ISSN: 2321-7782 (Online)
Volume 4, Issue 2, February 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Review on Block Based Copy Move Image Forgery Detection Techniques

Harpreet Kaur[1]
Student, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib - India

Sheenam Malhotra[2]
Assistant Professor, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib - India

Abstract: ***Digital images in every one's life depict very important role in various domains such as daily newspapers, magazines, multimedia, medical diagnosis, legal document and evidence in court. In today's digital world image forensics is extremely demanding field as images are the key source of communication, fastest means to transfer and exchange of the information but now truthfulness of images are easily lost by using freely available editing software like photo shop, GIMP, Paint.NET which manipulate the content and deny the authenticity and integrity of images. Image Forgery or tampering means to create fake images without leaving any visually detectable traces. One of the most common types of Image forgery is Copy move Image Forgery which is Pixel Based Technique. In Copy move (or region duplication or cloning) image forgery, region from image is copied and pasted anywhere in the same image to hide, clone or alter the content of an image. This paper reviews the Block Based Methods which are commonly used for identifying copy move image forgery.***

Keywords: Image forensics, Image Forgery, Tampering, Pixel based, copy-move forgery, Block-Based Methods.

I. INTRODUCTION

Digital images are widely used and key source of information exchange in various domains. Image Tampering which is also called image forgery is defined as adding, deleting, altering the content of an image without leaving any discernible footprints. In Image Forensics, detecting forgery in digital images is relatively an emerging research field. The availability of editing tools such as adobe photo shop, GIMP, Paint.NET, Corel paint shop, makes it very easy to modify the digital images without leaving any visually detectable footprints of image tampering. It is very hard to distinguish between the original and forged image with naked eyes. Image forgery is illegal act. Digital image forensic approaches are classified as active and passive (or blind) techniques. Active methods involve digital signature and watermark must be embedded inside the image but in passive or blind method the source image and pre-embedded information regarding the image is not available. Passive approach is widely used and popular as no prior information regarding the image is needed. Passive Approaches can be divided into five categories such as Pixel Based, format Based, camera Based, Physical Based, Geometry Based image forgery detection. Pixel based detection approach focuses on the pixel which is the smallest element that constitute an image and detect the statistical irregularities at pixel level. These techniques are categorized as Copy-Move, Splicing, Re-sampling, Retouching. Format based methods are used to detect the forgery in compressed images. Lossy JPEG Compression helps to identify the traces left after applying forgery. It is classified as JPEG Quantization, JPEG Blocking, Double and Multiple JPEG Compression. Camera-based image forgery approach is that when an image is captured from a digital camera, it passes to sensors through color filter array and moves from camera sensor to the memory by series of processing steps which can vary on the camera model. Physically-based approach used to detect inconsistencies in 3-D interaction between light, physical objects and the camera. Geometric based approach used to make measurement of objects and their positions relative to the camera. The most commonly used Pixel Based technique that is copy-move (or region duplication or cloning) image forgery in which the region of image is copied and pasted anywhere into the same image to hide, clone, alter or manipulate the content of image. The

important scene or part of an image which is intended to be hidden is covered with copied section of same image. People do forgery which becomes threat to society, to mislead others or for getting popularity without leaving any visual footprints of image tampering. Detecting image forgery in the digital images is very challenging task. Copy move forgery is easy to implement but difficult to detect than other types of forgeries like Splicing, Re-sampling etc.

II. Related Work

To detect image forgery large number of approaches has been proposed by various authors. This section introduces the currently used techniques in the area of digital image forgery detection. Block based methods mainly aims to divide an image into overlapping and non overlapping blocks of equal size rather than identifying the entire forged regions. Then calculate the transformation between each block and compare them in order to detect duplicate regions [1]. After divide an image into blocks, feature vectors are extracted and lexicographically sorted to check similarity between neighboring blocks and matching is performed between these block which leads to detect forgery. The most commonly used block based feature extraction methods are DCT (Discrete Cosine Transform), PCA (Principal Component Analysis), KPCA (Kernel PCA), DWT (Discrete Wavelet Transform), DyWT (Dyadic Wavelet Transform), SVD (Singular Value decomposition), LBP (Local Binary Pattern), FMT (Fourier Mellin Transform), Zernike, Gabor Filter etc.

Gagandeep Kaur et al. [1] presented the block based and key point based copy move forgery detection techniques. Gajanan K. Birajdar et al. [2] presented the overview of various passive image forgery detection techniques. Nitish Nirmalkar et al. [3] presented the review on pixel, format, physical, camera, geometric based approaches. Abdul et al. [4] before dividing an image into overlapping blocks, hybrid filter are applied then Completed Robust Local Binary Pattern (CRLBP) operator is used to extract the features. Feature vectors are lexicographically sorted and compared by using Euclidean distances to identify the forged regions and solve the problem of false matching and works efficiently in the presence of additive noise, blurring, rotation and compression.

Neha Jadhav et al. [5] presented DCT method which reduces time and for highly textured images DCT is better than any other forgery detection algorithms. Ghulam Muhammad et al. [6] presented the method to detect forgery in which Gabor filter is used as feature extraction method with different orientations and scales are applied to an image then DCT is calculated from all the filter outputs and DCT coefficients are concatenated to form feature vector. Revathy G S et al. [7] presented the method in which discrete wavelet transform is applied to an input image before dividing it into overlapping blocks. Features are extracted from each block by using histogram of oriented gradients and lexicographically these features are sorted. Matching is performed to identify forged regions. Sunil Kumar et al. [8] presented the DCT method which works with high stability even in extreme conditions of contrast change.

