

## ULOGA DIGITALNE FORENZIKE U DETEKCIJI COPY-MOVE NAPADA NA SLIKU THE ROLE OF DIGITAL FORENSICS IN COPY-MOVE IMAGE FORGERY DETECTION

Ranko Petrović

**REZIME:** Otkrivanje i dokazivanje zloupotreba informacione tehnologije postalo je jedno od ključnih pitanja današnjice, kako zbog posledica koje izaziva društvenoj zajednici, tako i zbog činjenice da su tradicionalne forenzičke metode i alati postali primitivni i neefikasni za upotrebu u informacionom ambijentu. Iako u opštem slučaju manipulacija nad slikom možda i nije ekskluzivni fenomen u svetu nauke, kritičari su izrazili zabrinutost jer nikada nije bilo tako lako omogućeno menjanje sadržaja i značenja slika, i to često do takvog savršenstva da je nemoguće vizuelno razlikovati falsifikat od autentičnih fotografija. Rad se bavi aktuelnim problemom copy-move manipulacije nad digitalnom slikom koja omogućava prikrivanje nekih značajnih i korisnih informacija u slici. Cilj rada je da se na osnovu pregleda i poređenja postojećih algoritama detekcije copy-move napada na sliku, koji se međusobno razlikuju po efikasnosti, složenosti i otpornosti na različite postobradne operacije, predloži najefikasnije ili potpuno novo rešenje koje je moguće softverski implementirati.

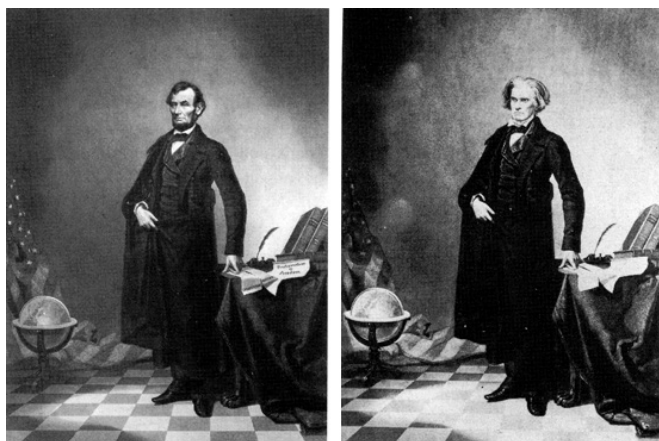
**KLJUČNE REČI:** digitalna slika, copy-move manipulacija, digitalna forenzika

**ABSTRACT:** Detecting and proving abuse of information technology has become one of the crucial issues of our time because of the consequences caused to the community, and the fact that traditional forensic methods and tools have become primitive and inefficient for use in the information environment. Although, in general, the manipulation of the image is not an exclusive phenomenon in the world of science, critics are concerned about the fact that it has never been so easy to modify the content and meaning of an image, often to such perfection that it is impossible to visually distinguish fake from authentic image. This paper presents current problem of copy-move forgery technique that allows concealing some important and useful information in the image. The purpose of this paper is to provide the survey of existing algorithms for copy-move forgery detection and to compare them in efficiency, complexity and resistance to different post-processing operations in order to propose the most efficient solution.

**KEY WORDS:** digital image, copy-move forgery, digital forensics

### 1. UVOD

Fotografija je svoju nevinost izgubila pre mnogo godina. Samo nekoliko decenija nakon što je snimljena prva 1814. godine, nad fotografijama su vršene raznorazne manipulacije. Tako je primenom određenih tehnika manipulacije još davne 1860. godine nastao čuveni portret američkog predsednika Abraham Linkolna koji u suštini predstavlja fuziju njegove glave i tela jednog drugog, lokalnog, političara, kao što se može i videti na **slici 1**[1].



**Slika 1.** Prva registrovana (poznata) manipulacija izvršena nad slikom [2]

Poslednjih godina, falsifikovanje slika ima značajan uticaj na nauku, pravo, politiku, medije i biznis. Neki slučajevi mogu dovesti čak i do nacionalnih i međunarodnih problema. Danas, više nego ikad ljudi su shvatili da ne mogu uvek i tek tako da prihvate fotografiju samo kao neku vrednost odštampanu na papiru jer se često dešava da slika sadrži mnogo više nego što naše oko može da primeti. Zahvaljujući digitalnim kamerama visoke rezolucije, moćnim kompjuterima kao i sofisticiranim softverima za obradu slike, manipulacije na slici su postale prostije i teže uočljivije. Zato danas postoji jasna potreba za razvojem forenzičkih algoritama za detektovanje manipulacija nad slikom kako bi se povratilo opšte poverenje u digitalnu fotografiju [1].

Među velikim brojem vrsta tehnika manipulacije posebno interesovanje izaziva **copy-move manipulacija** ili takozvano **kloniranje**, koja je ujedno i najčešći vid manipulacije nad slikom i spada u grupu tehnika takozvane slepe forenzike čiji je cilj da ispita autentičnost slike bez pomoći ugrađenih bezbednosnih šema kao što je na primer vodeni žig. Ona podrazumeva kopiranje dela originalne slike na neki drugi deo te iste slike sa ciljem da se ili prikriju određeni detalji ili da se neki drugi detalji originalne slike naglase [3]. Jedan od poznatijih primera jeste slika testiranja iranskih raketa iz 2008. godine koju su objavili mediji povezani sa iranskom vojskom, želeći da prikriju neuspešno lansiranje jedne od raketa koje se jasno vidi na originalnoj slici[4, 5].

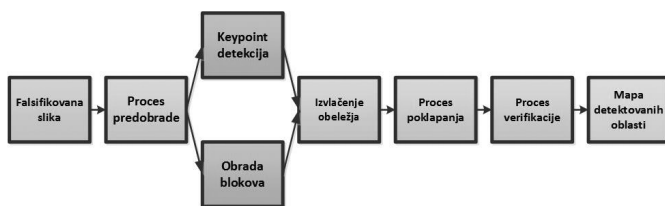


Slika 2. Primer copy-move manipulacije nad slikom pri kojoj je izvršeno kloniranje jedne od raketa[6]

Za razliku od vodenog žiga alati forenzike pretpostavljaju da svaka slika poseduje određene pravilnosti koje bivaju narušene ukoliko je nad njom izvršena određena manipulacija. Te pravilnosti mogu poticati iz različitih izvora, uključujući prirodno okruženje, kameru i naravno samu sliku [1]. Tako, bilo koja copy-move manipulacija uvodi korelaciju između originalnog segmenta slike i segmenta koji je kopiran. Ta korelacija predstavlja osnovu od koje je potrebno započeti istraživanje radi uspešne detekcije ove vrste manipulacije nad slikom. Kako će obrađena slika, odnosno falsifikat, najčešće biti sačuvan u JPEG formatu, formatu kompresije koji podrazumeva gubitke, i kako postoji mogućnost da nad njom naknadno bude primenjeno retuširanje ili neka druga tehnika za obradu slike na onom delu koji je modifikovan, originalni i kopirani segment neće biti potpuno identični, već će se aproksimativno poklapati. Ali može se zaključiti da pošto kopirani deo potiče iz iste, originalne slike, karakteristike kao što su paleta boja, tekstura, komponenta šuma, osvetljenje i mnoge druge biće kompatibilne sa ostatkom slike [7, 8].

## 2. OPŠTI ALGORITAM DETEKCIJE COPY-MOVE NAPADA NA SLIKU

Danas postoji veliki broj različitih algoritama za detekciju copy-move manipulacije (eng. Copy-Move Forgery Detection, CMFD) nad slikom koji se međusobno razlikuju u brzini, efikasnosti i otpornosti algoritma. Tokom poslednjih godina istraživanja su usmerena da se napravi potpuno automatski sistem za detekciju ove vrste falsifikovanja slike. Uprkos tom širokom spektru algoritama najveći broj njih u procesu detekcije prolazi kroz iste faze kao što je i prikazano na slici 3 [8].



