Tehnike manipulacije slikom i detekcija copy-move napada

Igor Franc, Miloš Stojmenović

***Sadržaj* — Pojavom računara i različitog softvera za obradu slika postalo je jednostavno falsifikovati ih. Kao jedan od najuspešnijih primena metoda analize slike je detekcija modifikacije digitalne fotografije. Iako postoje različiti sistemi za detekciju manipulacije digitalnom fotografijom njihov uspeh je ograničen i još uvek je u razvoju. Ovaj rad je napisan u pokušaju da pomogne ovim naporima tako što će dati kratak pregled poznatih metoda kao i smernice za dalje istraživanje u ovoj oblasti.**

***Ključne reči* — digital image forensics, copy-move atack, image forgeries, block matching, overlapping block**

I. UVOD

Digitalna fotografija je odavno prihvaćena kao dokaz nastanka prikazanih događaja a prihvatanje digitalne fotografije kao zvaničnog dokumenta je postala uobičajena praksa. Razvojem različitih softverskih alata postalo je lako kreirati, izmeniti i manipulisati digitalnom fotografijom bez očiglednih tragova manipulacije. Kao rezultat svega toga sve češće dolazi do situacija gde se više ne može garantovati integritet i autentičnost digitalnih fotografija. Ovo podriva kredibilitet digitalnih fotografija koje se ne mogu koristiti kao dokaz na sudu, na primer kao deo medicinske ili finansijske dokumentacije jer se ne može razlikovati da li je data digitalna fotografija original ili je modifikovana verzija.

Falsifikovanje digitalnih fotografija je rastući problem u krivičnim slučajevima. Trenutno nema uspostavljene metodologije kojom možemo automatski da proverimo autentičnost i integritet digitalnih fotografija. Otkrivanje manipulacije nad digitalnom fotografijom je važno polje istraživanja sa važnim implikacijama za obezbeđivanje kredibiliteta digitalnih fotografija [1]. U nedavnoj prošlosti velike količine falsifikovanih digitalnih fotografija moglo se videti u tabloid magazinima, modnoj industriji, naučnim časopisima, pa čak i na sudu.

Tehnike detekcije manipulacije slike se mogu podeliti na one sa aktivnim i pasivnim pristupom [2]. Kod onih sa aktivnim pristupom digitalna fotografija zahteva neku predobradu kao što je na primer watermark ili neka vrsta digitalnog potpisa sa vremenom kada je napravljena fotografija što ograničava njihovu primenu u praksi. Takođe na internetu postoji mnogo digitalnih fotografija koje nemaju watermark ili digitalni potpis. U takvom scenariu nije moguće koristiti aktivan pristup za detekciju autentičnosti fotografije. Za razliku od metoda sa aktivnim pristupom kod metoda sa pasivnim pristupom nije potreban nikakav watermark ili digitalni potpis koji je kreiran prilikom pravljenja fotografije[3].

Postoje tri tehnike koje su široko rasprostranjene i koriste se za manipulaciju digitalnom fotografijom [2]:

1. *Tampering* – falsifikovanje fotografije kako bi se dobio određeni rezultat
2. *Splicing* (*Compositing*) –ovom tehnikom se više slika spaja u jednu
3. *Cloning* (*Copy-Move*) – kloniranje određenih delova iste fotografije kako bi se neki objekti sakrili ili duplirali

U ovom radu će detaljno biti obrađene metode za detekciju kloniranja odnosno *Copy-Move.*

II. COPY – MOVE MANIPULACIJA

Copy-Move je specifičan način manipulacije fotografijom gde se deo same slike kopira na drugi deo iste slike. Ova manipulacija vrši se namerom da određeni objekat nestane sa slike tako da se preko njega kopira mali blok sa drugog dela iste slike. Pošto su kopirani delovi sa iste fotografije color palette, noise components, dynamic range i druga svojstva će biti kompatibilna sa ostatkom slike tako da ih je vrlo teško ljudskim okom otkriti.