Michael Zimba et al. [9] presented Discrete Wavelet Transform (DWT) and Principal Component Analysis- Eigen value Decomposition (PCA-EVD) to detect cloning forgery. S. A. Fattah et al. [10] presented 2D-DWT method applied on the forged image. Block matching is not performed on all the blocks which reduces computational burden, some candidate's e non-overlapping blocks are selected based on similarity then all overlapping blocks are compared with selected candidate with the help of which forged block is detected. Muhammad Ali Qureshi et al. [11] presented pixel based forgery detection techniques which require no prior information regarding the input image. Rohini. A. Maind et al. [12] presented DCT each cosine transformed block is represented by a circle. This method is robust to multiple copy-move forgery, blurring or nosing adding and having low computational complexity.

Chen-Ming Hsu et al. [13] presented efficient detection algorithm in which Gabor filter is applied to each block. Features are extracted from the histogram of orientated Gabor magnitude of overlapping blocks and identify forgery in images having translation, rotation, JPEG compression, blurring, and brightness adjustment.

Beste Ustubioglu et al. [14] presented the method in which he Image is divided into overlapping blocks and LBP value is obtained from each block, after that DCT is applied. LBP- DCT methods it is accurate than existing DCT based methods and lowers false negative values. Vivek Kumar Singh et al. [15] presented Zernike moments (ZM) rotation invariant property for fast copy-rotate-paste image forgery detection. Feng Liu et al. [16] presented DWT and SVD method for effectively detect and locate multiple copy-move forgery, even when an image was manipulated by Gaussian blurring, JPEG compression.

III. CONCLUSION

Nowadays, applying forgery to the images is very common and easy task with the help of editing tools which are easily and freely available. Various techniques are available which helps to detect the forgery in digital images. This paper gives an overview on the Block Based Techniques for detection of copy move forgery. Copy Move (or region duplication or cloning) is one of the most popular methods to perform forgery in the digital images in which region from an image is copied and pasted into the same image to hide, duplicate or clone the content of an image. A Lot of work has been done to detect copy move image forgery but still there is need to develop an efficient and robust method.

References

1. Gagandeep Kaur, Manjot Kumar, "Study of Various Copy Move Forgery Attack Detection Techniques In Digital Images", International Journal of research in computer application and robotics, ISSN: 2320-7345, vol. 3, no. 9, pp. 30-34, September 2015.
2. Gajanan K. Birajdar, "Digital image forgery detection using passive techniques: A survey," ELSEVIER, vol. 10, no. 3, pp. 226–245, June 2013.
3. Nitish Nirmalkar, Shailesh Kamble, "A Review of Image Forgery Techniques and their Detection," IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems, Coimbatore, pp. 1-5, March 2015.
4. Salam Abdul-Nabi Thajeel and Ghazali Sulong, "A Novel Approach for Detection of Copy Move Forgery using Completed Robust Local Binary Pattern," Journal of Information Hiding and Multimedia Signal Processing, ISSN: 2073-4212, vol. 6, no. 2, March 2015.
5. Neha Jadhav, Suvarna Kharat, Punam Nangare, "Copy-Move Forgery Detection Using Dct," International Journal of Emerging Technologies and Engineering (IJETE), ISSN: 2348 – 8050, vol. 2, no. 3, March 2015.
6. Ghulam Muhammad, "Image Forgery Detection Using Gabor Filter And DCT," International Conference on Electrical Engineering and Information & Communication Technology, vol. 8, no. 5, pp. 377-390, Oct. 2014.
7. Revathy G S, "Region Duplication Forgery detection using Histogram of Oriented Gradients," International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, vol. 4, no. 06, pp. 417-420, June 2015.
8. Sunil Kumar and J. V. Desai, "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors," I.J. Image, Graphics and Signal Processing, vol. 6, pp. 38-44, May 2015.
9. Michael Zimba, Sun Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection," International Journal of Digital Content Technology And its Applications, vol. 5, no. 1, pp. 251-258, Jan. 2011.
10. S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed, and C. Shahnaz, "A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT," IEEE, ISSN: 1548-3746, Aug. 2014.
11. Muhammad Ali, "A bibliography of pixel-based blind image forgery detection techniques," Signal Processing: Image Communication 39, ELSEVIER, pp. 46–74, Aug. 2015.
12. 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, vol. 4, Issue 2, pp. 49-53, May 2014.
13. Chen-Ming Hsu, "An Efficient Detection algorithm for Copy-Move Forgery", 10th Asia Joint Conference on Information Security, Kaohsiung, IEEE, May 2015.
14. Beste Ustubioglu, Guzin Ulutas, Mustafa Ulutas, Vasif Nabiyev and Arda Ustubioglu, "LBP-DCT Based Copy Move Forgery Detection Algorithm," Springer International Publishing Switzerland, ISSN: 1876-1100, pp. 127-136, 2016.
15. Vivek Kumar Singh and R. C. Tripathi, "Fast Rotation Invariant Detection of Region Duplication Attacks Even on Uniform Background Containing Digital Images," ELSEVIER, ISSN: 1877-0509, pp. 772 – 780, feb. 2015.
16. Feng Liu and Hao Feng, "An efficient algorithm for image copy-move forgery detection based on DWT and SVD," International Journal of Security and Its Applications, ISSN: 1738-9976, vol.8, no.5, pp. 377-390, 2014.