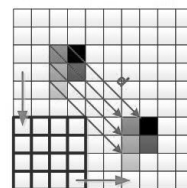
Slika 3. Opšti algoritam detekcije copy-move manipulacije [9]

Prvo se nad slikom vrši određena **predobrada** da bi se ona u potpunosti spremila za pretragu dupliranih regiona. Prebacivanje slike u boji u sliku na skali sivog (eng. grayscale), predstavlja tipičan primer predobrade.

Na osnovu detalja koji se mogu otkriti, kao i na osnovu načina pristupa kada je proces detekcije u pitanju razlikujemo dva tipa detekcije, detekciju koja se zasniva na obradi blokova slike i *keypoint* detekciju.

**Detekcija zasnovana na blokovima** podrazumeva podelu slike na pravougaone regione kao što je prikazano na slici 4. Za svaki taj region računa se vektor obeležja koji se naknadno upoređuju sa ciljem da se nađu slični. U prepoznavanju oblika, **vektor obeležja** (eng. **feature vector**) je n-dimenzionalni vektor numerički predstavljenih osobina posmatranog objekta.

Grayscale slika sa originalnim objektom i njegovom kopijom



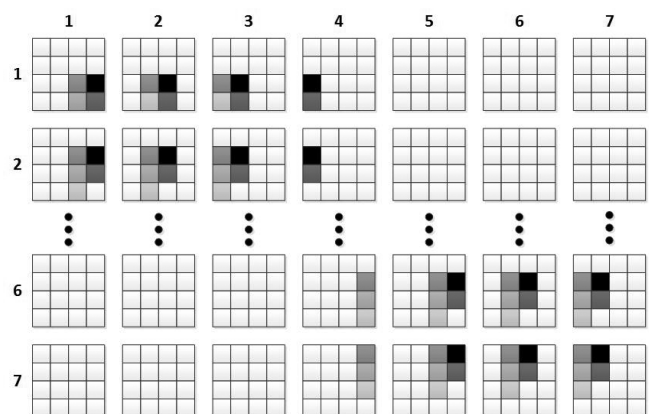
$N \times N$  - ukupan broj piksela slike

$b \times b$  - ukupan broj piksela maske

$(N-b+1)^2$  - ukupan broj pozicija maske

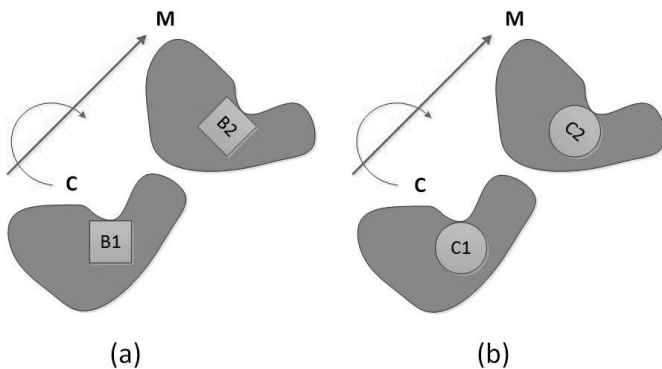
$d$  - rastojanje između originalnog i kopiranog bloka

Prvih 14 i poslednjih 14 pozicija maske u slici



Slika 4. Izdvajanje preklapajućih blokova na koje je slika podeljena

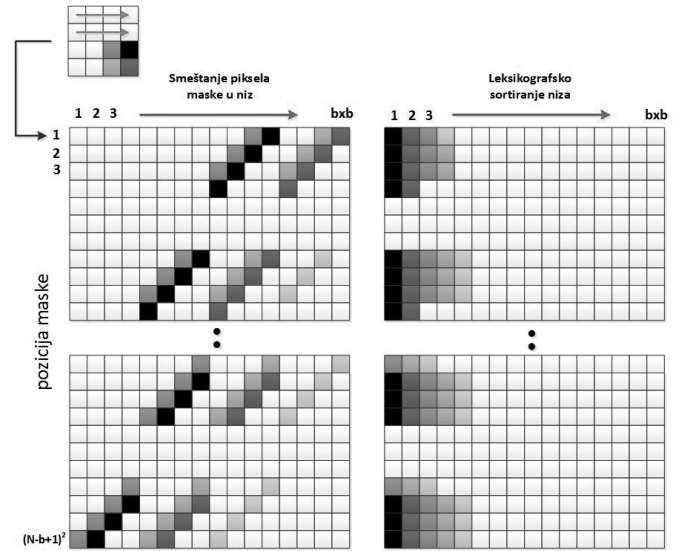
Međutim kada je kopirani region rotiran upotreba kvadratnog bloka neće doneti značajne rezultate kao što je i prikazano na slici 5. Zato se u nekim algoritmima kvadratni blokovi zamjenjuju kružnim blokovima koji omogućavaju da se prevaziđe problem rotacije. Slika se deli na mnogo preklapajućih kružnih blokova, a zatim se iz svakog bloka izdvaja vektor obeležja koji se posle koristi za međusobno poređenje blokova. Međutim treba imati u vidu da korišćenjem kružnih blokova i na taj način odbacivanjem svih piksela koji nisu obuhvaćeni datim krugom može doći do pojave lažnog alarma u algoritmu detekcije [10, 11].



Slika 5. Model dupliranog regiona koji je rotiran i šiftovan sa (a) kvadratnim blokom (b) kružnim blokom [10]

Nasuprot metodi zasnovanoj na blokovima **keypoint detekcija** uzima u obzir karakteristike samo onih regiona koje odlikuje visoka entropija koja u obradi slike predstavlja statističku meru slučajnosti koja može da se koristi na primer za kategorizaciju tekstone ulazne slike, i to bez ikakve prethodne podele slike.

Uloga **procesu poklapanja** je, ako postoji, da ukaže na visok stepen sličnosti između karakteristika dva ili više deskriptora što se tumači kao znak da je jedan od regiona slike kopiran. Što se tiče metode zasnovane na blokovima, za uparivanje sličnih vektora najčešće se koristi takozvano **leksikografsko sortiranje matrice** u kojoj svaki red predstavlja jedan vektor karakteristika kao što je prikazano na slici 6. Nakon ovakvog sortiranja najbliži vektori karakteristika će se javiti u uzastopnim redovima matrice, što znači da se odlučivanje vrši na nivou susednih vektora. Pored leksikografskog postoje i neke druge metode sortiranja koje se koriste. Keypoint metoda detekcije podrazumeva korišćenje takozvanog **kd-stabla** koje predstavlja strukturu podataka koja deli prostor i organizuje tačke u K-dimenzionalnom prostoru i vrlo je korisno u postupcima pretraživanja jer omogućava relativno efikasnu i direktnu pretragu najbližeg susedstva. Rezultati su pokazali da algoritam poklapanja kd-stablom daje bolje rezultate od leksikografskog sortiranja, ali sa druge strane je i znatno zahtevnije u pogledu memorijskog prostora.



Slika 6. Leksikografsko sortiranje vektora obeležja

**Proces verifikacije** podrazumeva u suštini proces filtriranja kako bi se odstranila lažna poklapanja. Susedni pikseli najčešće imaju veoma slične intenzitete što može dovesti do pojave netačnih rezultata, što se često dešava u slučajevima postojanja velikih uniformnih oblasti u slici kao što su nebo, trava, voda, pesak. Jedan od načina da se eliminišu takve pojave je korišćenje različitih kriterijuma rastojanja, a jedno od njih je i **Euklidovo rastojanje** (eng. **Euclidian distance**). Dva vektora obeležja, tj. dva susedna bloka  $(\sqrt{b} \times \sqrt{b})$  iz sortirane matrice, mogu se smatrati dupliranim ako su dovoljno slični tj. ako zadovoljavaju prag sličnosti  $T_1$  i ako je njihovo Euklidovo rastojanje veće od unapred određenog praga  $T_2$  [8, 12, 13]:

$$\sum_{x_1=1}^{\sqrt{b}} \sum_{y_1=1}^{\sqrt{b}} |B_1(x_1, y_1) - B_2(x_1 + \Delta x, y_1 + \Delta y)| \leq T_1$$

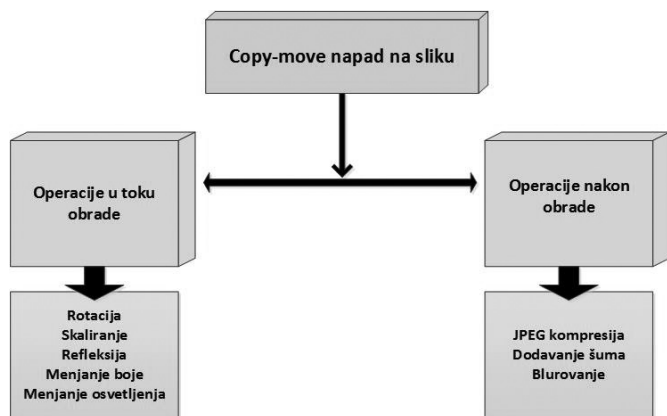
$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} > T_2$$

Takođe, jedan od načina detekcije dupliranih blokova je i da se ispita korelaciona funkcija koeficijentata odgovarajućih vektora obeležja.

