Izvor: [3]*)*

2.17 Detekcija manipulacije ljepljenjem elemenata

Identifikacija nedozvoljenih manipulacija u fotografskom kontekstu je vrlo bitan korak u dokazivanju autentičnosti fotografije. Jedna od najkorištenijih tehnika manipulacije je tehnika *copy paste*. Ta tehnika kopira dijelove iste ili različite fotografije te ih lijepi na drugu poziciju. Ova tehnika se koristi na dva načina. Prvi način je dodavanja elemenata koji nisu postojali u trenutku nastajanja fotografije, a drugi način je skrivanje elemenata fotografije. Ova tehnika svojim djelovanjem može zamijeniti sadržaj fotografije bez vidljivih

znakova krivotvorenja. Zbog jednostavnosti i popularnosti ove tehnike, manipulaciju je moguće izvesti koristeći se skoro svim programima za obradu fotografija. Takva vrsta manipulacije naziva se kloniranje. Na primjer: fotografija s vedrim nebom i jednim oblakom. Oblak se može zamijeniti kloniranjem dijelova vedrog nema te time potpuno ukloniti. Veličina područja manipulacije ovisi o veličini objekta kojeg se želi prikriti. Veliko područje manipulacije se primjećuje golim okom jer na fotografiji postoji uzorak koji se ponavlja na više mjesta. Problem nastaje kada je područje manipulacije vrlo malo, jer u tom slučaju ljudsko oko neće primijetiti promjene.

U slučaju kloniranja fotografije sa uzorkom iz iste fotografije, detekcija je vrlo jednostavna. Algoritam koji se upotrebljava za detekciju istih područja traži identične piksele na fotografiji te njihovo ponavljanje. Detekcija se temelji na pretpostavci da je korišteno veliko područje kloniranja za prikrivanje ili dodavanje elemenata. Grupa piksela se uspoređuje sa grupama piksela iste veličine. Ova vrsta analize je vrlo intenzivna zbog količine piksela osim u slučajevima kada je veličina fotografije mala. Također, rezultat ovisi i o količini manipulacije kloniranog područja i o stupnju kompresije manipulirane fotografije. Kako bi se se zaobišla i ova prepreka, koristi se analiza tzv. *robusno podudaranje,* tehnika koja koristi sortirane DCT koeficijente, razvrstavljajući ih po sličnim prostornim karakteristikama [41].

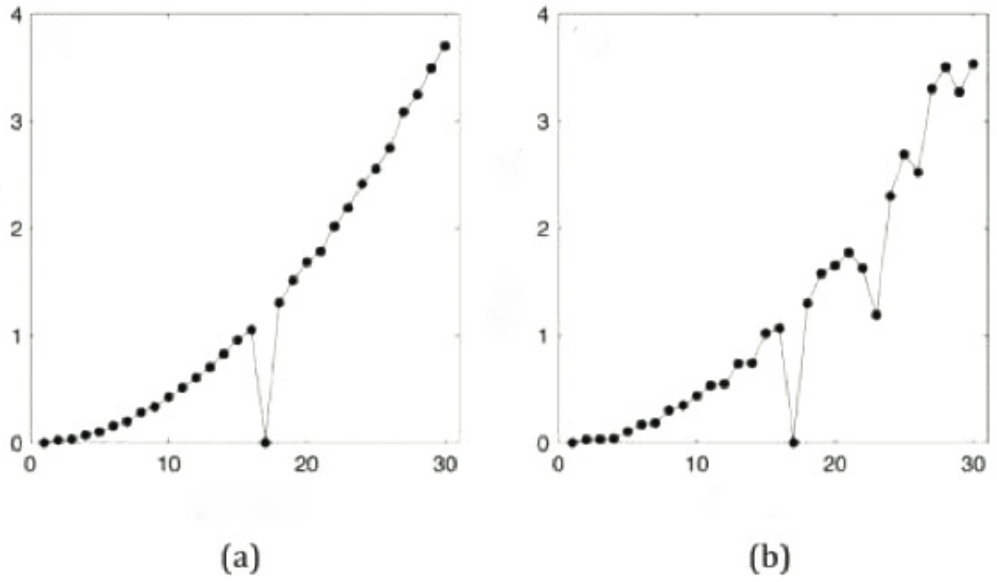
Osim toga, može se koristiti i aberacija boja kako bi se našli dijelovi fotografija nad kojima je provedena manipulacija. Skoro sve optičke leće stvaraju aberaciju boje zbog nemogućnosti ravnomjernoga fokusiranja svih valnih duljina svjetla na fotoosjetljivi senzor. Stupanj prostornog pomaka određuje pomak svjetla od optičkog centra leće objektiva. Kada je fotografija promijenjena, aberacija svjetla postaje nekonzistentna. Aberacija boja se ukazuje na rubovima elemenata fotografije ili u području visokog kontrasta, a ostavlja tragove zelene i magenta boje. Detekcijom *copy paste* tehnike, smjer aberacije boja može biti ne konzistentan. JPEG kompresija može otežati detekciju manipulacije ovom tehnikom pa je pouzdanije rješenje detekcija aberacije boja koja se pojavljuje kloniranjem elemenata.

2.18 Analiza greške JPEG zapisa

Greške nastaju stvaranjem JPEG zapisa, zbog pretvaranja prostorne domene u frekvencijsku domenu korištenjem DCT algoritma. Zatim kvantizacijske tablice izrađuju DCT koeficijente. Najveći dio greški nastaje u procesu kvantizacije, kada se vrijednosti zaokružuju na vrijednost najbližeg cijelog broja. Analiza JPEG greške fokusira se na proces kvantizacije i zaokruživanja pri kompresiji fotografije. U većini slučajeva, kod nastalih fotografija AC koeficijent se opisuje *Laplacianovom krivuljom* [42]. Laplacianova krivulja ima izrazito oštar vrh za razliku od npr. Gausove krivulje koja ima blagi oblik zvona. Kada se provodi proces kvantizacije, AC koeficijenti prestaju biti glatko raspoređeni već se grupiraju ovisno o faktoru kvantizacije Q. Nakon kompresije koeficijenti se ponovo pretvaraju u frekvencijsku domenu, te se radi toga vrijednosti šire Laplacianovom distribucijom ovisno o originalnim kvantizacijskim koracima.

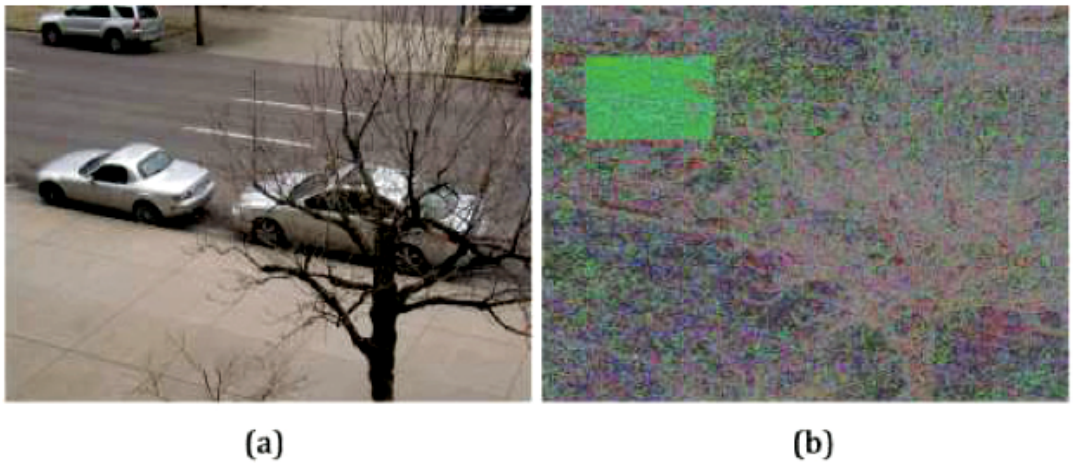
Hany Farid je predstavio još jednu metodu za detekciju manipuliranog prostora fotografije traženjem *JPEG duhova* [43]. Korištenjem JPEG kompresije faktora kvalitete *Q1* nastaje fotografija *C1*. Ako je fotografija ponovo spremljena s faktorom kvalitete *Q2,* nastaje zapis *C2*. Oduzimanjem DCT koeficijenta *C1* od *C2* dobiva se razlika između dvije komprimirane fotografije. Zbrajanjem kvadrante razlike DCT koeficijenta razlika raste povećanjem faktora kompresije *Q2* (slika 28a). Vrijednost će biti najmanja kada su faktori kvalitete jednaki, *Q1* = *Q2*, time otkrivajući faktor kompresije fotografije *C1*.

U drugom slučaju, fotografija komprimirana faktorom kvalitete *Q1* te naknadno komprimirana faktorom kvalitete *Q2* < *Q1*, nastaje fotografija *C2*. Ako se fotografija *C2* kompresira ponovo s faktorom kvalitete *Q1*, nastaje fotografija *C3*. Prikazom kvadratne razlike DCT koeficijenta za rasteći faktor *Q3*, najmanja razlika će biti kada su jednaki koeficijenti *Q3* = *Q2*. Naknadno, druga minimalna razlika će biti kada *Q3* = *Q1*, otkrivajući faktor kompresije fotografije *C1* (slika 28b). Ovaj drugi minimum na grafu, se naziva *JPEG duhom*.



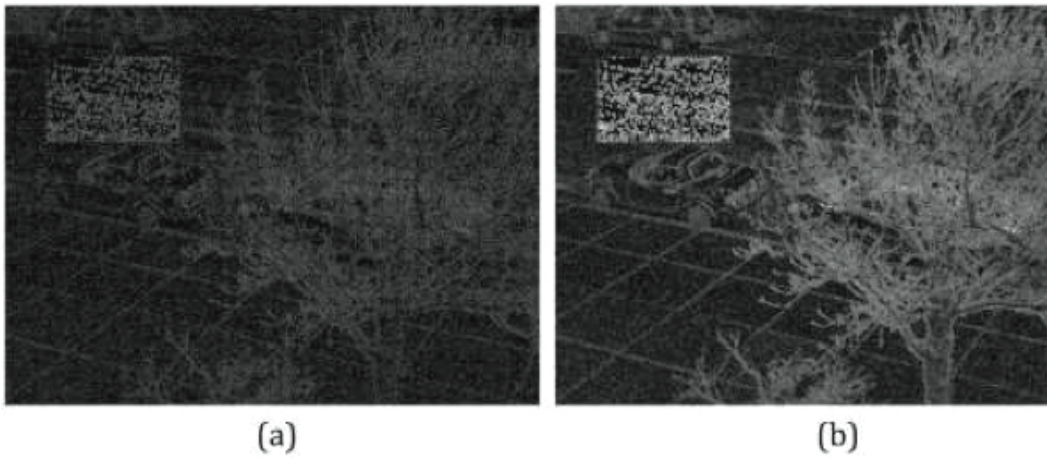
Slika 28: Grafovi prikazuju zbroj kvadratne razlike radi otkrivanja JPEG duhova

Krivotvorena područja mogu se lako dijagnosticirati ako se uzme sumnjiva fotografija, ponovo se kompresira sa drugim faktorom kompresije, te se oduzmu DCT vrijednosti koeficijenta na sumnjivoj fotografijom. Sva područja koja su krivotvorena na fotografiji, prikazivati će *JPEG duh* na manipuliranom dijelu (slika 29). JPEG duh je vrlo istaknut i lako uočljiv na većini fotografija.



Slika 29: Primjer traženja JPEG duhova (Izvor: [3]*)*

Navedena tehnika, upotrebljiva je jedino kada je manipulirano područje u manjoj kvaliteti nego fotografija koja se analizira. Osim toga, bilo kakvo nepodudaranje u polju 8 x 8 JPEG strukture uzrokovati će nemogućnosti stvaranja JPEG duha. Greške je također moguće detektirati označavanjem određenih komponenti DCT koeficijenta. Prve znakove krivotvorenja moguće je detektirati i u DC komponenti, prosjeku ukupne vrijednosti AC komponenti ili značajnim vrijednostima AC komponente svakog JPEG bloka [3]. Ciljajući na DCT označavanje, rezultati analize ovom tehnikom su vrlo učinkoviti (slika 30) [43].



Slika 30: Označavanje DCT komponenti (Izvor: [3]*)*

2.19 Porijeklo nastanka fotografije

Porijeklo nastanka fotografije je proces detekcije i traženja izvora fotografije radi identificiranja uređaja kojim je nastala fotografija. Za uspješnu identifikaciju potrebno je otkriti jedinstvene karakteristike svakog fotoaparata, skenera ili drugog uređaja za nastanak slika. Najveći dio tehnika za otkrivanje izvora temelji se na traženju grešaka fotoosjetljivog senzora. Temeljem takve analize dobiva se dobar temelj za daljnju analizu i dokazivanje autentičnosti.

