A Survey on Photo Forgery Detection Methods

Bilgehan Gurunlu[1,*], *Serkan Ozturk*[2]

[1]Department of Informatics, Kahramanmaras Sutcu Imam University, K.Maras, Turkey

[2] Department of Computer Engineering, Erciyes University, Kayseri, Turkey

Abstract. In recent years, digital image forgery detection has become one of the hardest studying area for researchers investigations in the field of information security and image processing. Image forgery detection methods can be divided into two extensive groups such as Active methods and Passive (Blind) methods. Active methods have been used data hiding techniques like watermarking and digital signatures. Passive forensic methods (or Blind) use image statistics or they investigate the attributes of the image to determine the forgeries. Passive detection techniques are also split into three branches; image splicing, image retouching, copy-move. Such image forgery detection methods are focus of this paper.

1 Introduction

Widespread of the digital cameras and the image editing tools like Adobe Photoshop, Microsoft Paint that gives for people doctored images for the bad aims. Increasing in image forensics has given boosting to special techniques for the detection of changing image. Image Forgery Detection is a new studying area which goals confirm the authenticity of image by collected information their feature. Diverse methods have been evolved to handle with changing image and forgery because of provide the origin of the image. We will evaluate different groups of algorithm. Unfortunately, we have not been able to review some important study here.

Digital image forgery methods can be classified two main categories. One of them active methods and the other passive(blind) methods[2]. Active methods must be have pre-embedded information, such as digital watermarking and steganography. Digital watermarking is a method embedding secret information in the data, can be divided two categories, visible and invisible [1]. Steganography's example of digital signatures.

Passive methods can be divided five group.

- Pixel Based (copy-move, resampling, splicing, statistical)
- Format Based (JPEG quantization, double JPEG, JPEG blocking) [2]
- Camera Based (chromatic aberration,color filter array,camera response, sensor noise)
- Physics Based (light direction(2-D), light direction(3-D), light environment) [3]

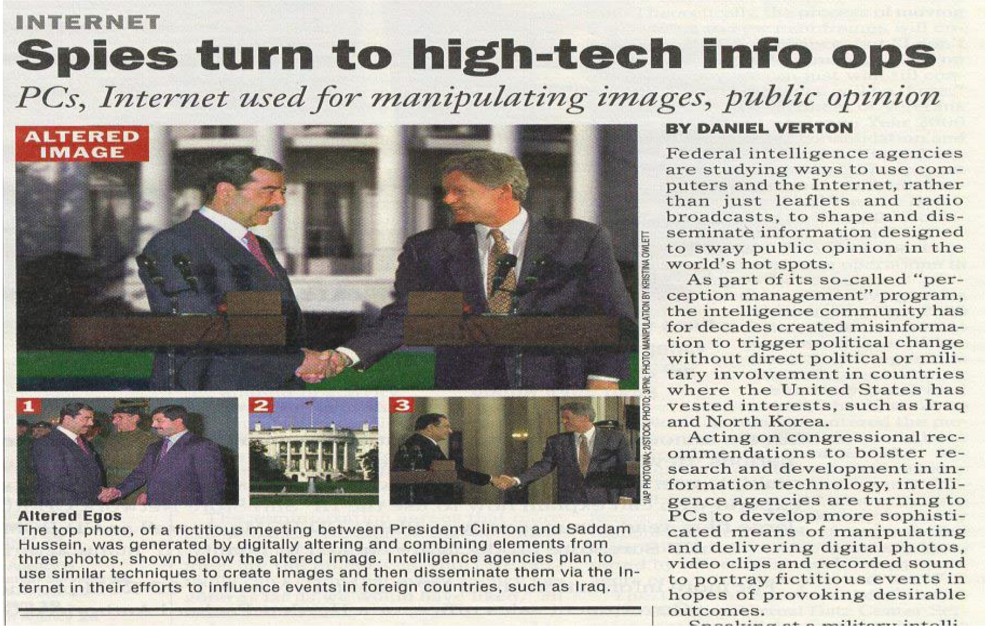
[*] Corresponding author: gurunlu@gmail.com

- Geometric Based (principal point, metric measurements) [4]

We evaluated the study on copy-move (or cloning) in this survey. Copy-move forgery detection methods are following three groups.