Konačni rezultati algoritma detekcije mogu se prikazati konstrukcijom **mape sa dupliranim regijama**. Formira se slika, veličine originalne slike, čije su vrednosti piksela jednake nuli (crna slika). Zatim se pikselima koji pripadaju detektovanim dupliranim regionima dodeljuje jedinstvena vrednost nijanse sive. Radi boljeg i jasnijeg prikaza nad mapom dupliranih regija se vrše određene operacije iz obrade slike. Tu se pre svega misli na **morfološke operacije** kao što je dilatacija praćena erozijom sa ciljem da se eliminišu eventualne rupe u dupliranim regionima, a zatim i obrnut proces, erozija praćena dilatacijom kako bi se eliminisali lažni parovi dupliranih blokova. U ovim procesima se najčešće koristi strukturni element u obliku diska prečnika od 20 piksela [8, 14, 12].



Međutim, sam proces falsifikovanja može da podrazumeva i mnogo više od jednostavnog dupliranja. Operacije koje se u tom slučaju primenjuju mogu dodatno da zakomplikuju stvar i mogu se podeliti u dve grupe: operacije u toku obrade (eng. intermediate processing operations) i operacije nakon obrade (eng. post-processing operations). **Operacije u toku obrade** se koriste sa ciljem da se obezbedi neka vrsta prostorne sinhronizacije i homogenosti između kopiranog regiona i njegovog susedstva. Ovu grupu operacija čine rotacija, skaliranje, odraz u ogledalu, modifikovanje osvetljenja, modifikovanje boje. Ove operacije se mogu koristiti nezavisno ili u kombinaciji. **Operacije nakon obrade** se koriste sa ciljem uklanjanja svih vidljivih tragova koje je za sobom ostavila copy-move manipulacija, kao što je na primer postojanje oštrih ivica. U ovu grupu spadaju dodavanje šuma, JPEG kompresija, kao i operacija blurovanja, tačnije zamućivanja delova slike [8].



Slika 7. Operacije nad slikom koje otežavaju detekciju copy-move manipulacije

Na osnovu svega do sada rečenog mogu se definisati opšti i minimalni uslovi koje bi algoritam detekcije ove vrste manipulacije trebalo da ispunjava kako bi se smatrao uspešnim [15]:

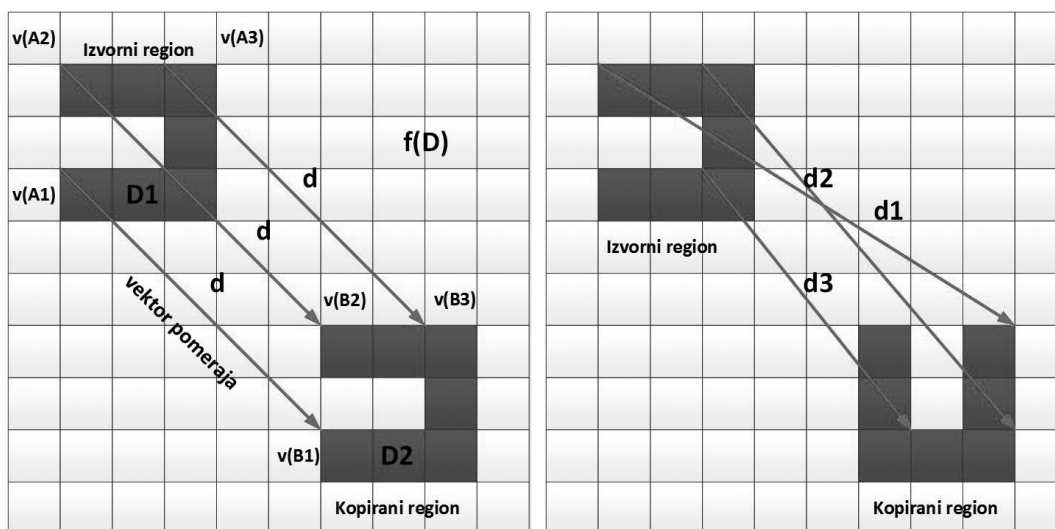
1. Algoritam detekcije mora biti osetljiv na aproksimativno poklapanje malih segmenata slike.
2. Algoritam treba da radi sa pretpostavkom da će falsifikovani segment pre biti jedna cela povezana oblast nego neko malo parče ili čak individualan piksel.
3. Algoritam treba da bude efikasan i da za što kraće vreme izvrši detekciju uz moguće pronalaženje lažnih segmenata odnosno segmenata koji nisu falsifikovani a koje je algoritam usled svojih nedostataka ipak detektovao.

Ključna stvar na kojoj se zasnivaju svi algoritmi za detekovanje copy-move manipulacije nad slikom je činjenica da izvorni region i njegova tražena kopija potiču iz iste slike. Time se očekuje da osobine izvornog i kopiranog regiona, kao što su temperatura boje, uslovi osvetljenja i šum, budu veoma slične [12].

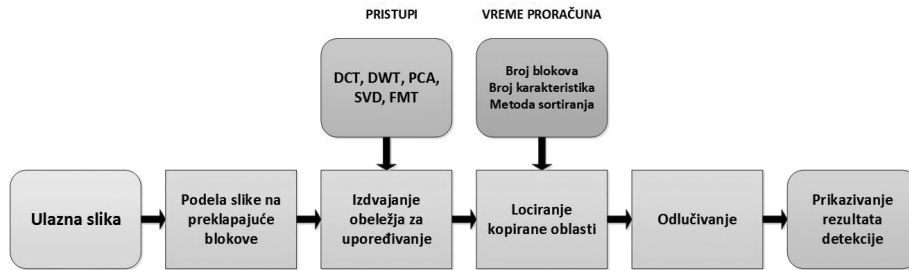
### 3. ALGORITMI ZASNOVANI NA POREĐENJU BLOKOVA

U prirodi copy-move manipulacije je da u falsifikovanoj slici postoje najmanje dva slična regiona, što je kao pojava u većini prirodnih, nemodifikovanih slika, teško ostvarivo. Jedna analiza 100 različitih prirodnih slika je pokazala da je malo verovatno da unutar jedne slike budu dva slična regiona, a da njihova veličina bude veća od 0,85% od veličine slike [16].

Ako je originalna slika označena sa  $f(x,y)$ , onda je modifikovana slika označena sa  $f'(x,y)$  i mora da važi:  $\exists$  regioni  $D_1$  i  $D_2$  koji su podskupovi  $D$  i vektor pomeraja  $d=(dx,dy)$ , (pretpostavimo da  $|D_1|=|D_2|>|D|*0.85\%$  i  $|d|>L$ ),  $f'(x,y)=f(x,y)$  ako  $(x,y)\notin D_2$  i  $f'(x,y)=f(x-dx,y-dy)$  ako  $(x,y)\in D_2$ , gde je  $D_1$  originalan region, a  $D_2$  region koji je kopiran,  $D_2=D_1+d$  [16]. Kao što je ranije rečeno da bi falsifikovana slika bila teža za otkrivanje, na  $f'(x,y)$  mogu biti primenjeni različiti procesi, tako da slika nad kojom je izvršena manipulacija postaje  $f''(x,y) = \Theta(f'(x,y))$  gde  $\Theta$  operator toga procesa kao što su na primer JPEG kompresija, skaliranje, rotacija. Primer rotacije je prikazan na slici 8 [14].