2.20 Šum i nesavršenost fotoosjetljivog senzora

Senzor zbog svojih mana stvara greške koje nisu sastavni dio scene koja se snima. Tehnološka ograničenja pri dizajnu i proizvodnji fotoosjetljivih senzora stvaraju greške koje su na fotografiji vidljive kao šum. Nesavršenosti su greške koje ostaju konstantne od fotografije do fotografije, dok je šum nasumičan, a ovisi o puno faktora. Greške koje nastaju zbog tehnoloških ograničenja možu se podijeliti u dvije vrste. Prve su nasumične greške, a druge su sistematične. Greške zbog vremena eksponiranja i procesa kvantiziranja nije moguće predvidjeti pa se smatraju nasumičnim. Vrijeme ekspozicije stvara grešku zbog impulsnog načina napajanja svakog piksela senzora. Što je duže vrijeme ekspozicije, više impulsa dolazi do senzora, time stvarajući veću grešku. Kvantizacijska greška nastaje u procesu pretvaranja svjetla iz neograničenih izvora informacija svjetla u ograničeni digitalni zapis. Ovakva greška stvara malu distorziju na fotografiji, ali moguće ju je minimalizirati povećanjem bitova dubine boja.

Šum uzorka je sistematična greška nastala korištenjem električnog foto osjetljivog senzora. Uzorak šuma je konzistentan na svim fotografijama, a sastoji se od šuma u tamnijim tonovima i nejednakosti foto odaziva PRNU (*photo-responce non uniformity*). Šum nastaje na svakom pikselu pojedinačno zbog elektroničkih karakteristika piksela. Šum ima uvijek isti uzorak, ali intenzitet tog šuma ovisan je o temperaturi.

PRNU je dominantan dio šuma uzorka nastao ograničenjima u proizvodnji fotoosjetljivih senzora [29]. Pikseli na fotoosjetljivom senzoru imaju zadaću pretvoriti fotone u elektrone. Zbog greški nastalih u proizvodnji fotoosjetljivih senzora, pikseli nemaju istu osjetljivost na svjetlo, a time uzrokuju šum jer istu jačinu svjetla drugačije bilježe. Dobiveni šum se naziva i *otisak fotoaparata* jer je jedinstven za svaki fotoaparat, a zabilježen na svakoj fotografiji. PRNU je ovisan o svjetlu te se jačina *otiska* pojačava sa intenzitetom svjetla koja dolazi na foto osjetljivi senzor.

Druga karakteristika senzora koja se može koristiti za identifikaciju izvora su neispravni pikseli koji postoje na svima fotoosjetljivim senzorima. Ti neispravni pikseli mogu se locirati i označiti na nastaloj fotografiji te ih koristiti za usporedbu. Budući da danas senzori imaju par miliona piksela, skoro pa je nemoguće da dva senzora na istim mjestima imaju neispravne piksele.

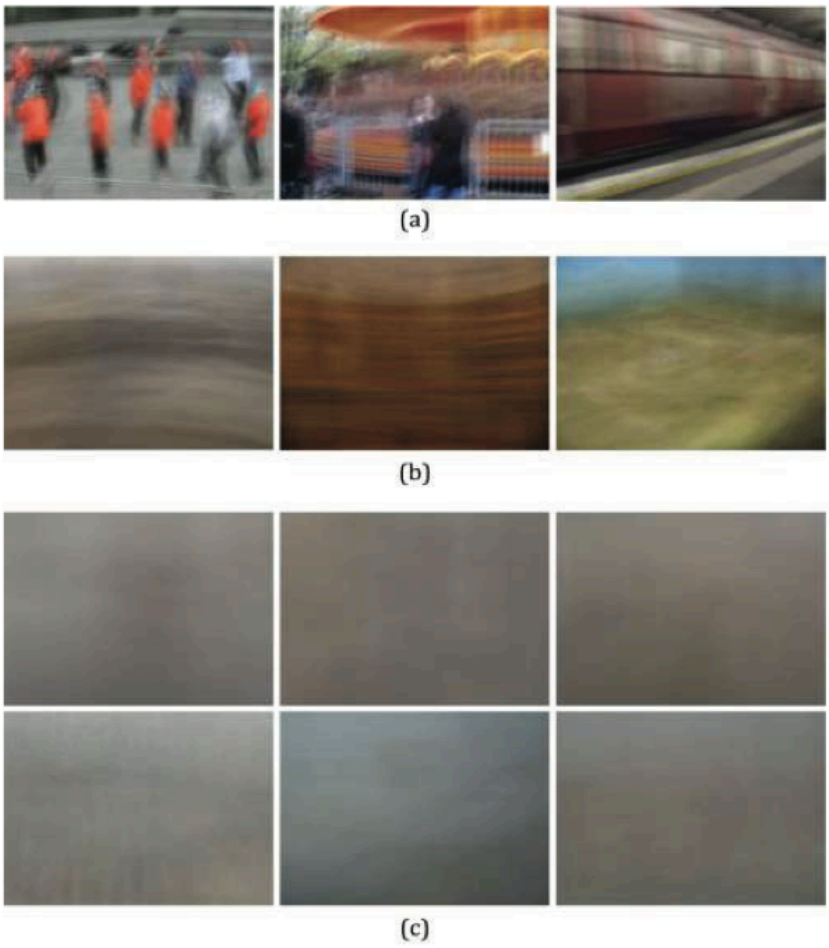
2.21 PRNU uzorak

Karakteristike PRNU svaku fotografiju čine jedinstvenom i omogućuju pronalazak *otiska fotoaparata* tj. fotoosjetljivog senzora [44–49]. PRNU postoji u svim foto senzorima te ga se zato smatra univerzalnim identifikatorom. Informacije koje sadrži PRNU čine ga jedinstvenim za svaki pojedinačni senzor neovisno o postavkama fotoaparata, sadržaja scene ili objektiva. Pokazalo se da kroz dulje vrijeme korištenja u različitim vremenskim uvjetima, PRNU i dalje ostaje nepromijenjen. Djelomično je otporan i na gubitak kvalitete JPEG kompresije, manipulacije fotografijom kao što su podešavanje svjetline, kontrasta, boje i gamuta [45].

Kao jedinstvena komponenta signala PRNU je prisutan u svim fotosenzorima, ali njegovo očitavanje ovisi o kvaliteti senzora i količini svjetla koja dolazi do senzora. Senzori koji se ugrađuju u mobitele i kompaktne fotoaparate imaju ne kvalitetniji čip od profesionalnih DSLR fotoaparata te je na njima lakše očitati PRNU uzorak. Količina svjetla koja dolazi do senzora je vrlo bitna, te da bi se uzorak lakše očitao potrebna je velika količina svjetla koju senzor mora zabilježiti. Zbog toga je PRNU uzorak teško očitati sa fotografija koje su snimljene u tamnim svjetlosnim uvjetima. PRNU uzorak je skoro pa nemoguće očitati sa samo jedne fotografije. Zbog toga nam je potrebna serija fotografija kako bi maknuli neželjeni nasumični šum i izolirali samo PRNU uzorak. Pokazalo se da je za jaki PRNU uzorak potrebno oko 50 fotografija [44].

Ako je sadržaj fotografija jednako osvijetljen, kao npr. kod vedrog neba broj fotografija se smanjuje na osam [50].

Na slici 31 prikazani su primjeri fotografija nastalih istim fotoaparatom. Fotografije su snimljene s različitim kompozicijama, u drugačijim svjetlosnim uvjetima. Korištenjem premalog uzorka fotografija, scena ostaje istaknuta te nije moguće očitati PRNU uzorak (slika 31a). Koristeći više fotografija snimljenih u istim svjetlosnim uvjetima i sa sličnom kompozicijom isto predstavlja problem očitavanja PRNU uzorka (slika 31b). Idealne fotografije za očitavanje PRNU uzorka jesu one koje predstavljaju široki izbor svjetlosnih uvjeta ili osvjetljenja scene. Također ne fokusirane fotografije ili fotografije vedrog nema pomažu u ispravnom očitavanju PRNU uzorka (slika 31c).



Slika 31: Skup fotografija potrebnih za dobivanje PRNU uzorka (Izvor: [3]*)*

Koriste se dvije metode za ublažavanje sadržaja scene nakon računanja prosjeka scene. Prva metoda koristi četvrti stupanj valne dekompresije kako bi prigušila ostatak sadržaja fotografije [44], [46–48]. Ova metoda je vrlo zahtjevna računska operacija te zahtjeva određeno vrijeme da bi se izvršila. Druga metoda je manje zahtjevna računska operacija, a to je primjenjivanje Gausovog zamučivanja fotografije [45], [49]. Dobiveni rezultat prigušene fotografije oduzima se od originalne fotografije. Razlika dobivena između te dvije fotografije je PRNU uzorak.

Uklanjanje šumova i uzimanje prosječnosti fotografije koristi se kod crno bijelih fotografija. Kolor fotografije sadrže tri nivoa boja: zeleni, crveni i plavi. Svaki nivo boje potrebno je zasebno obraditi te se dobivaju tri PRNU uzorka. Kako su kolor nivoi povezani zbog kolor filtera, potrebno ih je spojiti u jednu crno bijelu fotografiju *K* formulom [50]:

$$K = .3K_{crveno} + .6K_{zeleno} + .1K_{plavo} \tag{5}$$

gdje su *Kcrveno*, *Kzeleno* i *Kplavo* PRNU uzorci dobiveni od svakog nivoa boje.

Kada je PRNU uzorak dobiven, potrebno ga je usporediti s bazom PRNU uzoraka od različitih fotoaparata. Fotografije se uspoređuju radi traženja sličnosti koristeći algoritam za promjenu koeficijenta korelacije:

$$corr(X,Y) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(X*Y)}{\sqrt{\sum_{i=1}^{n}\sum_{i=1}^{m}(X*X)*\sum_{i=1}^{n}\sum_{i=1}^{m}(Y*Y)}} \tag{6}$$

gdje su X i *Y* PRNU uzorci fotografija, *m* i *n* visina i širina fotografije, odnosno predstavljaju rezoluciju fotografije. Ovaj algoritam se može koristiti samo kod PRNU uzorka iste rezolucije.

Ako je cilj analize povezati više fotografija sa istim izvorom, fotografije se moraju pripremiti na isti način. Da bi se dokazalo porijeklo fotografije potrebno je imati i pristup izvoru fotografije. U praksi se pokazalo da broj fotografija za ispravan PRNU uzorak osam ako je objekt slikanja izvan fokusa [50]. Jednom dobiveni PRNU uzorak uspoređuje se sa svim fotografijama u bazi, uključujući i sumnjive fotografije.

2.22 Neispravni pikseli

Analiza neispravnim piksela još je jedan od alata koji se koristi pri dokazivanju autentičnosti fotografije. Zbog količine piksela koju svaki foto senzor ima, vrlo je mala vjerojatnost da dva senzor na istim mjestima imaju neispravne piksele. Postoji pet vrsta neispravnih piksela. Najuočljivija neispravnost su *vrući pikseli*, koja se odnosi na piksel koji intezitet svjetla reagira najjačim naponom. Takvi neispravni pikseli stvaraju svjetla područja na fotografiji (slika 32). Zbog korištenja CFA filtera mogu prikazivati svjetlija područja u zelenom, crvenom, plavom i bijelom tonu. Druga vrsta neispravnih piksela su *mrtvi pikseli*, koji više nisu funkcionalni te nemaju reakciju na intenzitet svjetla. Područja *mrtvih piksela* na fotografiji se mogu vidjeti kao crna područja. Pikseli koji imaju *točkastu grešku* osciliraju prema stvarnim vrijednostima više od 6%. *Zaglavljeni pikseli* očitavaju maksimalan intenzitet svjetla. *Defekt bloka piksela* je polje piksela koji se imaju istu grešku.

Slika 32: Primjer vrućeg piksela na nekompresiranoj fotografiji

Vidljivost neispravnih piksela ovisi o sadržaju scene fotografiranja. Najbolji način za lociranje neispravnih *vrućih piksela* je fotografiranje više fotografija u uvjetima jako malog osvjetljenja, te onda računanjem prosjeka fotografija. Nastali nasumični šum će u tom slučaju nestati, a *vrući pikseli* ostati istaknuti. Kada se jednom ustanovi pozicija neispravnih piksela, na drugim fotografijama nastalih istim izvorom, lociranje postaje vrlo jednostavno.