- Brute Forces [5]
- Block-Base Techniques
- Keypoint Based Techniques

Brute force techniques is based exhaustive search and auto correlation methods [6]. Block based techniques use like this algorithms; DCT(Discrete Cosine Transform)[7], PCA(Principle Component Analysis) [8], SVD(Singular Value Decomposition)[8], DWT (Discrete Wavelet Transform)[10]. Keypoint based techniques use like this algorithms; SIFT(Scale Invariant feature transform), SURF(Speeded-up Robust features). An Digital forgery example of a newspaper report on Saddam and Bill Clinton photographs is shown in Figure 1.


ALTERED IMAGE
1
2
3

INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Speaking at a military intelli-

1/AP PHOTO/INA; 2/STOCK PHOTO; 3/PNI; PHOTO MANIPULATION BY KRISTINA OWLETT

Altered Egos
The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig.1. Digital Forgery Example [5]

2 Basic Steps of the Methods

Although there are a large number of proposed copy-move fraud detection methods, all the methods applies the general flow chart given in Figure 2. As seen in the flow chart, there are two alternatives techniques after pre-processing: block based methods and keypoint based methods. In both methods pre-processing steps are applied. For example; many methods studying on gray level images and so color channels must be combined.

Step 1. Image Pre-Processing; is the first step. Methods change some specific details on the image like image filtering, DCT coefficients, RGB to gray level before the feature extraction step [9].

Step 2. Feature Extraction; in the block based method the image is divided into sub-blocks in the form of a rectangle. For each sub-block, the feature vectors are computed. Then similar attribute vectors are matched. On the other hand, in feature based methods, only image regions with high entropy value are determined without any image subdivision. These regions are called “key points” and the feature vectors of these regions subtracted [10].

Step 3. Feature Matching; similarity between two feature is marked for a duplicated image. Some methods uses lexicographic sorting and others best-bin-first search(kd-tree algorithm) in determing the similar features vectors.

Step 4. Filtering; have been committed for decrease the possibility of the false positive matches. There are many distance algorithm with the near intensities. Some research proposed Euclidean distance[11], and someone correlation coefficient[12].

Step 5. Pro-Processing; this is last step of all the methods and its optional. The goal of this last step is to protect only those blocks(or keypoint) that share common feature. When considering a set of mappings for the region, it is expected that the source and target blocks(or keypoint) of these mappings are close to each other.

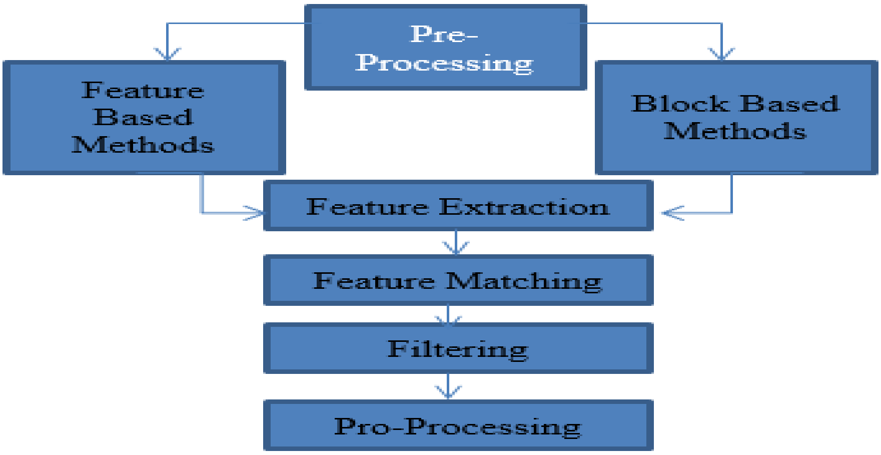


Fig.2. Image Forgery Detection Flow-Chart

3 Comparison of the Related Work

In this subdivision of manuscript, we supply some experimental solutions to describe the demonstration of the analytic algorithm suggested.

Author(s)	Techniques	Benefits	Drawbacks
[13]	Coefficient map and threshold. DWT and segmentation	A good result for diverse condition, copy-move and transformation	Execution time
[14]	Transform matrix. Segmentation	Give preferable result using SIFT	

[15]	Histogram of Gradient	High accurate ratio against to rotation, color reduction and contrast change attacks. Attribute size and calculation cost more effective	It needs to be developed and improved against large scale rotation, JPEG compression and scaling attacks
[16]	Binary DCT	Strong against contrast change, noises, JEG compression applied it also works on images at the same time	Like scaling and rotating weak against attacks
[17]	SVD and DCT	Low dimension. Multiple fraud detection. Robust to Gaussian blurring, JPEG compression and other operation.	Solely tested post-processing step
[18]	Fast Walsh-Hadamard Transform(FWHT)	Great correctness	Bad accuracy if the image transform
[19]	SURF and Nearest Neighbour Ratio(NNR)	Good to rotation, scaling and JPEG compression	Copy-move pixel are not localized
[20]	Convolution Neural Network (CNN)	Learned automatically	Copy-move pixel are not localized