Slika 8. Model dupliranog regiona bez rotiranja (a) i sa rotiranjem (b)



Slika 9. Algoritam detekcije na bazi preklapajućih blokova [18, 19]

Glavna ideja ove tehnike je da je bolje podeliti sliku na male preklapajuće ili nepreklapajuće blokove i onda izvršiti pretragu na nivou tih blokova umesto da se pokušava sa identifikacijom dupliranog regiona u celini. Blokovi se međusobno upoređuju sa ciljem da se utvrdi koji se blokovi poklapaju. Regioni ili oblasti slike koji su prekriveni takvim blokovima se označavaju kao kopirani regioni [17].

Na slici 9 je prikazan tipičan algoritam koji opisuje sve faze koje obuhvata proces detekcije copy-move manipulacije koja se zasniva na upoređivanju blokova na koje je slika podeljena [20]:

1. **Preklapajući blokovi (eng. Overlapping Blocks)** – prvi korak podrazumeva podelu slike na preklapajuće blokove veličine  $b \times b$  piksela.
2. **Izdvajanje obeležja (eng. Feature Extraction)** – Karakteristika bloka se definiše kao funkcija jednog ili više merenja koja predstavljaju neke kvantitativne osobine bloka. Rezultat ovog koraka je matrica vektora. Svaki red ove matrice ustvari predstavlja vektor obeležja jednog bloka.
3. **Poklapanje blokova (eng. Block Matching)** – Svi elementi u matrici sa vektorima obeležja se moraju sortirati sa ciljem da bi se pronašli slični blokovi.
4. **Odlučivanje (eng. Forgery Decision)** – Kao što je već rečeno neće uvek svi blokovi koji se poklapaju i koji su sortiranjem upareni, biti i oni koji pripadaju samo jednom kopiranom regionu. Kako duplirani region može u svom sastavu da ima veoma veliki broj blokova koji se poklapaju, cilj poslednjeg koraka u procesu detekcije jeste da se pronađe tačan broj dupliranih blokova. Za blokove koji se poklapaju, a koji se nalaze unutar jednog dupliranog regiona je karakteristično da imaju isto rastojanje. Ako su poklapajući blokovi međusobno povezani i imaju isto rastojanje, onda oni sigurno pripadaju regionima istog oblika.

Algoritmi detekcije copy-move manipulacije koji se zasnivaju na upoređivanju blokova se najviše međusobno razlikuju po vektoru obeležja koji koriste za poređenje blokova [21]. Skoro svaki pristup ovakvih detekcija podrazumeva deljenje slike na preklapajuće blokove i to upotrebom klizećeg prozora fiksne veličine koji se kreće po celoj slici. Svaki od ovih blokova je predstavljen **vektorom obeležja (eng. feature vector)**. Na osnovu karakteristika vektora obeležja svi algoritmi koji pripadaju ovoj vrsti detekcije se mogu podeliti u četiri grupe [12]:

1. Algoritmi kod kojih se obeležja zasnivaju na redukciji dimenzija (eng. dimensionality reduction-based)
2. Algoritmi kod kojih se obeležja zasnivaju na frekvenciji (eng. frequency-based)
3. Algoritmi kod kojih se obeležja zasnivaju na momentu slike (eng. moment-based)
4. Algoritmi kod kojih se obeležja zasnivaju na teksturi i intenzitetu (eng. texture and intensity-based)

### 3.1. ALGORITMI ZASNOVANI NA REDUKCIJI DIMEZNIJA

Ovoj grupi pripadaju algoritmi koji između ostalog omogućavaju i smanjenje veličine vektora karakteristika koji se izvlače iz blokova slike [08]. Tu spadaju: **analiza glavnih komponenti** (eng. Principal Components Analysis, PCA), **Kernelova analiza glavnih komponenti** (eng. Kernel Principal Components Analysis, KPCA) i **dekompozicija singularnih vrednosti** (eng. Singular Values of Decomposition, SVD) [12].

**Analiza glavnih komponenti** predstavlja jednu od najjednostavnijih multivarijantnih tehnika i ona se primenjuje na male blokove slike fiksne veličine da bi se dobila dimenzionalno smanjena reprezentacija vektora karakteristika koji su pri tom i veoma otporni na manje varijacije u slici koje nastaju kako dodavanjem šuma tako i upotrebom kompresije sa gubicima. Ova tehnika se koristi kada je veliki broj promenljivih u skupu redundantan, odnosno kada se više promenljivih odnosi na istu dimenziju i kada ne pružaju nikakvu dodatnu informaciju koja već nije obuhvaćena nekom drugom promenljivom. Dakle, analiza glavnih komponenti je statistička procedura koja koristi ortogonalnu transformaciju kako bi konvertovala skup potencijalno korelisanih promenljivih u skup vrednosti linerano nekorelisanih promenljivih, koje se nazivaju glavne komponente i pomocu kojih se predstavljaju blokovi slike [11, 14].

**Kernel analiza glavnih komponenti** predstavlja modifikovanu verziju analize glavnih komponenti koja mapira originalne ulaze u velikodimenzionalan prostor karakteristika pomoću kernel metoda. Kernel metode (eng. Kernel Methods) predstavljaju klasu algoritama koji se koristi za analizu i prepoznavanje oblika. Matematički gledano KPCA podrazumeva transformaciju trenutnih karakteristika u velikodimenzionalan prostor u kojem se računaju svojstveni vektori. Pri tome se ignorišu svi oni vektori sa malim svojstvenim vrednostima [22].

Tehnika zasnovana na **dekompoziciji singularnih vrednosti** se primenjuje na svaki blok slike sa ciljem smanjenja dimenzija vektora obeležja pri čemu je svaki blok predstavljen pomoću takozvanog SV-vektora. Vektor singularnih vrednosti ili SV-vektor je jedinstvena i stabilna reprezentacija bloka. Optimalna je za datu sliku u smislu da je energija koja je upakovana u datom broju transformacionih koeficijenata znatno uvećana [23]. Singularne vrednosti koje formiraju stabilan prikaz blokova slike su jedinstvene za matricu. Kroz veliki broj eksperimenata utvrđeno je da je samo nekoliko velikih singularnih vrednosti dominantno u većini prirodnih slika, dok su ostale singularne vrednosti prilično male. Takođe može se zaključiti i da su samo te relativno male singularne vrednosti osetljive na šum, dok velike singularne vrednosti sadrže najveći deo energije svakog bloka slike i imaju dobru stabilnost čak i u slučajevima kada je slika pogođena manjim poremećajima. Ovo su jedna od glavnih svojstava dekompozicije singularnih vrednosti čije prednosti algoritam detekcije koristi [24]. Metod detekcije dupliranih regiona koji se bazira na dekompoziciji singularnih vrednosti se može koristiti samostalno ili u kombinaciji sa diskretnom talasnom transformacijom [9, 23].

3.2. ALGORITMI ZASNOVANI NA FREKVENCIJI

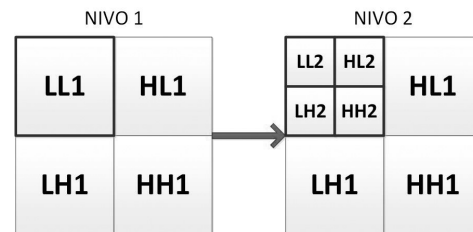
Algoritmi ove klase koriste procese kao što su **diskretna kosinusna transformacija** (eng. Discrete Cosine Transform, DCT), **diskretna talasna transformacija** (eng. Discrete Wavelet Transform, DWT) i **Furije-Melinova transformacija** (eng. Furier Mellin Transform, FMT) da bi se dobili odgovarajući karakteristični vektori [12].