Provedeno je istraživanje kako bi se ustanovila konzistentnost neispravnih piksela u ovisnosti o temperaturi [3]. Fotografije su snimane sa fotoaparatima na temperaturi od 0 do 40 ^{0}C. Pokazalo se da se smanjenjem temperature otežava pronalazak neispravnih piksela, ali kada se jednom locira, na drugim fotografijama ga je lako pronaći.

Jedno istraživanje pokušalo je odrediti utjecaj JPEG kompresije na vidljivost neispravnih piksela [3]. Rezultati pokazuju da JPEG kompresija do 50% nema utjecaja na vidljivost neispravnih piksela. Nakon toga, zbog JPEG načina zapisa, pikseli se počinju mijenjati i širiti prema susjednim pikselima.

2.23 Analiza stupnja inteziteta svjetla

Luminacija je mjera za nivo osvjetljenja fotografije koju foto osjetljivi senzor prihvaća [51]. Ako su dvije fotografije zabilježene sa dva različita fotoaparata pod različitim svjetlosnim uvjetima u slučaju razmjene elemanata tehnikom *copy paste* postojati će razlika koja možda nije vidljiva golim okom. Uglavnom, analizom stupnja luminacije se traže područja koja na istim optičkim udaljenostima ima različiti stupanj osvjetljenja. Manipulacija fotografijom ovisi isključivo o znanju manipulatora te njegovoj vještini maskiranja fotografije.

Kolor ili crno bijela fotografija moguće je pretvoriti u binarni slikovni zapis temeljen na zadanim vrijednostima praga. Binarni zapis fotografije može imati piksel zabilježen u crnoj ili bijeloj boji [51]. Određivanje gdje pripada koji piksel temelji se na zadanom pragu, koji u ovom slučaju može biti intenzitet svijetla fotografije.

Prag intenziteta svjetla fotografije može predstavljati decimalna znamenka vrijednosti od 0,00 do 1,00 [25]. Ako je vrijednost praga 0,75, a piksel ima vrijednost manju ili jednaku 0,75, uzima vrijednost crne boje. U slučajevima kada bi se za prag uzela vrijednost 1,00 cijeli binarni zapis fotografije bi bio crna boja, a ako bi se za prag uzela vrijednost 0,00 fotografija bi bila potpuno bijela. Određivanje ispravnog praga ovisno je o vrsti fotografije koja se analizira. Za početnu vrijednost bilo bi dobro uzeti 0,50, a onda ovisno o dobivenim rezultatima povećavati ili smanjivati prag. Generalno, cilj je prikazati sumnjiva područja koja mogu svjedočiti nenormalnim intenzitetima svjetla. Na slici 33 se nalazi duplikat slike 34a koja je zapisana kao bit mapa.

Slika 33: Binarni zapis fotografije s pragom svjetline 0.50

2.24 Analiza tona, zasićenja boje i intenziteta svjetla

Standardni zapis fotografije kao što je JPEG koristi RGB prostor boja. U RGB zapisu boja, svaki piksel ima vrijednost koja se sastoji od crvene, plave i zelene komponente [25]. Takav način prikaza smatra se standardom za stvaranje slike na računalima. U prostoru boja HSV (*Hue, Saturation, Value)* boje su opisane pomoću tona boje, zasićenja boje i intenziteta svjetla [51]. Na slici 38 a i b prikazane su fotografije u RGB prostoru boja odnosno HSV prostoru boju.

Slika 34: Fotografija prikazana u RGB i HSV prostoru boja

Prostor boja i svjetlina fotografije omogućuju jedinstvene metode analize fotografije. Odstupanja i anomalije u prikazu iniciraju mogućnosti manipulacije fotografijom. Ovim metodama pokušavaju se analizirati fotografije u različitim prostorima boja pri različitim intenzitetima svjetla u potrazi za znakovima manipuliranja. Kada je neko područje sa jedne fotografije spojeno sa drugom fotografijom takva fotografija se smatra manipuliranom. U tom slučaju pridodani elementi imaju različiti ton, intenzitet svjetla i zasićenje boja zbog nastanka fotografije pod drugačijim svjetlosnim uvjetima i zbog drugačijeg izvora fotografije [25]. Spomenutom HSV metodom moguće je otkriti područja manipulacije koja je zatim potrebno detaljno analizirati.

2.25 Detekcija rubova pomoću operatora prvog reda

Algoritmi za detekciju rubova svrstavaju se među klasične tehnike obrade fotografija, a primjenjuju se skoro uvijek pri traženju znakova manipulacije nad fotografijama [52]. Rubovi elemenata u fotografiji su vrlo bitni jer prikazuju položaj objekta, njegovu teksturu, veličinu i oblik. U analizi manipulacije fotografijom, detekcijom rubova se mogu otkriti dupli rubovi koji nastaju pri dodavanju elemenata u postojeću fotografiju. Do tog fenomena dolazi zbog zamućivanja prostora okolo nalijepljenih elemenata koji zajedno sa postojećim elementima tvore dupli rub.

Rub elemenata smatra se područje gdje se vrijednost intenziteta piksela mijenja iz vrlo visoke u vrlo nisku i obrnuto[53]. Operatori prvog reda u fotografiji traže točke prekida funkcijom koja za računanje koristi derivacije prvoga reda. Postoje razne maske za detekciju rubova koje se koriste kod analize fotografija među kojima su poznatije *Roberts, Sobel i Prewitt* maske [52]. Sobel maska je više osjetljiva na rubove u prostoru nego na rubove u horizontalnom i vertikalnom području. Maska Roberts ima sposobnost detektirati rubove i kod većih šumova u fotografiji dok je Prewitt maska bolja traženja vertikalnih i horizontalnih rubova [53].

2.26 Detekcija rubova pomoću operatora drugog reda

Operatori prvog reda jesu dobra temeljna tehnika koja se koristi pri analizi fotografije i detekciji manipulacije, dok operatori drugoga reda nude izrazitu mogućnost detekcije rubova elemenata fotografije. Zbog tehnika koje se primjenjuju, analiza je puno temeljitija, a time i pronalazak rubova puno veći i točniji. Algoritmi koji se nalaze u ovoj skupini koriste Laplacianove i Gausove

funkcije za analizu fotografija [53]. Mogućnosti detekcije rubova omogućavaju otkrivanje diskontinuiteta na fotografiji, a time i otkrivanje prvih znakova manipulacije nad fotografijom [52].

2.27 Alternativne tehnike detekcije rubova

Tehnike detekcije rubova pomoću operatora prvog i drugog reda uglavnom se temelje na Sobel i Prewitt maskama. Takve tehnike analize sadržaja fotografije koriste se radi otkrivanja duplih rubova. Drugo zanimljivo područje analize kako bi saznali što više informacija o fotografiji su primjena visoko prolaznih i nisko prolaznih filtera [25]. Ove metode filtriranja omogućuju drugačiji pristup analizi fotografije te mogu otkriti sitne anomalije koje mogu biti trag "krivotvorenju".

Korištenje filtera u prostornoj domeni temelji se na analiziranju piksela i svojstva okolnih piksela [54]. U slučaju kada je polje piksela veličine 3 x 3, svaki piksel za analizu ima uz sebe još i osam susjednih piksela. U prikazu ispod nalazi se apstraktni prikaz svakog piksela i njegovih osam susjednih piksela.

$$\begin{matrix} \left(x_{i-1,j-1}\right) & \left(x_{i-1,j}\right) & \left(x_{i-1,j+1}\right) \\ \left(x_{i,j-1}\right) & \left(x_{i,j}\right) & \left(x_{i,j+1}\right) \\ \left(x_{i+1,j-1}\right) & \left(x_{i+1,j}\right) & \left(x_{i+1,j+1}\right) \end{matrix} \tag{7}$$

Gdje je $x_{i,j}$piksel na poziciji *i,j* na fotografiji X, a ostatak varijabli predstavlja susjednih osam piksela [25]. Vrijednosti u skupu cijelih brojeva za svaki analizirani piksel obrađuje se *konvolucijskom maskom.* Formalno, dobivene vrijednost od piksela $x_{i,j}$i njegovih osam susjeda množe se sa odgovarajućim konvolucijskim koeficijentima te se međusobno zbrajaju.

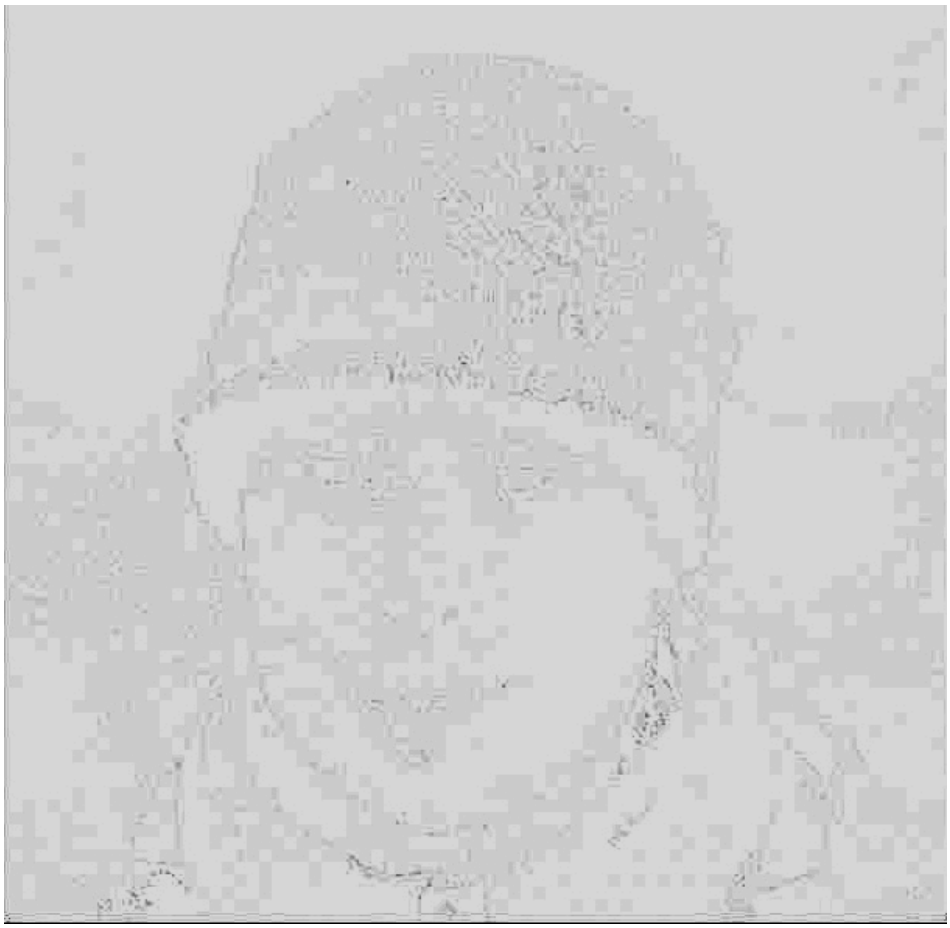
Dobivena vrijednost sada predstavlja varijablu $x_{i,j}$. U prikazu ispod prikazana je *konvolucijska maska* koja ostaje konzistentna u cijelom procesu filtriranja:

$$\begin{matrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{matrix} \tag{8}$$

U ovoj tehnici, dokazi koji upućuju na "krivotvorenje" otkrivaju duple rubove ili abnormalne uzorke na fotografiji. Dobro odabrani ili napravljeni uzorci povećavaju šansu otkrivanja anomalija u fotografiji, a najvažniji faktor je optimalna konvolucijska maska.

$$\begin{bmatrix} -1 & -2 & -1 \\ -2 & 12 & -2 \\ -1 & -2 & -1 \end{bmatrix} \tag{9}$$

Središnji piksel ima vrijednost 12 dok suma susjednih piksela iznosi –12. Analizom fotografije filtriraju se sve statistički slične vrijednost te se prikazuju samo bitno različite. Dobivene vrijednosti koje se ističu označavaju rubove elemenata ali i potencijalnu mogućnost manipuliranja fotografijom. Prikaz rezultata po prirodi je vrlo taman pa se radi lakšeg pregleda i analize rezultat invertira kako bi na bijeloj podlozi dobili sivo bijele tonove. U cijelom ovo procesu, fotografija se prvo pretvara iz RGB prostora boja u crno – bijeli prostor boja, a ta pretvorba nema utjecaja na statističke podatke o fotografiji. Nakon toga kreće proces filtriranja. Slika 35 prikazuje rezultat filtriranja fotografije.



Slika 35: Inverzni rezultat primjene alternativnih filtera

Ovom metodom dobiven je filtrirani prikaz originalne fotografije čiji rezultat je izokrenut radi lakšeg prikaza. Zbog veličine fotografije i detalja ponekad je potrebno dodatno analizirati dijelove unutar fotografije zbog šumova i skrivenih rubova koje sadrži fotografija.