(a) (b)

Sl. 1 – Copy- Move manipulacija:
a) originalna slika b) izmenjena slika

Igor Franc, Univerzitet Singidunum Beograd, Danijelova 32, 11000 Beograd, Srbija (telefon: 381-64-3579397), e-mail: ifranc@singidunum.ac.rs)

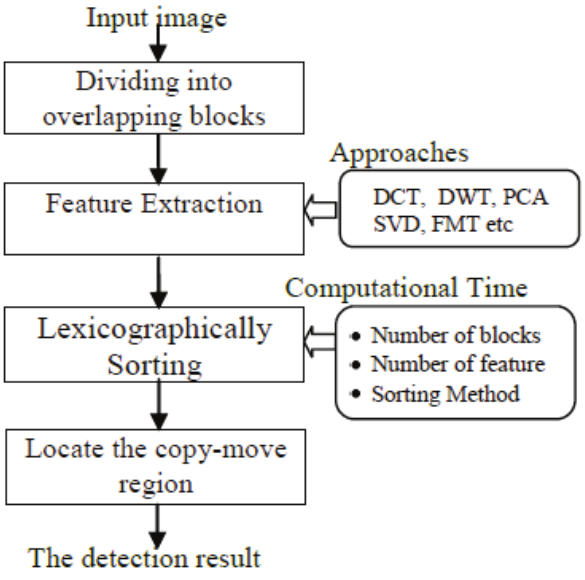
Miloš Stojmenović, Univerzitet Singidunum Beograd, Danijelova 32, 11000 Beograd, Srbija (telefon: 381-64-3298932), e-mail: mstojmenovic@singidunum.ac.rs).

III. DETEKCIJA COPY – MOVE

Najlakši način da se otkrije Copy-Move falsifikovanje je da se koristi exhaustive search. U ovom pristupu slika i njenja pomerena verzija(*shifted version*) se preklapa i traži se određeno blisko poklapanje blokova. Ovaj pristup je efikasan i jednostavan ali samo kada su u pitanju male slike.

Druga tehnika za oktrivanje manipulacije bazira se na autokorelaciji. Sve Copy-Move manipulacije uvode korelaciju između originalnog i kopiranog segmenta. Međutim ovaj metod nema veliku računarsku složenost i često ne uspeva da otkrije falsifikat.

U većini drugih pristupa slika se deli na blokove (*overlapping blocks*). Ideja je da se pronađe povezan blok koji je kopiran i premešten. Kopirani region sa satoji od više blokova koji se preklapaju. Rastojanje između svakog dupliranog bloka će biti isto jer se svaki blok preselio sa istim pomerajem. Sledeći korak je izvući karakteristike iz ovih blokova što bi dalo veoma slične ili iste rezultate za duplirani blok. Nekoliko autora predstavlja korišćenje različitih karakteristika za blok (*image block*). Ovi blokovi su vektorizovani i ubačeni u matricu a zatim se vektori leksikografski sortiraju za kasniju detekciju. Vreme izračunavanja zavisi od faktora kao što su broj blokova, tehnike sortiranja i broj karakteristika (*feature*).



Sl. 2 – Prikaz jednog sistema za detekciju Copy-Move falsifikovanja baziranog na blokovima

Tokom poslenjih 10 godina istraživanja su usmerena na to da se napravi potpuno automatski sistem za detekciju Copy-Move falsifikovanja. U međuvremenu neki važni koraci napravljeni su u ovoj oblasti. Dalje u radu biće predstavljene do sada predložene i implementirane metode detekcije i to u dve različite grupe. One koje mogu da detektuju Copy-Move falsifikovanje bez skaliranja i rotiranja će biti prvo predstavljene dok će u drugoj grupi biti noviji rezultati koji su otporni na skaliranje i rotiranje ali do određene granice.

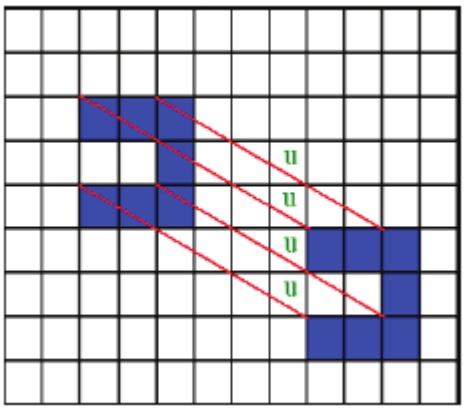
A. *Detekcija kopiranja regija bez skaliranja i rotiranja*

Fridrich [4] je prvi predložio metod za detekciju Copy-Move falsifikovanja. U njegovom metodu prvo se slika podeli na male blokove koji se preklapaju praćene sa *feature* ekstrakcijom. Zatim se računaju Discrete Cosine Transform (DCT) koeficijenti za svaki blok. Kada se izračunaju DCT koeficijenti se leksikografski sortiraju kako bi se proverilo da li su blokovi slični ili ne.