Algoritmi detekcije zasnovani na **diskretnoj kosinusnoj transformaciji** koriste DCT koeficijente kao karakteristike koje se izvlače iz blokova radi njihovog poređenja, a koji su pri tom otporni na dodavanje Gausovog šuma i na JPEG kompresiju. Poređenje blokova na osnovu njihovih DCT koeficijenata je jedna od prvih tehnika koja je primenjena sa ciljem detektovanja dupliranih regiona u slici [8, 9]. DCT poseduje određena korisna svojstva koja su od naročito značaja u obradi slike kao što su: pakovanje, odnosno sabijanje energije, dekorelacija, simetrija i tako dalje. Naročito je značajna za kompresije sa gubicima jer ima mogućnost jakog sabijanja energije pošto se najveći deo informacije signala koncentriše u nekoliko DCT komponenti koje se nalaze na niskim frekvencijama [24]. Nakon podele slike na blokove, za svaki blok se računa DCT transformacija, a zatim se dobijeni DCT koeficijenti kvantiziraju sa korisnički definisanim parametrom Q i smeštaju u matricu A koja se posle leksikografski sortira. Q-faktor kontroliše osetljivost algoritma na stepen međusobnog poklapanja blokova, dok veličina bloka B i prag T kontrolišu kolika je minimalna veličina segmenta koji se može detektovati [15].

Proces **diskretne talasne transformacije** podrazumeva redukciju veličine slike na svakom nivou upotrebom dvodimenzionalnih filtara, čime se slika dekomponuje na različite frekvencijske nivoe. Međutim, većina aplikacija koristi odvojivu transformaciju u kojoj se prvo filtrira svaki red slike, a zatim se tako filtrirani redovi ponovo filtriraju, ali ovaj put po kolonama. Na taj način se jednom dekompozicijom slike dobijaju četiri opsega [1, 25]:

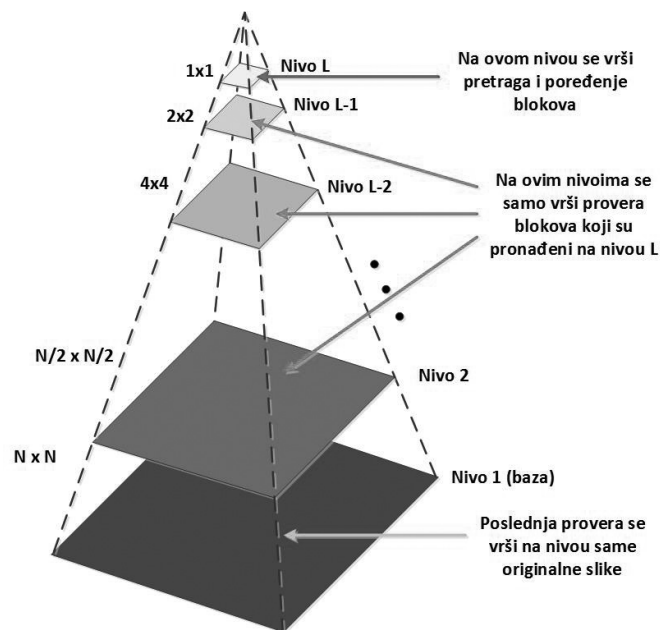
1. Niskofrekventno filtriranje redova, praćeno niskofrekventnim filtriranjem kolona čime se dobija takozvani **Low-Low (LL) opseg**
2. Niskofrekventno filtriranje redova, praćeno visokofrekventnim filtriranjem kolona čime se dobija takozvani **Low-High (LH) opseg**
3. Visokofrekventno filtriranje redova, praćeno niskofrekventnim filtriranjem kolona čime se dobija takozvani **High-Low (HL) opseg**
4. Visokofrekventno filtriranje redova, praćeno visokofrekventnim filtriranjem kolona čime se dobija takozvani **High-High (HH) opseg**

U većini slučajeva kada su u pitanju slike od interesa najveći deo energije je smešten u LL opseg. Na svakom nivou LL slika se deli na četiri manje slike. Ove pod-slike se posle mogu međusobno kombinovati kako bi se opet dobila originalna slika [25].



Slika 10. Dekompozicija slike [23]

Osnovna prednost korišćenja talasne transformacije je u tome da se iscrpno poređenje blokova slike vrši na nivou sa najmanjom rezolucijom čime se značajno poboljšava vreme i tačnost detekcije u odnosu na druge tehnike [26]. Algoritam detekcije se odvija u dve faze. U prvoj fazi vrši se detaljno pretraživanje identičnih blokova ali u okviru slike čije su dimenzije smanjene pomoću diskretne talasne transformacije. U drugoj fazi se detektovani blokovi iz prve faze upoređuju na različitim DWT nivoima [27].



Slika 11. Piramidalna dekompozicija slike [26]

**Furije-Melinova transformacija** u kombinaciji sa log-polarnim koordinatama spada u tehnike detekcije copy-move napada na sliku koje su znatno više otporne na kompresije sa gubicima, ali i na manipulacije koje podrazumevaju skaliranje i rotaciju dupliranog regiona, što do sada nije bio slučaj. Znači karakteristike blokova koje se dobijaju pomoću FMT-a ne samo da su otporne na JPEG kompresiju, blurovanje ili dodavanje šuma, već su takođe invarijantne na procese skaliranja i translacije [28]. Za invarijantnost u odnosu na rotaciju pogodan pristup je da se koriste kružno-harmonijske funkcije (eng. circular-harmonic functions) slike  $f(r,\theta)$  u polarnim koordinatama [29]:

$$f_m(r) = \frac{1}{2\pi} \int_0^{2\pi} f(r,\theta) \exp(-jm\theta) d\theta$$

gde je kružno-harmonijska frekvencija  $m$  celobrojna vrednost. Da bi se postigla i dodatna invarijantnost na skaliranje primenjuje se radijalna-Melinova transformacija na gore pomenutu kružnu-Furijeovu transformaciju [29]:

$$M_{s,m} = \int_0^1 r^{s-1} f_m(r) dr$$

gde je radijalna promenljiva  $r$  normalizovana tako da je intenzitet slike jednak nuli za  $r>1$ , dok je u opštem slučaju promenljiva  $s$  u Melinovoj transformaciji kompleksna vrednost. Onda se invarijantni deskriptori slike zasnovani na gore pomenutoj kombinaciji kružno-Furijeove i radijalno-Melinove transformacije mogu objediniti i nazvati **Furije-Melinovi deskriptori** (eng. **Fourier-Mellin descriptors**) [29].

### 3.3. ALGORITMI ZASNOVANI NA MOMENTU SLIKE

**Momenti slike** (eng. **image moments**) su skalarne vrednosti koje se koriste u kategorizaciji funkcije kao i za snimanje njenih značajnih karakteristika. Osnovne prednosti momenata su njihova neosetljivost na specifične vrste deformacija, kao što su različite geometrijske operacije i njihova moć diskriminacije koja im omogućava da razlikuju objekte koji pripadaju različitim klasama [8]. Glavne tehnike koje se primenjuju i istražuju, uključuju invarijantne momente, geometrijske momente, rotacione momente, kompleksne momente i mnoge druge. Dakle različite forme moment-deskriptora se intezivno koriste kao karakteristike objekta koje se koriste u njegovom prepoznavanju. Pošto je segment slike konačna oblast  $i$ , u najgorem slučaju se sastoji od konačnog broja kontinualnih delova, može se izračunati skup momenata, takav da se može koristiti za jedinstven opis informacija koje se sadrže u posmatranom segmentu slike [30]. Dvodimenzionalni moment  $m_{pq}$ , reda  $(p+q)$ , funkcije slike  $f(x,y)$  je definisan integralom [31]:

$$m_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x^p y^q f(x,y) dx dy$$

Ovoj kategoriji pripadaju: algoritam zasnovan na **Hu momentima** (eng. Hu Moments, HU) kojeg odlikuje povećana efikasnost i robusnost na raznorazne postobradne tehnike kao

što su blurovanje ili JPEG kompresija [17]; algoritam zasnovan na **Zenrike momentima** (eng. Zernike Moments, Zernike) koji je takođe otporan na dodavanje šuma, blurovanje i rotaciju objekta [8]; i algoritam zasnovan na **blur invarijantnim momentima** (eng. Blur-Invariant Moments, BLUR). Algoritmi u ovoj kategoriji takođe imaju manju veličinu vektora karakteristika i nisu preterano kompleksni. U svakom slučaju performanse ovih algoritama su obećavajuće, naročito kada je u pitanju njihova invarijantnost na rotaciju.