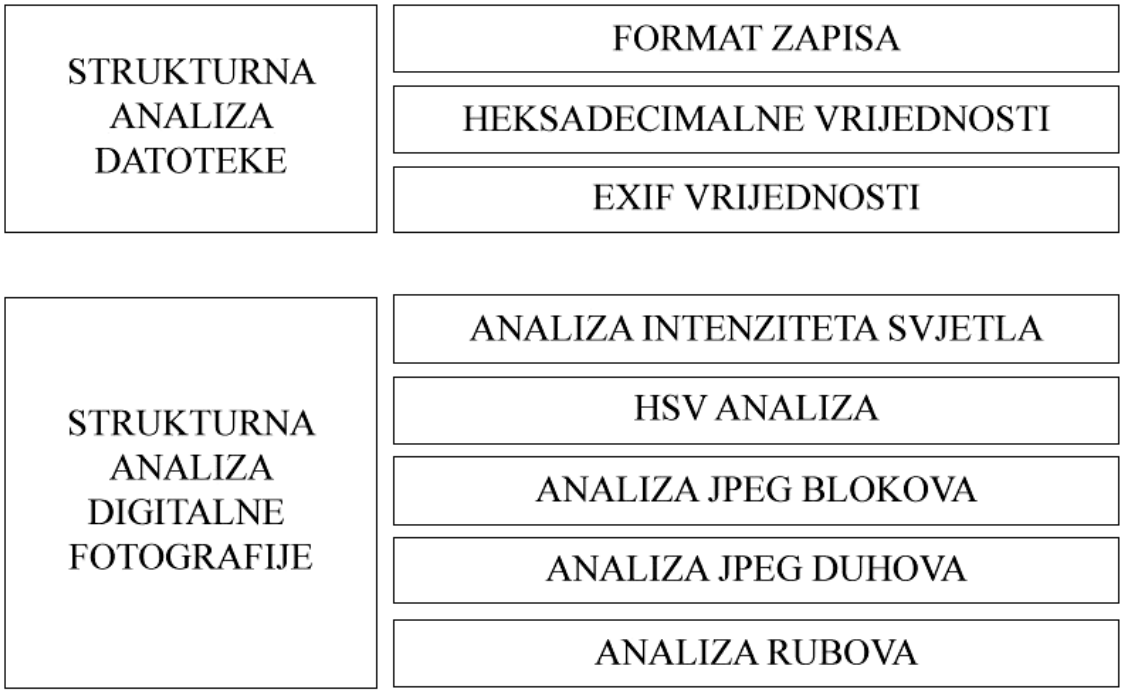
3 EKSPERIMENTALNI DIO

Zadatak analize i istraživanja digitalnog zapisa fotografske slike radi dokazivanja autentičnosti vrlo je složeni proces u kojem je uz korištenje raznih metoda za analizu vrlo bitan faktor i istražitelj tj. njegovo razumijevanje i interpretacija dobivenih rezultata. Digitalna je fotografija skup binarnih vrijednosti pohranjenih na mediju za pohranjivanje po unaprijed zadanim pravilima i algoritmima. Zbog toga je digitalna datoteka matematičke prirode, a ne fizičke. Ispitivanje i analiza zahtijevaju određenu razinu stručnosti i temeljno poznavanje procesa nastanka fotografije kako bi se sistematično moglo krenuti u proces dokazivanja autentičnosti. Svaka fotografija je jedinstvena, a time i svaki slučaj dokazivanja autentičnosti. Zaključke ispitivanja donosi istražitelj, a tehnike za analizu fotografije su samo alat kojim se služi. Svakom tehnikom analize istražitelji dobivaju sve više informacija o fotografiji, njezinom nastanku i načinu izrade.

3.1 Opis ispitivanja

Za ispitivanje autentičnosti digitalnog zapisa fotografije napravljen je optimalan model proizašao iz tehnika opisanih u teoretskom dijelu ovoga rada. Model se dijeli na dva dijela, prvi dio koji će se baviti analizom strukture digitalne datoteke i drugim dijelom koji će se baviti strukturnom analizom digitalne fotografije (slika 36). Analiza strukture datoteke bavi se proučavanjem podataka o digitalnom zapisu te njegovom nastanku. Ovim se želi ustanoviti format zapisa digitalne fotografije. Zatim će se analizirati EXIF zapis u potrazi za nedosljednim informacijama. Ovakvom vrstom ispitivanja uglavnom je

odmah moguće ustanoviti da li su prikazani podaci točni ili lažni. Ako su podaci promijenjeni ne mora značiti da je sadržaj fotografije krivotvoren, nego može biti samo naznaka da je računalna aplikacija za obradu fotografija bila u interakciji sa fotografijom.



Slika 36: Model za ispitivanje autentičnosti digitalne fotografije

Nakon provedene analize *strukture datoteke* prelazi se na *strukturnu analizu digitalne fotografije*. U strukturnoj analizi istraga se provodi na nivou piksela u potrazi za manipuliranim područjima. Uglavnom se traže znakovi *copy paste* načina manipuliranja. Primijenjene tehnike temelje se na statističkoj analizi korištenjem algoritama specijalizirane namjene. U drugom dijelu analize koristiti će se tehnike temeljene na analizi intenziteta svjetla, tona, boje, detekcije rubova, JPEG duhova, greške JPEG zapisa i kompresiji fotografije.

Intenzitet svjetla, ton i boja svojstva su koja utječu na nastajanje fotografije, a njihovom obradom u fotoaparatu nastaje konačna digitalna fotografija. Mijenjanjem tih vrijednosti računalnim aplikacijama za obradu

fotografija, manipulirana područja fotografije mogu imati bitno drugačija svojstva od originalne okoline. Zbog toga se provodi analiza intenziteta svjetla, tona i boje. U ovoj analizi nužna je interakcija čovjeka i računala, a algoritmi koji se koriste u analizi su samo alat. Zaključak donosi istražitelj koji na temelju dobivenih rezultata i prikaza fotografije određuje postoje li znakovi manipulacije.

Za detekciju duplih rubova i traženje duhova na fotografiji u ovom modelu koriste se algoritmi sa visoko prolaznim filterima i određenim konvolucijskim maskama radi temeljne analize. Zbog lakšeg pregleda, u dobivenom rezultatu boje se prikazuju obrnuto kako bi se vidjela područja manipulacije. Također, rezultat se mora pažljivi pogledati u potrazi za duplim rubovima ili sitnim greškama nastalim kod manipulacije. Kod nekih dobivenih rezultata na prvi pogled se ne vide razlike te je potrebno dodatno pojasniti dobiveni prikaz povećanjem kontrasta.

Izradom krivotvorene fotografije iz dvije ili više JPEG fotografija može doći do odstupanja u statističkim podacima. Kada je fotografija krivotvorena, može sadržavati razne komadiće koji su smanjeni, izrezani, izokrenuti kako bi prikaz bio što realniji. Također, dijelovi fotografije nisu komprimirani istim faktorom kvalitete. Svi ti faktori utječu na stvaranje sitnih anomalija u digitalnom zapisu. Zbog toga se primjenjuje tehnika analize kompresije JPEG zapisa koja fotografiju dijeli u blokove 8 x 8 piksela te analizom svakog bloka fotografije traži statističke anomalije.

U ispitivanju će biti četiri različita slučaja sa fotografijama "nepoznatog porijekla". Kroz analizu uz unaprijed predloženi model testiranje će se vršiti svim tehnikama te će se donijeti zaključak ovisan o ukupnom rezultatu testirana. Slučajevi fotografija su predstavljeni na (slici 37, slici 38, slici 39, slici 40).

Slika 37: Prvi slučaj istrage autentičnosti fotografije

Slika 38: Drugi slučaj istrage autentičnosti fotografije

Slika 39: Treći slučaj istrage autentičnosti fotografije

Slika 40: Četvrti slučaj istrage autentičnosti fotografije

Rezultati analize ovih tehnika mogu dati dovoljan dokaz i znakove manipulacije nad fotografijom. U prvom dijelu analize će se koristiti računalne aplikacije otvorenog koda *file* i *JPGsnoop,* a u drugom dijelu analize zbog specifičnih potreba i tehnika analize koristiti će programski kod napisan u računalnoj aplikaciji MATLAB. Primjenom ovog modela prikazi će se nekoliko scenarija i postupak istraživanja i analize digitalne fotografije. U svrhu bilježenja rezultata napravljena je tablica u kojoj su navedene sve tehnike analize te kategorije gdje se označuje uspješnost pojedinih analiza. Predloženi model prvenstveno se usredotočuje na analizu krivotvorina nastalih *copy paste* tehnikom. Za fotografije koje sadrže dijelove koji nisu izvorni dio scene, može se sa sigurnošću reći da su krivotvorene. Ovim područjem su se J. Fridrich i J. Lukas intezivno bavili te razvili vrlo učinkovite tehnike za detekciju krivotvorenih područja fotografije . Najbolji način za dokazivanje autentičnosti je korištenje testova primjenom što više različitih tehnika analize. Kvaliteta manipulacije fotografijom najviše ovisi o autoru manipulacija, a detekcija vrhunskih manipulacija iziskuje mnogo vremena i strpljenja u analizi. Svakim danom nastaju nove tehnike manipulacije, a time nastaju i nove tehnike, metode i modeli za analizu i ispitivanja digitalnih fotografija u svrhu dokazivanja autentičnosti.

4 REZULTATI I RASPRAVA

Primjenom modela za ispitivanje autentičnosti digitalne fotografije istražena su četiri slučaja. Svaka fotografija se može smatrati posebnim slučajem i svakom istraživanju treba pristupiti sa puno pažnje za primjećivanjem detalja. Učinkovitost ovog modela te pojedinih tehnika predstavljena je u ovom poglavlju. Ispitivanje se vrši sistematično za svaku fotografiju posebno, a svakim ispitivanjem se dobiva sve više informacija o nastanku digitalne fotografije.

4.1 Strukturna analiza datoteke

4.1.1 Format zapisa

Prvi korak kod istraživanja digitalne fotografije je ispitivanje strukture digitalnog zapisa kako bi se utvrdilo da li datoteka uopće odgovara JPEG pravilima zapisa. Ovo ispitivanje provodi se jer računalo ne zna razliku pri imenovanju datoteka, a time je moguće proizvoljno imenovati bilo koju datoteku i ekstenziju. Rezultati u *Tablici 1*prikazuju da je u svim slučajevima JPEG zapis ispravan. Ispitivanje je izvršeno s računalnom aplikacijom *file* , a rezultati dobiveni su:

- Slučaj_1.jpg: JPEG image data, JFIF standard 1.02
- Slučaj_2.jpg: JPEG image data, JFIF standard 1.01
- Slučaj_3.jpg: JPEG image data, JFIF standard 1.02
- Slučaj_4.JPG: JPEG image data, EXIF standard

Također, dobiveni rezultati prikazujui standard koji se koristio pri zapisu JPEG fotografije.

Tablica 1: Rezultati ispitivanja formata digitalnog zapisa

SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1	**X**		
Slučaj 2	**X**		
Slučaj 3	**X**		
Slučaj 4	**X**		

4.1.2 Heksadecimalne i EXIF vrijednosti digitalnog zapisa

Za analizu i pregled EXIF i heksadecimalnih vrijednosti koristila se računalna aplikacija *JPEGsnoop* koja detaljno prikazuje parametre fotografije. U tablici 2, prikazani su dobiveni rezultati. Računalnom aplikacijom *JPEGsnoop* moguće je vidjeti sve parametre nastanka fotografije, od modela fotoaparata do svakog pojedinog elementa ekspozicije pri nastanku digitalne fotografije.