Sličan pristup predlaže i A.C.Popescu [5] ali on koristi principle component analysis (PCA) kako bi redukovao dimenzije DCT blokova. Ovaj metod je otporan na JPEG kompresiju do 50% i vreme potrebno za sortiranje je O(32x k lg k).

G.Li [6] predlaže metod koji smanjuje vreme potrebno za sortiranje na O(8k lg k). Po ovoj metodi slika se deli na 4 dela primenom discrete wavelet transform (DWT). Ovaj metod je otporan na JPEG kompresiju do 70%.

W. Luo [7] predlaže metodu koja se bazira na karakteristikama bloka piksela (*pixel block characteristics*). Slika se prvo podeli na male blokove (*overlapping blocks*) i računaju se karakteristike za svaki blok (*feature*). Ovim pristupom smanjuje se vreme potrebno za sortiranje na O(7k lg k). Ovaj metod je otporan na JPEG kompresiju do 30% kao i na Gaussian blurom i dodatnim šumom sa SNR 24 dB.



Sl. 3 – Detekcija bez skaliranja i rotiranja

Myna [8] predlaže metod bazira na wavelet transformaciji za detekciju a zatim se vrši exhaustive search da bi se identifikovali slični blokovi na slici i mapiranje njih u log-polar koordinate a zatim se koristi korelacija kao kriterijum sličnosti.

Jing Zhang [9] predlaže metod baziran na novoj ideji o poklapanju piksela (pixel-matching) za pronalazenje duplih regija. Po ovom metodu prvo se koristi DWT (Discrete Wavelet Transform) da bi se smanjila veličina a

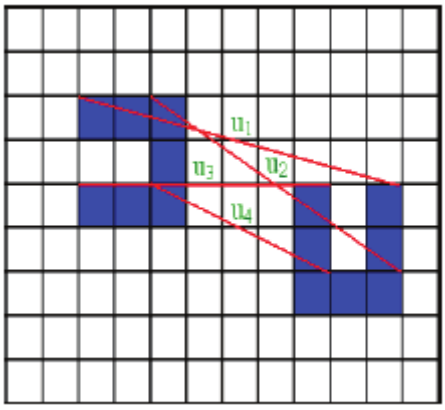
zatim se u fazi korelacije računa *spatial offset* između kopirane i nalepljene regije. Na kraju se koristi MMO (Mathematical Morphological Operations) za uklanjanje izolovanih tačaka. Predložena metoda ima manju kompleksnost računanja i iz tog razloga je otporna na različite tipove Copy-Move tehnika.

B. Detekcija kopiranja regija sa skaliranjem i rotiranjem

Bayram [10] predlaže metod sa primenom Fourier Mellin Transform (FMT) na blokove (*image block).* Prvo se primeni FMT na svaki blok a onda se rezultati razvrstavaju u log-polar koordinate. Ovaj metod je otporan na JPEG kompresiju do 20% kao i na rotaciju sa 10 stepeni i skaliranje do 10%.

Hwei-Jen Lin [11] predlaže metod u kome je veličina svakog bloka *16x16* u vektoru sa karakteristikama (*feature vektor*) sa 9 dimenzija. Za razliku od svih ostalih metoda gde se vrednosti čuvaju kao float brojevi ovde se čuvaju kao integer brojevi. Zatim se vektor sa karakteristikama (*feature vektor*) sortira uz pomoć *radix sort* algoritma što značajno smanjuje vreme potrebno za sortiranje na O(9k). Ograničenje ovog metoda je što ne može da detektuje kopirane regije male veličine. Međutim na osnovu rezultata eksperimenta koji su autori uradili metod radi dobro sa rotacijom od 90, 180 i 270 stepeni.

H. Huang [12] predstavlja metod koji se bazira na statističkim karakteristikama (*statistical features*) poznate kao scale invariant features transform (SIFT). SIFT deskriptor je otporan na iluminaciju, skaliranje, rotiranje i slične operacije. Prvo se izračunaju SIFT deskriptori i onda se deskriptor upoređuje sa svim ostalim kako bi se našle sve moguće kopirane regije. Iako ovaj metoda može da otkrije duplirane regije postoji jedno ograničenje a to su performanse algoritma.