### 3.4. ALGORITMI ZASNOVANI NA TEKSTURI I INTENZITETU

Tekstura i intenzitet su svakako karakteristike slike koje se najčešće proučavaju u okviru obrade slike ili u okviru nekih kompjuterskih grafičkih aplikacija [8]. Tekstura je region slike u kome je skup lokalnih statističkih ili drugih lokalnih svojstava slike sporo promenljiv, konstantan ili približno periodičan [32]. Uobičajeno se za teksturu može smatrati da je to set različitih varijacija intenziteta (nivoa sivog) koji prati određene obrasce koji se ponavljaju [8]. Ona na neki način opisuje prostorno uređenje nivoa sivog piksela u jednom regionu slike [33]. Teško je analizirati teksturu razmatranjem vrednosti jednog piksela jer je ona pod uticajem susednih piksela. Kao rezultat tekstura je veoma važna karakteristika slike za proces njene karakterizacije i za proces prepoznavanja.

Sa druge strane deskriptori na bazi intenziteta imaju široku upotrebu za izdvajanje karakteristika na pozicijama tačaka od značaja. Glavna prednost pristupa koji se zasnivaju na teksturi i intenzitetu jeste što je veličina vektora karakteristika značajno smanjena. Međutim algoritmi koji pripadaju ovoj grupi nisu pokazali visok nivo otpornosti na operacije u obradi slike, naročito kada su u pitanju geometrijske operacije [8]. **Luo** i **Bravo-Solorio algoritmi** pripadaju ovoj klasi i oni kao prva tri elementa vektora obeležja koriste komponente crvene, zelene i plave boje, tačnije njihove srednje vrednosti na nivou bloka. Preostali elementi se dobijaju na osnovu informacije o lumentnoj komponenti. Luo algoritam koristi direktnu informaciju iz blokova, dok Bravo-Solorio algoritam razmatra entropiju bloka kao informaciju od značaja [9, 16, 34]. U ovu klasu spadaju još i **Lin-ov algoritam** koji proračunava prosečnu vrednost nivoa sivog svakog bloka i njegovih podblokova i **Wang-ov algoritam** koji za elemente vektora obeležja koristi srednje vrednosti inteziteta kružnih blokova sa različitim radijusima oko bloka koji se nalazi u centru [12].

### 4. ALGORITMI ZASNOVANI NA KEYPOINT-U

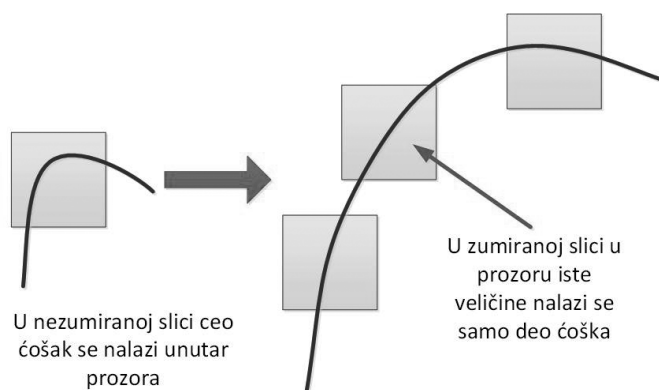
Algoritmi zasnovani na keypoint-u predstavljaju posebnu grupu algoritama za detekciju copy-move napada na sliku i njihov koncept se, za razliku od do sada obrađenih metoda, ne zasniva na podeli slike na blokove, iz kojih se potom izvlače određene karakteristike koje se potom koriste za međusobno upoređivanje. Umesto toga, karakteristike se izvlače na nivou cele slike [8]. Metode koje se zasnivaju na keypoint-u oslanjaju se na identifikaciju i selekciju regiona slike sa velikom entropi-



jom. Upravo ti regioni predstavljaju pomenute keypoint-e [12]. Svaki keypoint je okarakterisan vektorom karakteristika koji se sastoji od seta različitih statističkih podataka koje slika u sebi sadrži, a koji su skupljani u lokalnom susedstvu posmatranog keypoint-a [35]. Nakon identifikacije i selekcije vrši se izdvajanje vektora karakteristika, i to jedan vektor po jednom keypoint-u. Shodno tome se može izvesti zaključak da se vrši znatno manji proračun vektora karakteristika u odnosu na metode koje se zasnivaju na blokovima, jer ih ima znatno manje, a što na kraju dovodi do smanjenja ukupne kompleksnosti algoritma. Postoje dve različite verzije vektora karakteristika koji su bazirani na keypoint-u, odnosno dve različite metode, **SIFT (eng. Scale-Invariant Feature Transform)** i **SURF (eng. Speeded Up Robust Feature)**. Ove metode se koriste za izdvajanje svojstvenih lokalnih karakteristika u slici i za proizvodnju keypoint deskriptora koji reprezentuju te izdvojene karakteristike. Deskriptori koji se tom prilikom dobijaju su invarijantni na rotaciju, translaciju i skaliranje, a delimično su invarijantni i na promene osvetljenja. Takođe, deskriptori su robusni i na lokalne geometrijske promene [8]. Određene razlike koje postoje između ova dva algoritma, zasnivaju se na različitim pristupima naknadne obrade odgovarajućih karakteristika [12].

#### 4.1 DETEKCIJA SIFT METODOM

Neke od do sada obrađenih metoda su uspešno izlazile na kraj sa geometrijskom operacijom kao što je rotacija. To znači da na primer u rotiranoj slici možemo da nađemo iste ćoške, jer je očigledno da ćošak, ostaje ćošak čak i kada se slika rotira. Međutim, u slučaju primene skaliranja, taj ćošak, ne mora da bude isto ćošak i u skaliranoj slici, što se najbolje može videti i na slici 12.



Slika 12. Problem invarijantnosti usled procesa skaliranja

Na prethodnoj slici je očigledno da se ne može koristiti isti prozor u detekciji istog keypoint-a koji je različito skaliran. To znači da nam je za detektovanje većih ćoškova potreban veći prozor. Jedan od algoritama za detekciju copy-move napada na sliku koji je otporan na skaliranje je SIFT (eng. Scale-Invariant Feature Transform) algoritam koji se sastoji iz nekoliko faza [36, 37]:

1. Scale-space detekcija ekstremnih vrednosti
2. Lokalizacija keypoint-a
3. Dodeljivanje orijentacije

#### 4. Generisanje SIFT deskriptora

Prva faza podrazumeva pretragu svih razmera (eng. scale) i lokacija na slici uz pomoć efikasne DOG (eng. Difference-of-Gaussian) funkcije sa ciljem da se identifikuju potencijalne tačke od interesa koje su invarijantne na skaliranje i rotaciju. Detekcija lokacija koje su invarijantne na skaliranje slike, može se ostvariti pronalaženjem svih stabilnih karakteristika u svim mogućim razmerama date slike, i to korišćenjem kontinualne funkcije skaliranja koja je poznata kao scale-space. **Scale-space** je način predstavljanja slike u više različitih nivoa koji se međusobno razlikuju po rezoluciji. Ako se slika predstavi kao funkcija  $I(x,y)$  gde su  $x$  i  $y$  koordinate, onda se scale-space može predstaviti kao  $L(x,y,\sigma)$ , dodavanjem treće koordinate  $\sigma$  koja u stvari predstavlja faktor skaliranja. Na osnovu različitih eksperimenata, utvrđeno je da je jedina validna maska scale-space filtriranja, Gausova funkcija. Zato se može reći da je rezultat scale-space filtriranja slike definisan funkcijom  $L(x,y,\sigma)$ , dobijen konvolucijom Gausove funkcije različitih standardnih devijacija (različitih nivoa skaliranja),  $G(x,y,\sigma)$ , i početne, ulazne slike  $I(x,y)$  [37]:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