Tablica 2: Ispitivanje EXIF i heksadecimalnih vrijednosti

SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1		**X**	
Slučaj 2		**X**	
Slučaj 3		**X**	
Slučaj 4	**X**		

U prvom, drugom i trećem slučaju postoje mogući znakovi manipulacije jer je među EXIF podacima pronađen zapis o interakciji računalne aplikacije i ispitivane fotografije. Dio EXIF podatak sadrži informacije o proizvođaču i modelu fotoaparata i vremenu nastanka tj. zadnjem vremenu interakcije računalne aplikacije i fotografije (slika 41, slika 42 ,slika 43). Međutim, EXIF zapis je samo zabilježio interakciju fotografije i računalnog programa, ali ne i stvaru promjenu u samoj fotografiji. U ovim slučajevima postoji mogućnost samo da je digitalnoj fotografiji promjenjena veličina.

```
EXIF IFD0 @ Absolute 0x00000026
  Dir Length = 0x000C
  [ImageDescription                ] = "OLYMPUS DIGITAL CAMERA         "
  [Make                            ] = "OLYMPUS IMAGING CORP.  "
  [Model                           ] = "SP800UZ                "
  [Software                        ] = "Adobe Photoshop CS4 Windows"
  [DateTime                        ] = "2013:01:27 13:11:39"
  [ExifOffset                      ] = @ 0x03E0
  Offset to Next IFD = 0x00000644
```

Slika 41: Prikaz dijela EXIF podataka iz Slučaja 1

```
EXIF IFD0 @ Absolute 0x00000026
  Dir Length = 0x000B
  [Make                              ] = "NIKON CORPORATION"
  [Model                             ] = "NIKON D90"
  [Orientation                       ] = Row 0: top, Col 0: left
  [XResolution                       ] = 300/1
  [YResolution                       ] = 300/1
  [ResolutionUnit                    ] = Inch
  [Software                          ] = "Adobe Photoshop CS6 Windows"
  [DateTime                          ] = "2013:01:15 22:39:48"
  [ExifOffset                        ] = @ 0x00F0
  [GPSOffset                         ] = @ 0x0380
  Offset to Next IFD = 0x00000394
```

Slika 42: Prikaz dijela EXIF podataka iz Slučaja 2

```
EXIF IFD0 @ Absolute 0x00000026
  Dir Length = 0x000C
  [ImageDescription                  ] = "OLYMPUS DIGITAL CAMERA "
  [Make                              ] = "OLYMPUS IMAGING CORP.  "
  [Model                             ] = "SP590UZ                "
  [Software                          ] = "Adobe Photoshop CS4 Windows"
  [DateTime                          ] = "2013:01:19 01:20:14"
  Offset to Next IFD = 0x00000670
```

Slika 43: Prikaz dijela EXIF podataka iz Slučaja 3

U četvrtom slučaju nema nikakvih znakova manipulacije niti tragova koji upućivali na bilo kakvu manipulaciju (slika 44). Kako se vidi u EXIF zapisima, svaki zapis je različiti ovisno proizvođaču fotoaparata jer EXIF nema definirane standardne kategorija koje bi svi proizvođači trebali upisivati.

```
EXIF IFD0 @ Absolute 0x00000014
   Dir Length = 0x000B
   [Make                             ] = "Canon"
   [Model                            ] = "Canon EOS 1100D"
   [Orientation                      ] = Row 0: top, Col 0: left
   [XResolution                      ] = 72/1
   [YResolution                      ] = 72/1
   [ResolutionUnit                   ] = Inch
   [DateTime                         ] = "2012:03:13 16:30:27"
   [Artist                           ] = ""
   [YCbCrPositioning                 ] = Co-sited
   [Copyright                        ] = ""
   [ExifOffset                       ] = @ 0x015C
   Offset to Next IFD = 0x000022F0
```

Slika 44: Prikaz dijela EXIF podataka iz Slučaja 4

4.2 Strukturna analiza digitalne fotografije

4.2.1 Analiza intenziteta svjetla

Analiza intenziteta svjetla koristi se radi otkrivanja manipulacije *copy paste* tehnikom iz više različitih fotografija. Naime, ako su dvije fotografije zabilježene sa dva različiti fotoaparata pod različitim svjetlosnim uvjetima stvoriti će se razlika koja nije vidljiva golim okom. Analizom intenziteta svjetlosti otkriti će se razlika u područjima koji na istoj optičkoj udaljenosti imaju različiti stupanj osvjetljenja. U tablici 3prikazni su rezultati dobiveni ovom analizom.

Tablica 3: Rezultati analize intenziteta svjetla

SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1	**X**		
Slučaj 2	**X**		
Slučaj 3		**X**	
Slučaj 4	**X**		

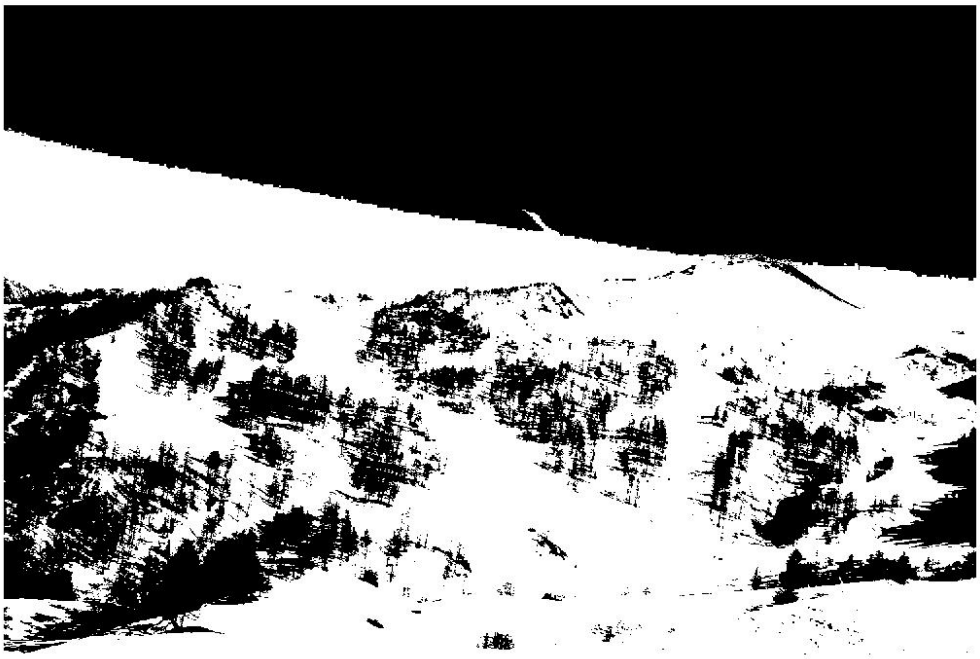
U prvom, drugom i četvrtom slučaju ne postoji dovoljno znakova koji bi naslućivali mogućnosti manipulacije jer se niti jedno područje nema veliko odstupanje od svoje okoline (slika 45, slika 46, slika 47). U trećem slučaju oblak

ima dosta različiti intenzitet svjetla naspram svoje okoline, a zbog toga postoji sumnja da je nastao u različitim svjetlosnim uvjetimašto upućuje na prve znakove manipulacije *copy paste* tehnikom (slika 48).

Slika 45: Slučaj 1, analiza intenziteta svjetla

Slika 46: Slučaj 2, analiza intenziteta svjetla

Slika 47: Slučaj 3, analiza intenziteta svjetla



Slika 48: Slučaj 4, analiza intenziteta svjetla

4.2.2 Analiza tona, zasićenja boje i svjetline

Ovom analizom fotografije se prikazuju u drugačijem prostoru boja, a samim time imaju drugačiji pogled na tonove, zasičenje boja i svjetlinu. Manipulirana područja koja su zaljepljena na originalnu fotografiju mogu imati različite tonove, zasičenje i svjetlinu koju u RGB prostoru boja nije moguće uočiti. Zbog toga se primjenjuje ova tehnika, a rezultati su prikazani u *tablici 4*.

Tablica 4: Rezultati HSV analize

SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1	**X**		
Slučaj 2			**X**
Slučaj 3	**X**		
Slučaj 4	**X**		

U prvom slučaju nije moguće ispravno provesti HSV analizu jer je fotografija crno bijela. Za uspješnu analizu potreba je kolor fotografija kako bi se što učinovitije analizirao svaki piksel te usporedo ton, zasičenje i svjetlina sa okolinom (slika 49).

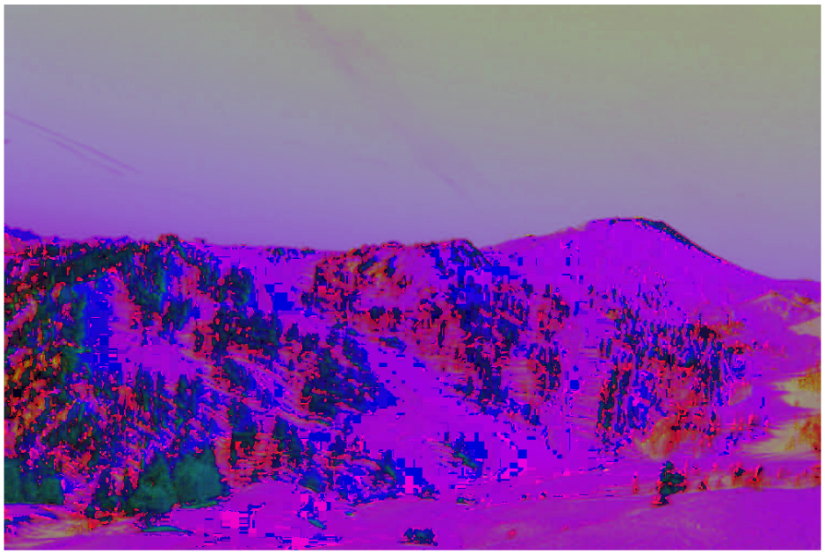
Slika 49: Slučaj 1, HSV analiza

U dugom slučaju, velika razlika naspram okoline se primjećuje u lijevom kutu fotografije , a to označava mogući znak manipulacije *copy paste* tehnikom (slika 50**)**.

Slika 50: Slučaj 2, HSV analiza

U trećem i četvrtom slučaju ne postoji niti jedno područje koje se ističe od okoline pa samim time nema dovoljno znakova koji bi prikazivali znakove manipulacije (slika 51, slika 52).

Slika 51: Slučaj 3, HSV analiza



Slika 52: Slučaj 4, HSV analiza

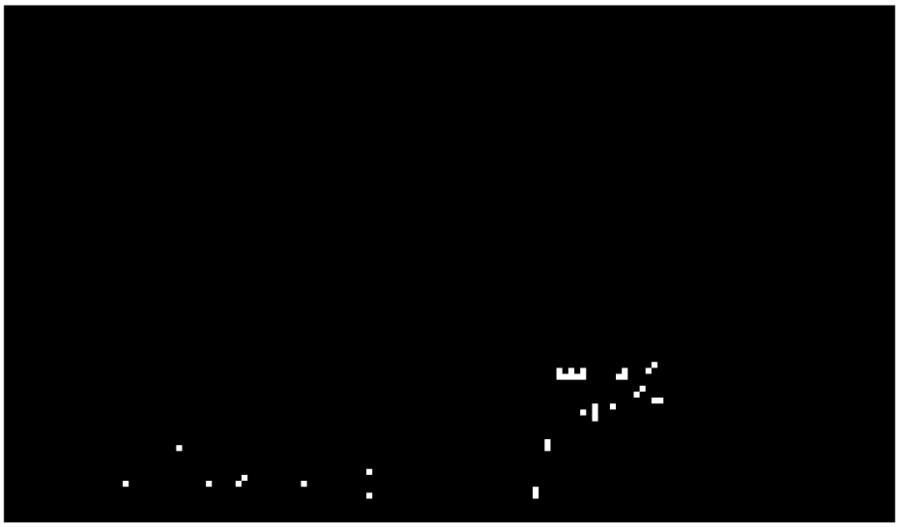
4.2.3 Analiza JPEG blokova

Primjenom ove analize traže se područja fotografije koja se razlikuju u kvaliteti JPEG kompresije. U ovoj analizi potrebno je odrediti prag osjetljivosti prepoznavanja blokova zbog postojanja šuma u fotografiji. Vrijednost praga može biti između 0 i 100, a najbolje je krenuti sa razinom praga 50 pa ovisno o potrebi povećavati ili smanjivati prag za vrijednost 5. Rezultati ove analize prikazani su u tablici 5.