Sl. 4 - Detekcija sa rotiranjem

Xunyu Pan [13] predlaže metod za detekciju koji se kao i prethodni bazira na SIFT algoritmu ali i u kome nije bitan ugao rotiranja kopirane regije. Prvo se izračunaju SIFT deskriptori i onda se oni grupišu u blokove (*non-overlapping*) za istraživanje. Poklapanje SIFT tačaka (*keypoints*) u blokovima za istraživanje se izračunava. Posle toga preračunavaju se moguće transformacije između originalnog i kopiranog bloka i kopirane regije se pronalaze na osnovu korelacione mape (correlation map). Iako ovaj metod pronalazi kopirane regije bez obzira na ugao rotiranje on ima takođe nedostatak a to je performansa samog altoritma.

Seung_Jin Ryu [14] predlaže metod koji se bazira na Zernike momentima (*Zernike moments*). Autor predlaže da se koriste Zenrike momenti jer je on pronašao da su oni superiorniji od drugih algoritama. Po ovom metodu prvo se slika podeli u MxN blokove sa podblokovima od LxL i da se onda računaju magnitude Zenrike momenata i sačuvaju kao vektor za svaki podblok (*sub-block*). Zatim se ti vektori sortiraju leksikografski . Rezultati ovog eksperimenta koji je izvršio autor pokazuju da se ovim metodom mogu pronaći kopirane regije koje su rotirane pod nekim uglom.

IV. ZAKLJUČAK

Iako je u radi prikazan veliki broj tehnika za detekciju Copy-move manipulacije i vidi se da je došlo do većih pomaka u ovoj oblasti još uvek ne postoji potpuno automatski sistem za detekciju koji je robustan na različite vrste manipulacije. Tri velika izazova su detektovati manipulaciju nad slikom koja je kompresovana (*compression*), detektovati manipulaciju nad slikom sa šumom (*noise*) i detektovati manipulaciju nad slikom sa rotacijom. Sofisticirani alati koji se pojavljuju će sve više zakomplikovati situaciju i otežati detekciju.

Po mišljenju autora za sada najbolje tehnike za detekciju su one koje se baziraju na SIFT algoritmu. Međutim tu postoji problem sa lošim performansama ovog algoritma pa bi u budućnosti trebalo na tome raditi ili eventualno koristiti neki sličan algoritam koji se bazira na invarijantama (*invariants*) a koji ima bolje performanse. I na kraju da zaključima da je oblast digitalne forenzike slike relativno nova oblast i da je potrebno još dosta istraživanja uraditi na ovu temu.

LITERATURA

[1] H.T. Sencar, and N.Memon, "Overview of State-of-the Art in Digital image Forensics", World Scientific Press, 2008

[2] B.L.Shivakumar and S.Santhosh Baboo, "Digital Image Forgery Detection", SAJOSPS, Vol. 10(2), pp. 116-119, 2010

[3] Lou Weigi, Qu Zhenhua, Pan Feng, and Herang Jiwu, " Survey of Passive Technology for Digital Image Forensics", Frontiers of Computer Science in China, Vol. 1(2), pp. 166-179, May 2007

[4] Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003.

[5] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of Computer Science, Dartmouth

[6] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, July 2-5, 2007, pp. 1750-1753.

[7] W .Luo, J. Huang, and G. Qiu, "Robust Detection of Region Duplication Forgery in Digital Image," in Proceedings of the 18th International Conference on Pattern Recognition, Vol. 4, 2006, pp. 746-749.
[8] A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping," in Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), Vol. 3, pp. 371-377, 2007.
[9] H . Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-276, 2008.
[10] Sevinc Bayram, Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of ICASSP 2009, 2009.
[11] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection", in WSEAS Transaction on Signal Processing, Vol 5(5), pp. 188-197, May 2009.
[12] H . Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-276, 2008.
[13] Xunyu Pan and Siwei Lyu, "Detecting Image Region Duplication Using SIFT Features", in: International Conference on Acoustics, Speech, and Signal Processing, Dallas, TX, 2010
[14] Seung-Jin Ryu, Min-Jeong Lee and Heung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery using Zernike Moments", in: 12th International Workshop on Information Hiding, Calgary, Alberta, Candada, 2010

ABSTRACT

With the advent of computers and various software to process images become easy to forge them. As one of the most successful applications of image analysis is methods to detect modifications of digital photography. Although there are different systems for detecting manipulation of digital photography, their success is limited. This paper was written in an attempt to assist these efforts by providing a brief overview of known methods and guidelines for further research.

TECHNIQUES OF IMAGE MANIPULATION AND DETECTION OF COPY-MOVE ATTACK

Igor Franc, Miloš Stojmenović