gde je:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}}$$

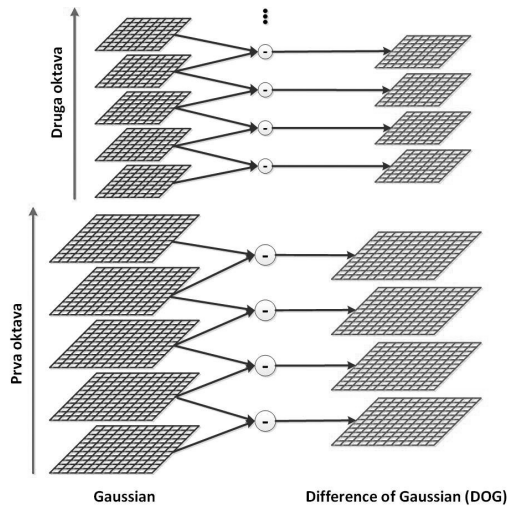
Scale-space filtriranje koje se primenjuje kako bi se na kraju izdvojili odgovarajući keypoint-i, nakon filtriranja Gausovim, podrazumeva i filtriranje Laplasovim filtrom (eng. Laplacian of Gaussian, LoG), za različite vrednosti parametra skaliranja  $\sigma$ . Tako će u već pomenutom primeru sa detektovanjem ćoška, Gausova funkcija sa malim  $\sigma$  davati velike vrednosti za male veličine ćoška dok će maska sa velikim  $\sigma$  kao rezultat davati velike vrednosti za velike ćoškove. Znači, mogu se pronaći svi lokalni maksimumi za sve odgovarajuće lokacije (space) i razmere (scale) čime se dobija lista  $(x,y,\sigma)$  vrednosti što znači da je detektovan potencijalan keypoint na lokaciji  $(x,y)$  i u razmeri  $\sigma$ .

Međutim LoG je previše složen algoritam pa se zato u SIFT metodi koriste razlike slika koje su filtrirane Gausovim filtrom, ali sa različitim vrednostima  $\sigma$ , odnosno različitim vrednostima faktora skaliranja. Te vrednosti  $\sigma$  se obično razlikuju u multiplikativnoj konstanti  $k$  [38]:

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned}$$

Ovaj proces se realizuje za različite oktave slike u okviru Gausove piramide, kao što je i prikazano na sledećoj slici 13. Za svaku oktavu scale-space-a inicijalna slika više puta konvoluirana sa Gausovom funkcijom čime se dobija set scale-space slika prikazanih na levoj strani. Susedne Gausove slike se odumiraju kako bi se dobile DoG slike prikazane na desnoj strani. Posle svake oktave, slika se pododabira sa faktorom 2, a zatim se ceo proces ponavlja.





Slika 13. Proces nastajanja DoG slika

Nakon što se izračunaju sve DoG slike, algoritam počinje potragu lokalnih ekstremuma za sve moguće lokacije i faktore skaliranja. Na primer, jedan piksel slike se poredi sa svojih osam suseda na istom nivou, ali poredi se takođe i sa odgovarajućih devet piksela slike koja je na nivou iznad (veći faktor skaliranja), kao i sa devet piksela slike koja je na nivou ispod (manji faktor skaliranja). Ako je u pitanju lokalni ekstremum, onda se radi o potencijalnom keypoint-u [39].

Druga faza podrazumeva lokalizaciju keypoint-a. Scale-space detekcija ekstremuma kao rezultat daje preveliki broj potencijalnih keypoint kandidata, pri čemu su neki od njih potpuno nestabilni, pa samim tim i neupotrebljivi. Razvojem funkcije scale-space u Tejlorov red moguće je preciznije odrediti lokacije ekstremuma. Takođe ako je intenzitet ekstremuma manji od nekog unapred određenog praga, potencijalni keypoint se odbacuje. Kako DoG ima veći odziv na ivice u slici, i ivice moraju biti odstranjene. Dakle, odstranjivanjem keypoint-a sa niskim kontrastom, koji su zbog toga osetljivi na šum, i keypoint-a u vidu ivica (slabo lokalizovani duž ivica), preostaju nam samo keypoint-i od interesa [37, 39].

Treća faza je ključni korak u postizanju invarijantnosti deskriptora u odnosu na rotaciju slike i podrazumeva dodeljivanje svakom keypoint-u jedne ili više orijentacija koje se zasnivaju na pravcima lokalnog gradijenta. Za svaki keypoint slike  $L(x,y,\sigma)$  se može izračunati gradijent magnitude  $m(x,y)$  kao i orijentacija  $\theta(x,y)$  i to na osnovu razlike piksela [37]:

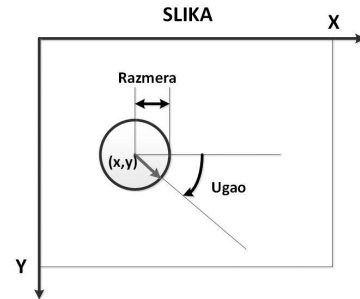
$$m(x,y) = \sqrt{L_1^2 + L_2^2}$$

$$\theta(x,y) = \arctan\left(\frac{L_2}{L_1}\right)$$

gde su  $L_1=L(x+1,y,\sigma) - L(x-1,y,\sigma)$  i  $L_2=L(x,y+1,\sigma) - L(x,y-1,\sigma)$ .

Na kraju se formira histogram orijentacija, pri čemu svaki bin histograma pokriva po deset stepeni, a na osnovu gradijenta orijentacija tačaka unutar regiona oko keypoint-a. Orijetacija koja odgovara maksimumu sa histograma se dodeljuje keypoint-u [39].

Prethodnim fazama svaki keypoint je opisan pomoću sledećih parametara: koordinatama  $(x,y)$ , razmerom i orijentacijom (ugao izražen u radijanima) kao što je i prikazano na slici 14. Ovi parametri obezbeđuju invarijantnost keypoint-a na rotaciju i skaliranje u slici.



Slika 14. SIFT keypoint sa svojim parametrima

Poslednja faza podrazumeva proračun SIFT deskriptora za svaki keypoint i zasniva se na regionu od  $16 \times 16$  piksela oko odgovarajućeg keypoint-a. Region se deli na podblokove veličine  $4 \times 4$  piksela i za svaki taj podblok se formira histogram orijentacija sa 8 binova (8 različitih orijentacija), što znači da ukupno ima 128 dostupnih informacija koje se predstavljaju u obliku vektora, čime se konačno formira SIFT deskriptor. SIFT procedura se završava formiranjem baze keypoint-a i informacija o njihovim karakteristikama koje uključuju koordinate, razmeru, orijentaciju i SIFT deskriptor. Najbolji kandidat za poklapanje sa odgovarajućim keypoint-om se pronalazi identifikacijom njegovih najbližih suseda u bazi keypoint-a. Najbliži sused je definisan kao keypoint sa minimalnim Euklidovim rastojanjem za deskriptor vektor [37].