Tablica 5: Rezultati analize JPEG blokova

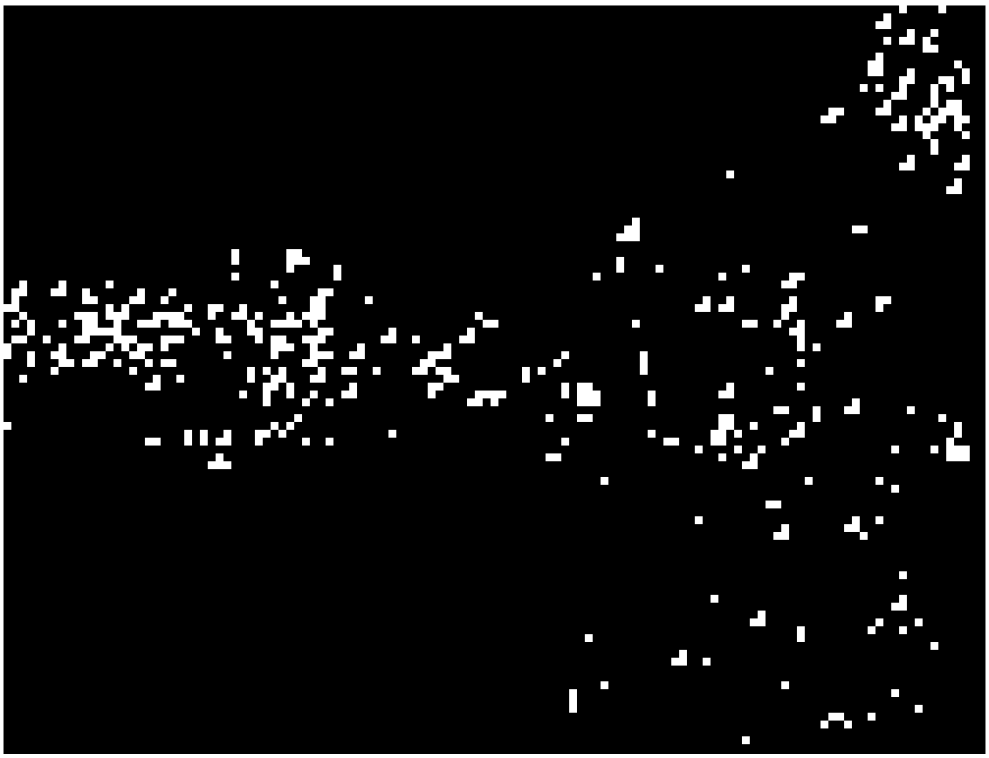
SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1		X	
Slučaj 2			X
Slučaj 3	X		
Slučaj 4	X		

U prvom slučaju postoji vjerovatnost da je fotografija krivotvorena jer su analizom ustanovljena područja koja imaju različitu kvalitetu kompresije (slika 53). U drugom slučaju je HSV analizom utvrđeno postajanje manipuliranog područja, a analiza JPEG blokova samo potvrđuje da je područje u lijevom dijelu slike manipulirano (slika 54). U trećem i četvrtom slučaju ne postoji područje koje se bitno ističe od okolne te nije moguće zaključiti da postoji područje manipulacije (slika 55, 56).



Slika 53: Slučaj 1, rezultat analize JPEG blokova

Slika 54: Slučaj 2, rezultat analize JPEG blokova



Slika 55: Slučaj 3, rezultat analize JPEG blokova

Slika 56: Slučaj 4, rezultat analize JPEG blokova

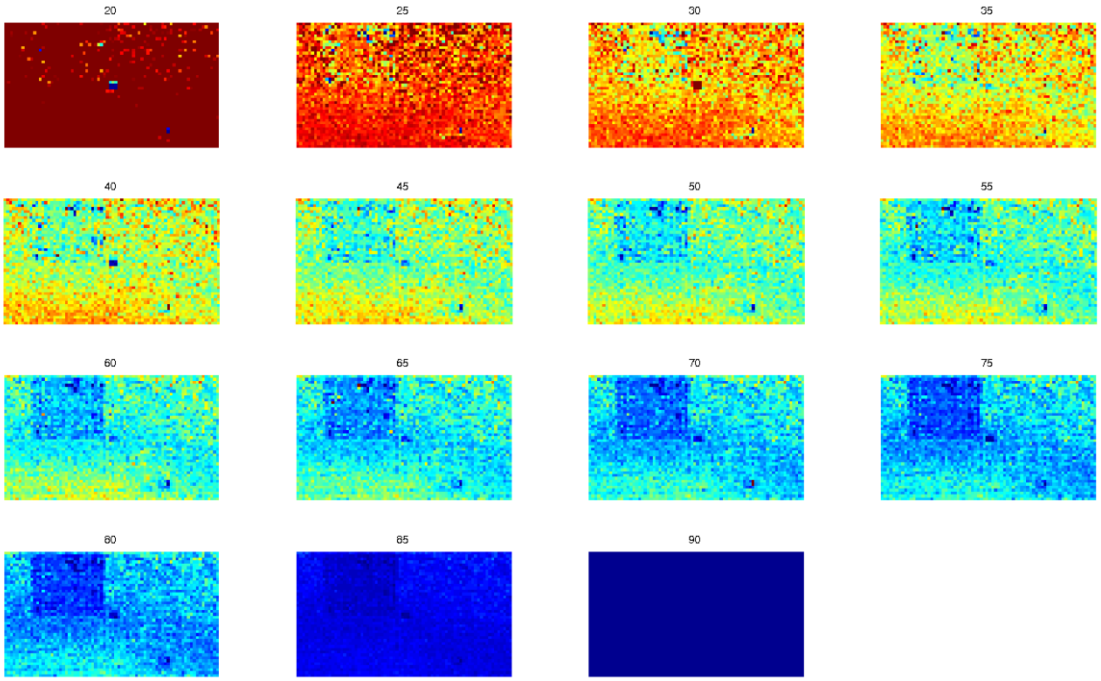
4.2.4 Analiza JPEG duhova

Dupli rubovi ili JPEG duhovi nastaju kod lijepljenja objekata niže kvalitete kompresije na originalnu fotografiju. Ova metoda se pokazala najučinkovitijom u potrazi za manipuliranim područjima. U analiziranju digitalnih fotografija, kod uspoređivanja korišteni su faktori kvalitete od 20 do 90 kako bi se detaljno analizirala fotografija. U *tablici 6* prikazani su dobiveni rezultati.

Tablica 6: Rezultati analize JPEG duhova

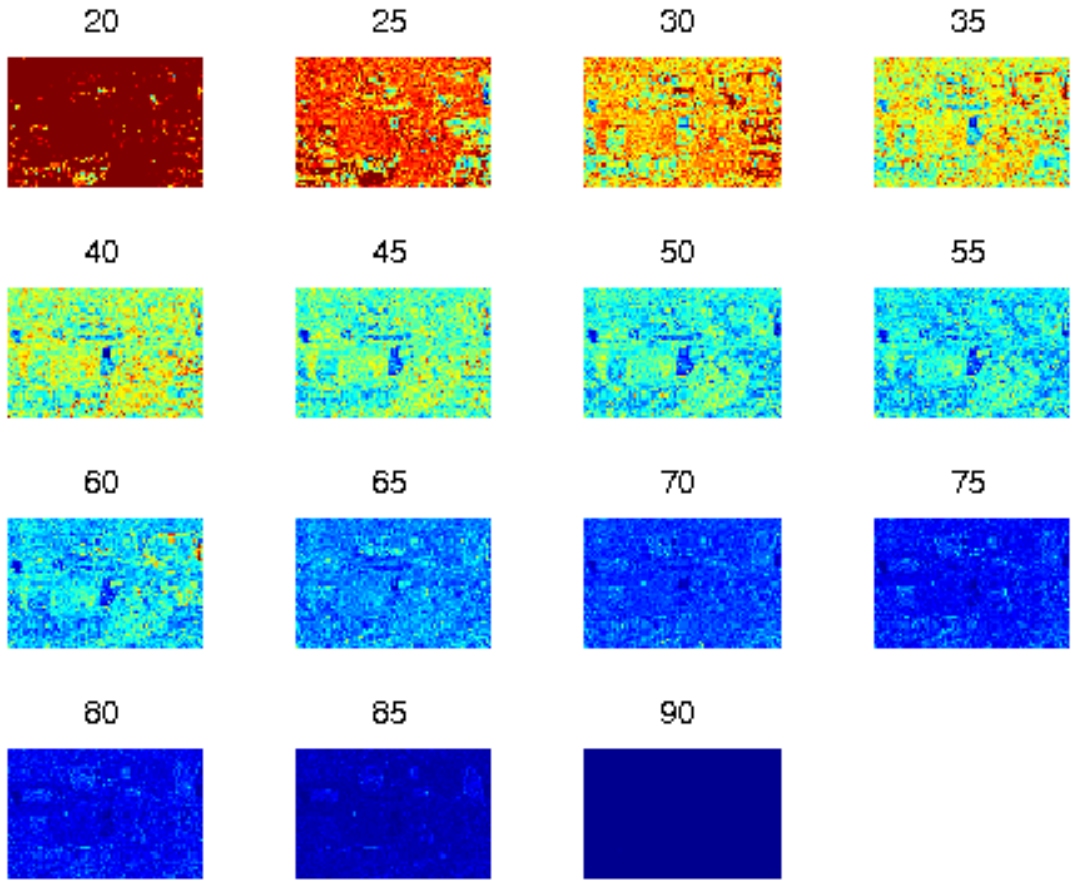
SLUČAJ	**NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM**	**MOGUĆI ZNAKOVI MANIPULACIJE**	**SIGURNI ZNAKOVI MANIPULACIJE**
Slučaj 1			**X**
Slučaj 2			**X**
Slučaj 3			**X**
Slučaj 4	**X**		

U prvom slučaju, na kvaliteti kompresije 50 počinju se uočavati prvi znakovi manipuliranog područja, a najjasnije područje manipulacije se vide kod kvalitete kompresije 75 (slika 57).



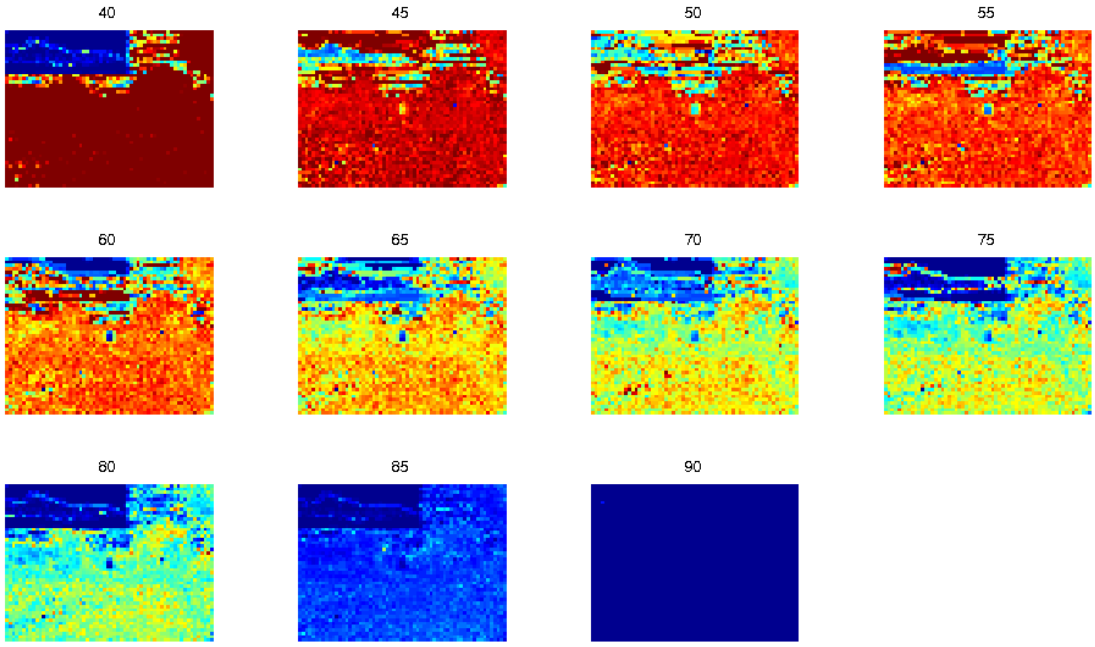
Slika 57: Slučaj 1

U drugom slučaju tragovi JPEG duhova se primjećuju kod faktora kvalitete 40, 45, 50 i 55. Kako su rezultati u prijašnjim analizama pokazali sumnjivo područje na lijevoj strani fotografije ovom analizom dobiva se još čvršći dokaz te opravdanju sumnju da je fotografija manipulirana (slika 58).