4 Conclusion

In this paper, a brief survey of the image forgery detection(IFD) methods will be help the researcher in this studying area. We have mostly surveyed publication on IFD between 2013 and 2018. We provided a wide review of up-to-date copy move forgery methods. The methods are classifying two groups; like block base and keypoint based. Although both methods are superior to themselves, there have been more recent publications on block based methods last five years.

References

1. V. Aslantaş, Ş.Özer, S.Öztürk, "Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms", Optics Communications, vol.282, pp.2806-2817, (2009).
2. M. D. Ansari, S. P. Ghrera, V. Tyagi, “Pixel-Based Image Forgery Detection A Review”, IETE Journal of Education, 55(1), 40-46, (2014).
3. H. Farid, “A survey of image forgery detection”, IEEE Signal Processing Magazine, 26(2), 16-25, (2009).

4. M.K. Tohnson, H. Farid, “Metric measurements on a plane from single image” Dept. Comput.Sci., Darmouth College, Tech. Rep. TR2006-576, (2006).
5. J. Fridrich, D. Soukal, J. Luka, “Detection of copy-move forgery in digital iamges”, Digital Forensic Research Workshop, pp.6-8, (2003).
6. N.K. Gill, R. Garg, A. Doger, “A review paper on digital image forgery detection techniques”, 8th ICCCNT 2017, pp.1-7, (2017).
7. E. Ardizzone, A. Bruno, G. Mazzola,” Copy-move forgery detection via texture description” ACM Workshop on multimedia in forensics, security and intelligence, pp.59-64, (2010).
8. B. Soloria, A. K. Nandi,” Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics”, International Journal of Signal Processing, pp.1759-1770, (2011).
9. A. Makandar, B. Halalli,” A review on preprocessing techniques for digital mammography images”, International Journal of Computer Applications, pp.0875-887, (2015).
10. I. Amerini, L.Ballan, Caldelli, Caldelli, A. D. Bimbo, “A SIFT-based forensic method for copy-move attack detection and transformation recovery”. IEEE Transactions on Information Forensics and Security, 6(3), 1099–1110, (2011).
11. S. Ryu, M. Lee, H. Lee, “Detection of Copy-Rotate-Move Forgery using Zernike Moments,” in Information Hiding Conference, Jun. 2010, pp. 51–65. (2010).
12. S. Bravo-Solorio, A. K. Nandi, “Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling,” in International Conference on Acoustics, Speech and Signal Processing, May 2011, pp. 1880–1883. (2011).
13. C. M. Pun, X. C. Yuan, X.L. Bi. "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching." IEEE, (2015).
14. L. Jian. "Segmentation-based Image Copy-move Forgery Detection Scheme." IET, (2015).
15. J.C. Lee, C.P.Chang, W.K. Chen. “Detection of copy–move image forgery using histogram of orientated gradients. Information Sciences, Informatics and Computer Science Intelligent Systems Applications, 3(21), 250-262, (2015).
16. S.Kumar, J. V. Desai, S. Mukherjee, “Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors”. International Journal of Image, Graphics and Signal Processing (IJIGSP), 7(6), 38-44, (2015).
17. J.Zhao, J.Guo, “Passive Forensics for Copy-Move Image Forgery Using a Method Based on DCT and SVD”. ForensicSci.Int.233,158–166.(2015).
18. B.Yang, X.Sun, X.Chen, J.Zhang, X.Li, “An Efficient Forensic Method for Copy – Move Forgery Detection Based on DWT-FWHT”, RadioEng.22,1098–1105. (2013).
19. E.Silva, T. Carvalho, A. Ferreira, A. Rocha, “Going Deeper into Copy-Move Forgery Detection: Exploring Image Tell tales via multi-scale analysis and voting processes. J Visual Commun Image Represent.;29:16–32, (2015).
20. J. Chen, X. Kang, Y. Liu, ZJ. Wang,”Median Filtering Forensics Based on Convolutional Neural Networks. IEEE Signal Process Lett. 22:1849–1853, (2015).