### 5. ZAKLJUČAK

Detekcija copy-move napada, kao najrasprostranjenije manipulacije nad slikom, i dalje predstavlja jedan od ključnih problema u oblasti digitalne forenzike slike. Kroz ovaj rad su predstavljene mnoge tehnike, sa svim svojim prednostima i manama, koje se danas koriste u cilju rešavanja ovog problema. Najveći izazovi sa kojima se opisane tehnike suočavaju, ogledaju se u detekciji dupliranih regiona koji su dodatno podvrgnuti određenim operacijama kao što su kompresija, dodavanje šuma, rotacija i skaliranje, gde su po svoj prilici najbolje rezultate u detekciji pokazale tehnike koje se zasnivaju na keypoint-ima, kao što je SIFT metoda, a ne one koje se zasnivaju na blokovskoj metodi na kojoj se zasniva i većina današnjih algoritama. Međutim keypoint metode su osetljive na regione slike sa niskim kontrastom i na sadržaj slike koji se ponavlja, sa čime blokovske metode nemaju problema, tako da ni one nisu u potpunosti idealne. Sa druge strane drugi veliki izazov predstavlja i vreme proračuna, obzirom da se gotovo u svakom algoritmu obrađuju ogromne količine podataka u vidu različitih vektora karakteristika koje međusobno treba uporediti. I u oblasti digitalne forenzike slike često važi pravilo za algoritam, da što bolje rezultate daje, to je i komplikovaniji. Zato je neophodno balansirati između ova dva zahteva koja istovremeno, uz automatizaciju algoritama, određuju i pravac u kojem treba da se dalje razvija mlada

nauka kao što je digitalna forenzika slike. Takođe, prezentovane metode bi trebalo da podstaknu društvo u razvoju nekih novih algoritama koji će kombinovati prednosti pojedinačnih metoda u jedan zajednički super detektor.

## LITERATURA

- [1] Hursev Taha Sencar, Nasir Memon, Digital Image Forensics, Springer Science + Business Media New York 2013
- [2] Tehseen Shahid, Atif Bin Mansoor, Copy-Move Forgery Detection Algorithm for Digital Images and a New Accuracy Metric, International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009.
- [3] Matthias Kirchner, Notes on Digital Image Forensics and Counter-Forensic, The Department of Computer Science, TU Dresden, Germany, 2011.
- [4] Hany Farid, A survey of Image Forgery Detection, Dartmouth College, 2009.
- [5] Hany Farid, Image forgery detection – A survey, IEEE Signal Processing Magazine [16] March 2009.
- [6] Seung-Jin Ryu, Min-Jeong Lee, Heung-Kyu Lee, Detection of Copy-Rotate-Move Forgery Using Zenrike Moments, Information Hiding, Lecture Notes in Computer Science, Volume 6387, pp 51-65, 2010.
- [7] B. L. Shivakumar, S. Santhosh Baboo, Detecting Copy-Move Forgery in Digital Images> A Survey and Analysis of Current Methods, Global Journal of Computer Science and Technology, Vol. 10 Issue 7 Ver. 1.0 September 2010.
- [8] Osamah M. Al-Qershi, Bee Ee Khoo, Passive detection of copy-move forgery in digital images: State-of-the-art, Forensic Science International 231, 284-295, Elsevier, Ireland 2013.
- [9] Anil Dada Warbhe, Rajiv V. Dharskar, Vilas M. Thakare, Block Based Image Forgery Detection Techniques, International Journal of Engineering Sciences and Research Technology, 2015.
- [10] Guangjie Liu, Junwen Wang, Shiguo Lian, Zhiquan Wang, A passive image authentication scheme for detecting region-duplication forgery with rotation, Journal of Network and Computer Applications 34, 1557-1565, 2011.
- [11] Rohini A. Maind, Alka Khade, D.K. Chitre, Image Copy Move Forgery Detection using Block Representing Method, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-2, May 2014.
- [12] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou, An Evaluation of Popular Copy-Move Forgery Detection Approaches, IEEE transaction on Information forensic and security, November 2012.
- [13] Qing-Chu Yang, Chung-Lin Huang, Copy-Move Forgery Detection in Digital Image, Advances in Multimedia Information Processing – PCM 2009, pp 816-825, Springer, 2009.
- [14] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, Fast Copy-Move forgery Detection, WSEAS Transactions on Signal processing, Issue 5, Volume 5, May 2009.
- [15] Jessica Fridrich, David Soukal, Jan Lukas, Detection of Copy-Move Forgery in Digital Images, Proceedings of Digital Forensic Research Workshop, 2003.
- [16] Weiqi Luo, Jiwu Huang, Guoping Qiu, Robust Detection of Region-Duplication Forgery in Digital Image, Pattern Recognition, 2006. ICPR 2006. 18th International Conference
- [17] Salam A. Thajeel, Ghazali Bin Sulong, State of the art of copy-move forgery detection techniques: a review, International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.
- [18] Charmil Nitin Bharti, Purvi Tandel, A Survey of Image Forgery Detection Techniques, IEEE WiSPNET conference, 2016.
- [19] Tu K. Huynh, Thuong Le-Tien, A Survey on Image Forgery Detection Techniques, The IEEE RIVF, International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), 2015.
- [20] Mohammad Akbarpour Sekeh, Mohd. Aizaini Maarof, Mohd. Foad Rohani, Babak Mahdian, Efficient image duplicated region detection model using sequential block clustering, Digital Investigation 10 (2013) 73-84, Elsevier Ltd, 2013.
- [21] Vincent Christlein, Christian Riess, Elli Angelopoulou, A Study for the Detection of Copy-Move Forgeries, Friedrich-Alexander Universitat Erlangen – Nurnberg, 2010.
- [22] K.V. Hulmukhe, M. B. Jhade, Exploring Forgeries by Detecting Duplicated Image Regions, International Journal of Software and Web Sciences, 2013.
- [23] Sunil Kumar, S. Mukherjee, Copy-Move Forgery Detection in Digital Images: Progress and Challenges, International Journal on Computer Science and Engineering, Vol. 3, No. 2, February 2011.
- [24] Jie Zhao, Jichang Guo, Passive forensics for copy-move image forgery using method based on DCT and SVD, Forensic Science International 233, 158-166, 2013.
- [25] Vivek Kumar Singh, R.C. Tripathi, Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method, International Journal of Advanced Science and Technology, Vol. 35, October 2011.
- [26] Saiqa Khan, Arun Kulkarni, An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform, International Journal on Computer Science and Engineering, Vol. 02 No. 05, 1801-1806, 2010.
- [27] Meenakshi Sundaram, Nandini C, Copy-Move Forgery – A Survey, International Conference on Advanced Computing, Communication and Networks – CCN, 1286-1289, 2011.
- [28] Sevinc Bayram, Husrev Taha Sencar, Nasir Memon, An efficient and robust method for detecting copy-move forgery, Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009.
- [29] Yunlong Sheng, Henri H. Arsenault, Experiments on pattern recognition using invariant Fourier-Mellin descriptors, Optical Society of America, Vol. 3, No. 6, 1986.
- [30] Simon Xinmeng Liao, Image Analysis by Moments, The Department of Electrical and Computer Engineering, The University of Manitoba, Canada, 1993.
- [31] Babak Mahdian, Stanislav Saic, Detection of copy-move forgery using a method based on blur moment invariants, Forensic Science International 171, 180-189, 2007.
- [32] Katarina Kuzmanović, Segmentacija tekstone korišćenjem diskretne talasne transformacije, XIII Telekomunikacioni forum TELFOR 2005, Beograd, 2005.
- [33] Miodrag V. Popovic, Digitalna obrada slike, Akademski misao, Beograd, 2006.
- [34] Sergio Bravo-Solorio, Asoke K. Nandi, Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Processing 91, 1759-1770. 2011.
- [35] Xunyu Pan, Siwei Lyu, Region Duplication Detection Using Image Feature Matching, IEEE Transactions on information forensics and security, VOL. 5, NO. 4, December 2010.
- [36] David G. Lowe, Distinctive Image Features from Scale-Invariant Keypoints, International Journal of Computer Vision, 2004.
- [37] Atefeh Shahroudnejad, Mohammad Rahmati, Copy-Move Forgery Detection in Digital Images Using Affine-SIFT, Amirkabir University of Technology, ICSPIS 2016, 14-15 Dec. 2016.
- [38] Shiv Prasad, B. Ramkumar, Passive Copy-Move Forgery Detection using SIFT, HOG and SURF Features, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016.
- [39] Hailing Huang, Weiqiang Guo, Yu Zhang, Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm, IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008.



**Ranko Petrović**, Vlatacom institut visokih tehnologija, Beograd

**Kontakt:** ranko.petrovic@vlatacom.com  
ranko.petrovic@mts.rs

**Oblasti interesovanja:** Računarske mreže, Zaštita računarskih mreža, Multimedije, Digitalna forenzika