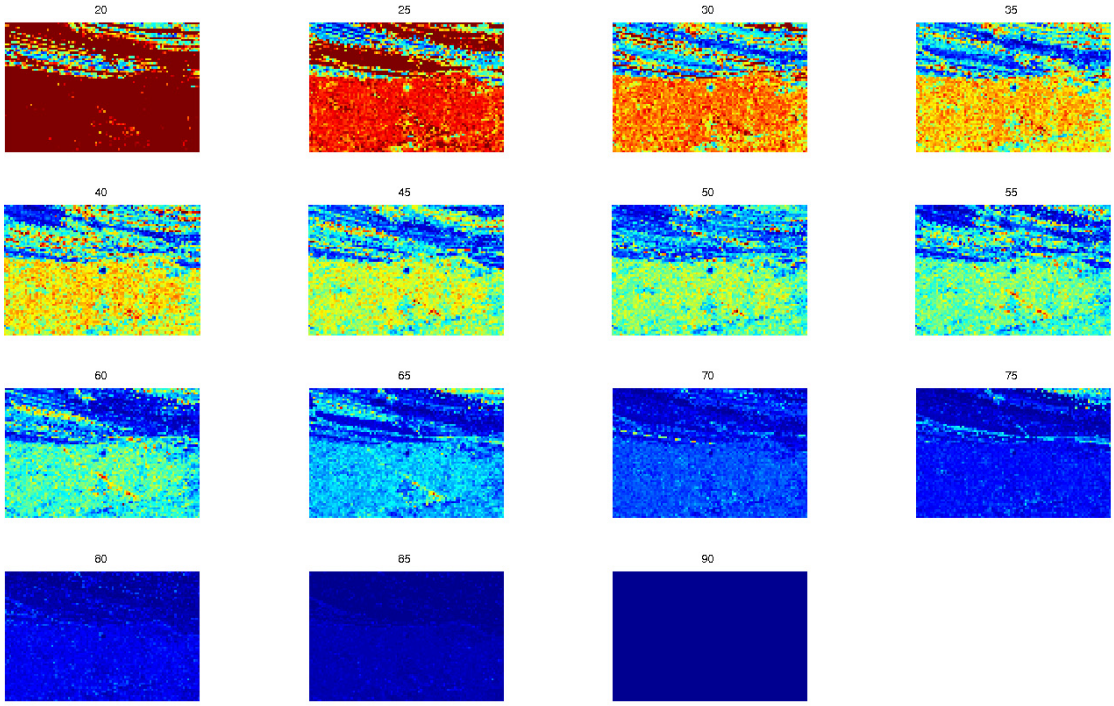
Slika 58: Slučaj 2

U trećem slučaju JPEG duh je uočen u gornjem lijevom kutu, tj. sumnja se da je na originalnu fotografiju naknadno zalijepljen oblak (slika 59). Uz analizu inteziteta svjetla s kojom je postojala mogućnost manipulacije fotografijom u istom području, ovom analizom dobivamo još čvršli dokaz za postojanjem manipulacije. Skoro pri svim nivoma kompresije vidi se sumnjivo područje na digitalnoj fotografiji.



Slika 59: Slučaj 3

U četvrtom slučaju kao i u svim analizama do sada nisu zabilježeni znakovi manipulacije fotografijom (slika 60).



Slika 60: Slučaj 4

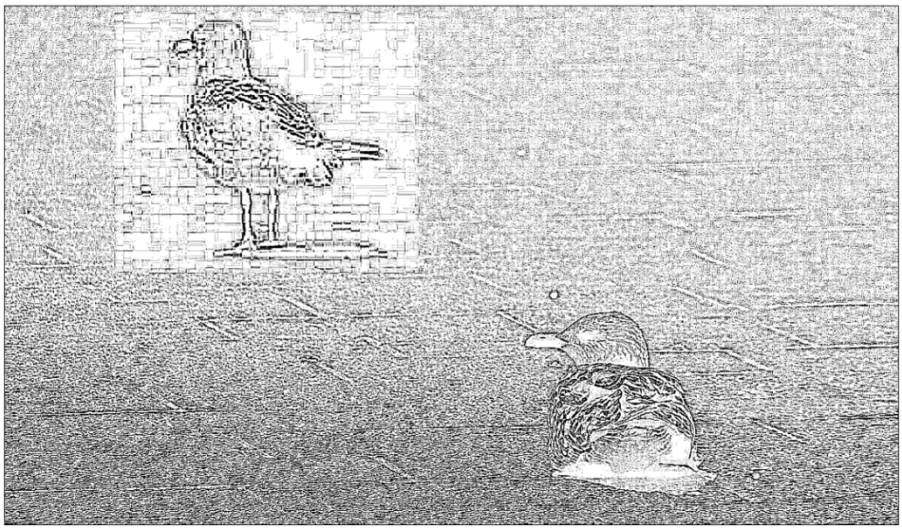
4.2.5 Analiza i detekcija dvostrukih rubova visokopropusnim filterima

Kod dodavanja novih elemenata na postojeću fotografiju dolazi do promjene u statističkim podacima JPEG zapisa. Ovom analizom dobiveni rezultat prikazuje područje manipulacije. Dobiveni rezultat radi lakše interpretacije potrebno je dodatno vizualno obraditi. Rezultati su prikazani u tablici 7.

Tablica 7: Rezultati dobiveni anlizom detekcije rubova

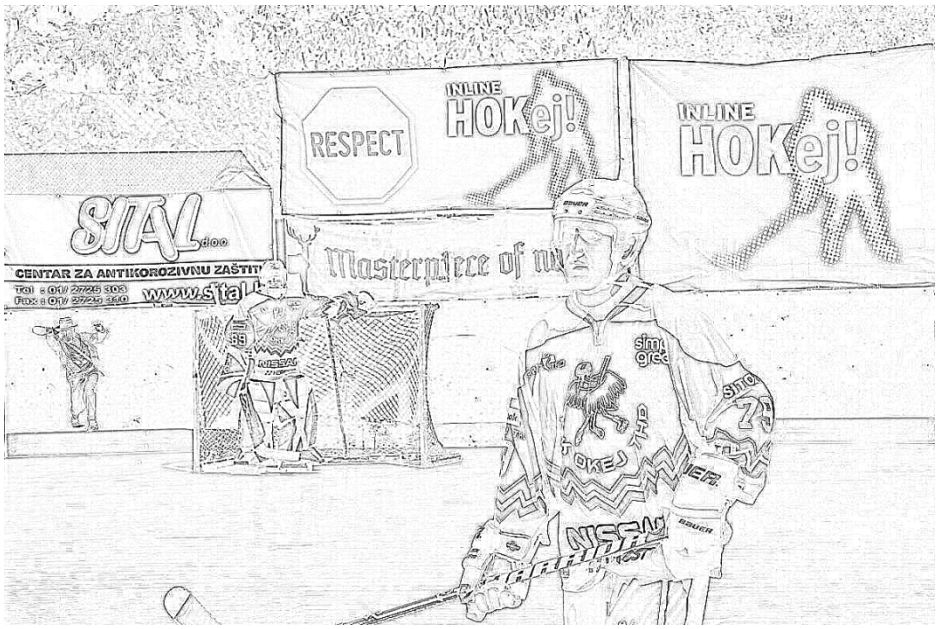
SLUČAJ	**NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM**	**MOGUĆI ZNAKOVI MANIPULACIJE**	**SIGURNI ZNAKOVI MANIPULACIJE**
Slučaj 1			**X**
Slučaj 2		**X**	
Slučaj 3			**X**
Slučaj 4	**X**		

U prvom slučaju nakon obnutog prikaza boja i pojačanja kontrasta jasno se prikazuje razlika i ne konzistentnost digitalne fotografije (slika 61).Dio fotografije je bio pod utjecajem manipulacije *copy paste* tehnikom, te je na originalnu fotografiju dodan sadržaj.



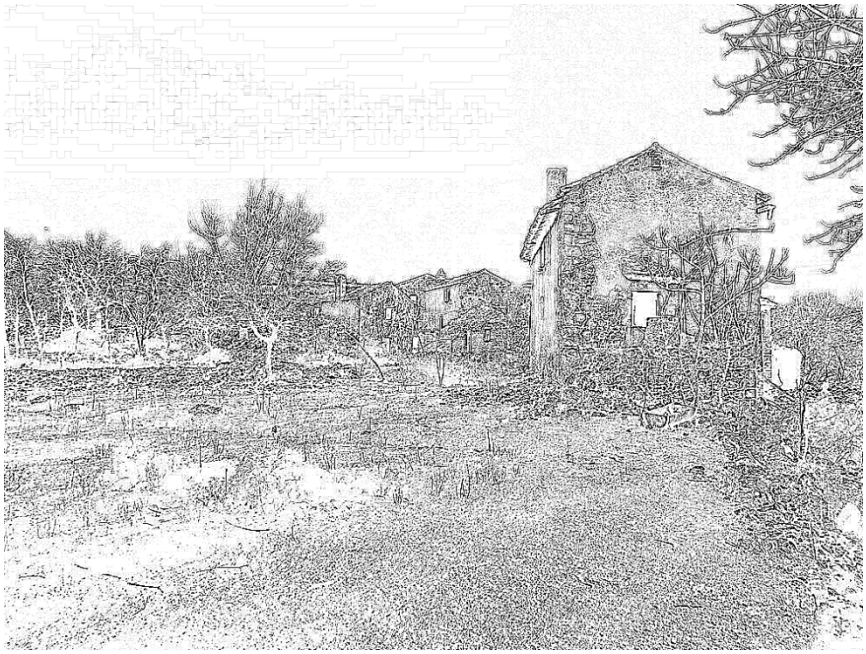
Slika 61: Slučaj 1

U drugo slučaju gdje su ostale tehnike pokazale znakove manipulacije pri velikom povećanju dobivenog rezultata može se vidjeti trag dvostrukih rubova, a time se i ovom tehnikom daje naslutiti da je fotografija manipulirana (slika 62).



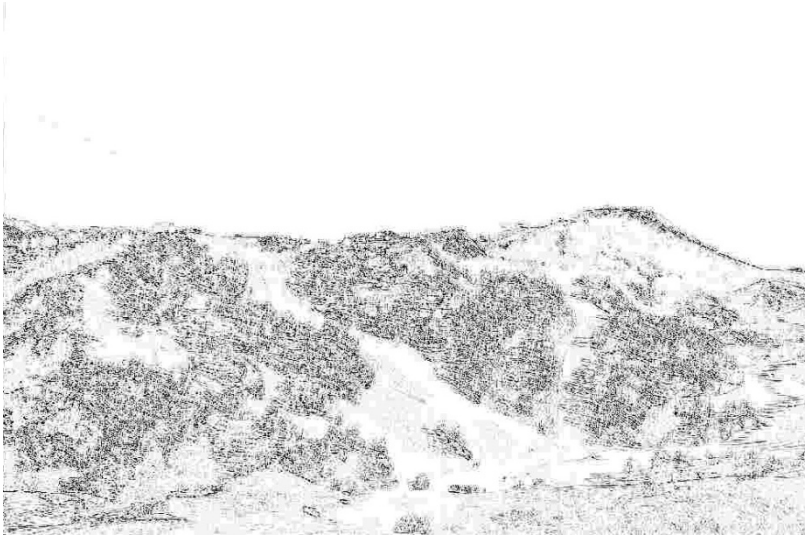
Slika 62: Slučaj 2

U trećem slučaju se primjećuje velika ne konzistentnost podataka u području neba i oblaka što uz ostale dokaze upućuje da je fotografija krivotvorena (slika 63).



Slika 63: Slučaj 3

U četvrtom slučaju niti jednom tehnikom nisu nađeni rezultati manipulacije, a ova analiza ne upućuje na postoje bilo kakvih tragovi manipulacije (slika 64).



Slika 64: Slučaj 4

4.3 Rasprava ukupnih rezultata

Nakon detaljne istrage i primjene predloženog modela, konačni rezultat donosi istražitelj. Primjena tehnika analize iz predloženog modela služe samo kao alat kojim se istražitelju olakšava prikaz određenih informacija o fotografiji, a samim time i donošenje zaključaka. Rezultate istrage ova četiri slučaja prikazana su u tablici 8.

Tablica 8: Konačni rezultati istrage

SLUČAJ	NEDOVOLJNO ZNAKOVA ZA MANIPULACIJOM	MOGUĆI ZNAKOVI MANIPULACIJE	SIGURNI ZNAKOVI MANIPULACIJE
Slučaj 1			**X**
Slučaj 2			**X**
Slučaj 3			**X**
Slučaj 4	**X**		

Model kojim se radila istraga podijeljen je na dva dijela. Zadatak prvog dijela istrage bio je utvrđivanje ispravnosti digitalnog zapisa, a iz EXIF podataka se moglo odlučiti o daljnjem tijeku istrage. Primjeri na kojima se radila analiza nisu koristili napredne tehnike manipulacije pa se struktura zapisa i EXIF podatci nisu mijenjali radi prikrivanja tragova korištenja računalnih aplikacija za digitalnu obradu fotografija. Kod prikrivanja tragova manipulacije u strukturi zapisa potrebno je imati puno znanja i vještine u manipulaciji te poznavati samu strukturu zapisa datoteka.

U drugom dijelu istrage sve tehnike i metode bile su namjenjene traženju naknadno zaljepljenih ili obrisanih elemenata fotografije. Većina manipulacija fotografijom se događa iz razloga što se želi nešto prikriti ili dodati na originalnu scenu pa su zbog toga odabrane tehnike analize koje su sastavni dio predloženog modela. Tehnike intenziteta svjetla i HSV analize spadaju u jednostavne analize zbog jednostavnih i brzih algoritama. U određenim slučajevima primjenom samo tih tehnika analize se može naslutiti moguća manipulacija. U ostalim tehnikama primjenjeni algoritmi su puno kompleksniji, a sama analiza zahtjeva puno više vremena koje se proporcionalno povećava rezoluciji fotografije.

5 ZAKLJUČAK

U ovom radu opisane su i primijenjene tehnike kojima se može provesti forenzička analiza digitalnih zapisa fotografija, s ciljem dokazivanja autentičnosti i integriteta digitalnog zapisa fotografije. Nakon opisa i objašnjavanja tehnika u teoretskom dijelu rada izrađen je model po kojemu se provela analiza strukture zapisa digitalne datoteke i analiza strukture digitalne fotografske slike.

Rezultati primjene predloženog modela i tehnika za analizu i dokazivanje autentičnosti digitalnog zapisa fotografije pokazuju mogućnost uspješne detekcije manipulacija na digitalnim fotografijama. Forenzikom digitalnog zapisa fotografske slike moguće je dokazati autentičnost fotografije i porijeklo njezinog nastanka. Dokazivanje autentičnosti ne ovisi samo o primjenjenim tehnikama za analizu već je veliki faktor u cijelom procesu ispitivanja istražitelj. Istražitelj je osoba koja bi trebala biti jako dobro upoznata s procesom nastanka digitalne fotografije, upoznata s tehnikama analize koje se primjenjuju,sposobna razlučiti dobivene rezultate i donijeti zaključak svakog ispitivanja.

U predloženom modelu za ispitivanje digitalnih fotografija primijenjene su tehnike koje pokrivaju područje strukturne analize digitalne datoteke i strukturne analize same digitalne fotografije. Brzina analize se proporcionalno povećava s rezolucijom digitalne fotografije te se pri izradi ovog modela o tome vodila briga. Cilj je bio izraditi učinkoviti model koji za ukupnu analizu digitalne fotografije ne zahtijeva puno vremena. Pokazalo se da je izrađeni model vrlo učinkovito te daje brzoostvario sva očekivanja u analizi. Ispitivanje se temeljilo na provjeri autentičnosti JPEG zapisa s naglaskom na detekciji*copy paste* tehnike manipulacije. Ova tehnika manipulacije trenutno je najkorištenija metoda manipulacije s vrlo uvjerljivim rezultatom te je uglavnom neprimjetna ljudskom oku.

Strukturnom analizom digitalnog zapisa datoteke istražuje se datoteka u kojoj se nalaze informacije koje predstavljaju digitalni zapis fotografije. Svaka vrsta datoteke ima drugačiju strukturu te informacije pohranjuje na drugačiji način. Provjerom ispravnosti datoteke moguće je ustanoviti da li je struktura zapisa JPEG fotografije ispravna, a time se može doći do zaključka na koji je način nastala digitalna fotografija. Provjerom EXIF zapisa moguće je dobiti prve znakove moguće manipulacije nad digitalnom fotografijom jer računalni programi mogu ostaviti tragove ako su bili u interakciji s ispitivanom fotografijom.

Tehnike primjenjene u strukturnoj analizi digitalnog zapisa fotografije pokazale su se kao vrlo uspješne u potrazi za manipuliranim područjima. Najuspješnija tehnika u potrazi za manipuliranim područjima na digitalnoj fotografiji je*analiza JPEG duhova* koja je u sva tri manipulirana slučaja prepoznala sumnjivo područje dok su ostale tehnike dale naslutiti moguće postojanje manipulacije.

Sistematično ispitivanje digitalnog zapisa fotografije po predloženom modelu je uspješno otkrilo manipulacije na fotografijama.

Ovaj model moguće je proširiti kako bi analiza bila još detaljnija uz primjenu drugih tehnika opisanih u ovom radu. Proširivanjem ovog modela analize treba voditi računa i o vremenu potrebnom za ispitivanje digitalnih fotografija.

6 LITERATURA

[1] Mikota M., (2000). *Kreacija fotografijom*. V.D.T., Zagreb

[2] Hedgecoe J., (2005). *The book of photography*, DK Publishing, London

[3] Anderson S. D., (2011). *Digital Image analysis: analytical framework for authenticating digital images*, Master Thesis, University of Colorado

[4] Lester P., (1991.)*Photojournalism: An ethical approach,* Lawrence Erlbaum Associates, Hillsdale, New Jersey

[5] Connor K. and Farid H., (2011). *Image Authentication and Forensics, dostupno na*: http://www.fourandsix.com/photo-tampering-history/, 23.12.2012.

[6] Brink B., (1998). *News PhotographerQuestion of ethics: Where does honesty in photojournalism begin?,*21–22, 23–33.

[7] Pingdom, *Exploring the software behind Facebook, the world's largest site, dostupno na:* http://royal.pingdom.com/2010/06/18/the-software-behind-facebook/, 23.12.2013

[8] Scientific Working Groups on Digital Evidence and Imaging Technology, "Section 12," Vol. 1.7, No. Technology, Scientific Working Groups on Digital Evidence and Imaging.

[9] Johnson M. K. and FaridH.(2007). *Exposing Digital Forgeries in Complex Lighting Environments*, dostupno na: http://www.mit.edu/%7Ekimo/publications/envmap/tifs07a.pdf, 12.12.2012.

[10] Johnson M. K. and FaridH.*Exposing digital forgeries by detecting inconsistencies in lighting*, dostupno na: http://www.mit.edu/~kimo/publications/lighting/lighting.html,15.11.2012.

[11] ConotterV., BoatoG., FaridH.*Detecting photo manipulation on signs and billboards,* dostupno na: http://livingknowledge.europarchive.org/images/publications/icip10.pdf

[12] Scientific Working Groups on Digital Evidence and Imaging Technology, “Section 16 Best Practices for Forensic Photographic Comparison,” Vol. version 1.

[13] Rogers M. K., SmithJ. M. (2010) *Computer Forensics for the Forensic Audio Professional*, dostupno na: http://www.aes.org/e-lib/browse.cfm?elib=15492, 01.12.2012.

[14] Chisum W. J., TurveyB. E., (2000). *Evidence dynamics: Locard’s exchange principle & crime reconstruction*,*Journal of Behavioral Profiling*, 1.

[15] CaseyE. (2009). *Handbook of Digital Forensics and Investigation*. Elsevier Academic Press, Burlington

[16] Scientific Working Groups on Digital Evidence and Imaging Technology, “SWGDE and SWGIT digital & multimedia evidence glossary,” vol. 0, pp. 1–15.

[17] Ryan D. J., ShpantzerG. (2003).*Legal Aspects of Digital Forensics*

[18] Scientific Working Groups on Digital Evidence and Imaging Technology (2006). *Best practices for computer forensics*, Vol. 1, No. July, 1–11

[19] Lanh T. V., Chong K.S., EmmanuelS., KankanhalliM. S. (2007).*A Survey on Digital Camera Image Forensic Methods*

[20] American academy of forensic sciences bylaws,(2012). dostupno na: http://www.aafs.org/aafs-bylaws#Art2, 23.01.2013.

[21] BaatzW. (1997). *Photography*. Barron’s Educational Series, New York

[22] SiegalJ. A., SaukkoP. J., KnupferG. C. (2000).*Encyclopedia of forensic sciences*. Academic Press , San Diego

[23] CouncilI. T. I. (1986).*Coded character sets - 7-bit american national standard code for information interchange*, Vol. 1986., No. Travanj 1986.

[24] KeeE., JohnsonM. K., FaridH. (2011).*Digital Image Authentication from JPEG Headers*, dostupno na: http://www.cs.dartmouth.edu/~erickee/papers/tifs11.pdf, 15.12.2012.

[25] SturakJ. B. (2011).*Forensic Analysis of digital image tampering*, Master Thesis, Air force Institute of technology

[26] CohenK. (2007).*Digital Still Camera Forensics*, Vol. 1, No. 1, 1–8

[27] KhayamS. A., (2003). *Discrete cosine transform*, dostupno na: http://www.dcd.zju.edu.cn/DCT_Theory%20and%20Application.pdf, 21.11.2012.

[28] WallaceG. K. (1991).*The JPEG Still Picture Compression Standard 2 Background : Requirements and Selection*, dostupno na: http://white.stanford.edu/~brian/psy221/reader/Wallace.JPEG.pdf, 01.12.2012.

[29] FaridH., (2008). *Digital image forensics*,*Scientific American*, Vol. 298, No. 6, Jun. 2008., 66–71

[30] Campbell F. W.,RobsonJ. G., (1968).*Application of fourier analysis to the visibility of gratings*,*The Journal of Physiology*, Vol. 197, 551–566

[31] GallagherA. C., (2005). *Detection of linear and cubic interpolation in JPEG compressed images*, dostupno na: http://chenlab.ece.cornell.edu/, 20.12.2012.

[32] PopescuA. C. (2005).*Exposing digital forgeries by detecting traces of re-sampling*,*IEEE Transactions on Signal Processing*, Vol. 53, No. 2, 758–767

[33] FoveonI. (2012). *X3 Technology*,dostupno na: http://www.foveon.com/article.php?a=69, 21.12.2012.

[34] LukacR., PlataniotisK. N., HatzinakosD., AleksicM. (2006). *A new CFA interpolation framework*,*Signal Processing*, Vol. 86, No. 7, Jul. 2006. 1559–1579

[35] FaridH. (2006). *Digital Image Ballistics from JPEG Quantization*, dostupno na: http://www.ists.dartmouth.edu/library/204.pdf, 22.12.2012.

[36] KornblumJ. D. (2008). *Using JPEG quantization tables to identify imagery processed by software,Digital Investigation*, Vol. 5, Sep. 2008., S21–S25

[37] LuoW., HuangJ., MemberS., (2010).*JPEG Error Analysis and Its Applications to Digital Image Forensics*,*IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 3, 488–491

[38] AlinH. F., Popescu C. (2010).*Statistical Tools for Digital Forensics*, dostupno na: http://citeseerx.ist.psu.edu, 22.12.2012.

[39] StammM. C., TjoaS. K., LinW. S., LiuK. J. (2010), *Anti-forensics of JPEG compression*, dostupno na: http://ieeexplore.ieee.org, 23.12.2012.

[40] LaiS., BöhmeR. (2011).*Countering counter-forensics: The case of JPEG compression*,*dostupno na: http://is.uni-muenster.de/, 23.12.2012.*

[41] FridrichJ., SoukalD., J. Lukáš, (2003). *Detection of Copy-Move Forgery in Digital Images*, dostupno na: http://ws2.binghamton.edu/fridrich/Research/copymove.pdf, 23.12.2012.

[42] Reininger R. C.,GibsonJ. D., (1983). *Distributions of the two-dimensional DCT coefficients for images*,*IEEE Transactions on communications*, Vol. 31, No. 6, 835–839.

[43] FaridH., (2009). *Exposing digital forgeries from JPEG ghosts*,*IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 1, 154–160.

[44] KhannaN., MikkilineniA. K., ChiuG. T. C., DelpE. J., (2009). Forensic camera classification: Verification of sensor pattern noise approach, dostupno na: http://https://engineering.purdue.edu/~prints/, 23.12.2012.

[45] AllesE. J., GeradtsZ. J., Veenman C. J. (2009). *Source camera identification for heavily compressed low resolution still images*, *Journal of Forensic Sciences*, Vol. 54, No. 3, 628–638.

[46] ChenM., FridrichJ., LukasJ., GoljanM., (2007). *Imaging sensor noise as digital x-ray for revealing forgeries*, dostupno na: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.85.928, 24.12.2012.

[47] ChierchiaG., ParrilliS., Poggi G., SansoneC., VerdolivaL. (2010). *On the Influence of Denoising in PRNU based Forgery Detection*, dostupno na: http://dl.acm.org/citation.cfm?id=1878002, 24.12.2012.

[48] LukasJ., FridrichJ., Goljan M. (2006).*Digital camera identification from sensor pattern noise*,*IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, 205–215.

[49] JenkinsN., (2009). *Digital Camera Identification*, dostupno na: http://www.cl.cam.ac.uk/teaching/, 26.12.2012.

[50] FridrichJ.(2009). Digital image forensics,*IEEE Signal Processing Magazine*, Vol. 26, No. 2, 26–37.

[51] SachsJ., (1996). *Digital Image Basics*, dostupno na: http://www.dl-c.com/basics.pdf, 28.12.2012.

[52] Lukas J. (2000). *Digital Image Authentication Using Image Filtering Techniques,* dostupno na: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.26.3997, 29.12.2012.

[53] L. C. M. (2012). *Introduction to Computer Vision and Image Processing,* dostupno na: http://homepages.inf.ed.ac.uk/rbf/CVonline/, 29.12.2012.

[54] BaxesG. A. (1994). *Digital Image Processing*, John Wiley & Sons, New York