JOURNAL OF COMPUTING TECHNOLOGIES

ISSN 2278 – 3814

Available online at www.jctjournals.com

Volume 1, Issue 2, June 2012

A Review on Passive Approach for Image Manipulation Detection Techniques for Copy Move Forgery

Ashwini V. Malviya[1], Dr. S. A. Ladhake[2]

[1] *Department of Electronics & Telecommunication, Sipna College of Engineering & Technology, Amravati, Maharashtra, India*

ash.malviya@gmail.com

[2]*Principal, Sipna College of Engineering & Technology, Amravati, Maharashtra, India*

saladhake@yahoo.co.in

Abstract— ***It* has been seen that there is a tremendous progress in Image processing technologies. The impact of visual information is stronger over theoretical information in many fields such as journalism, legal evidence, medical images, forensic investigation and glamour photography. But with the rise in image processing technologies, there is also an increase in image manipulation techniques. Today we come across image processing software that produce doctored Images with high sophistication, which are manipulated in such a way that the tampering is not easily visible to naked eye. The authenticity of a digital image has become a challenging task due to the various tools present in the photo editing software packages. There are number of ways of tampering an Image, such as splicing two different images together, removal of objects from the image, addition of objects in the image, change of appearance of objects in the image or resizing the image. This Image manipulation detection technique detects traces of digital tampering in the complete absence of any form of digital watermark or signature and is therefore referred as passive. Lot of research is been carried out for detection, correction and prevention of digital Image forgeries. In this paper we discuss the techniques employed by different researchers for mainly copy-move forgery which may be used for removal of object and addition of object in the image by duplication. Also discussing the pros and cons of every methodology, which may result in a creating a new metric to achieve accuracy in these detection techniques.**

Keywords— **Image tampering detection, Copy move forgery, Image Manipulation, Digital forensic, Image forgery detection.**

I. INTRODUCTION

Image manipulation is the application of image editing techniques to manipulate the images in order to create an illusion or deception in contrast to mere enhancement or correction.

Image forgery is neither new, nor recent. Sophisticated digital cameras and photo- editing software packages are nowadays easily accessible. As a result, it has become relatively easy to manipulate digital images and create forgeries. The legal system routinely relies on a range of forensic analysis such as DNA or fingerprint identification, forensic odontology, forensic entomology and forensic geology [10]. Criminal scene photographs which are presented as evidence in court of law plays an important role in giving final verdict of a particular legal case. Image processing is also of great significance in journalism, manipulating the image for public view, is one of the common cause to mislead the masses. We find number of celebrities‘ images doctored in glamour photography to give a flawless look to the celebrities.

This demands a reliable image manipulation detection system, able to detect whether a photograph is real or altered. Though these manipulation are sometimes not noticeable by human eye, they do affect the statistics of the image, because of detection of tampering is possible. Thus it becomes very important to develop efficient techniques which may detect these forgeries which are addition of an object in image, removal of object from image and change of appearance of the object in image.

A. An Active Approach For Manipulation Detection

Image can be authenticated by Digital watermarking. Various watermark techniques [12], [17] have been proposed in recent years, which can be used not only for authentication, but also for being an evidence for the tamper detection. Wang et al. [13] and Lin et al. [14] both embedded watermarks consisting of the authentication data and the recovery data into image blocks for image tamper detection and recovery in the future. The drawback of watermark techniques is that one must embed a watermark into the image first. Also a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. Many other techniques that work in the absence of any digital watermark or signature have been proposed.

B. Passive Approach For Manipulation Detection

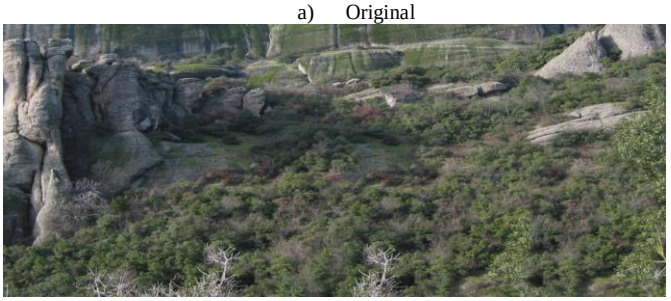
In contrast to approaches such as active digital watermarking and Steganography [17], passive techniques for image manipulation detection are carried out in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools for passive or blind approach for manipulation detection can be roughly categorized as pixel-based techniques, format-based techniques, camera-based techniques geometric based techniques [10].

In this paper we discuss one of the pixel based detection technique which is passive techniques for image forensics which operate in the absence of any watermark or signature.

II. COPY MOVE MANIPULATION

One of the most common image manipulations is to copy move (copy paste, cloning) forgery. Here one part of the image is copied and pasted on the object which is not desired. This manipulation is termed as copy-move forgery as depicted in figure 1 [3].

a) Original



b) Manipulated

Fig:1.a) Original and b) Manipulated images. The undesired object is hidden by pasting a portion from the same image [3].

Also part of the image may be pasted in the same image to enhance the image as depicted in figure 2.

a) Original

b) Manipulated

Fig:2. a) Original and b) Manipulated Images. Part from the original image is copied and pasted onto the same image to enhance the image [1].

There is a need of developing computationally efficient algorithms to authenticate the images by manipulation detection techniques. As the duplicated region may be of any shape and may be at any location, if the copy move manipulation is done carefully, it may be difficult to detect the cloned portion.

III. COPY MOVE MANIPULATION DETECTION.

The underlying building block of a digital image, in the digital domain, is the pixel. In this paper we discuss about the different pixel-based technique that detects statistical inconsistency introduced at the pixel level for detection of copy move forgery.

Computationally efficient algorithms have been developed to detect duplicated image regions. In the following part we will discuss about the various algorithms been developed for copy move manipulation detection where the portion of the image is copied and pasted on the same image without any change in illumination, without any rotation, scaling, etc. The authors in [2] first apply a block discrete cosine transform (DCT). Duplicated regions are detected by lexicographically sorting the DCT block coefficients and grouping similar blocks with the same spatial offset in the image. In a related approach, A.C. Popescu and H. Farid [3] apply a principal component analysis (PCA) on small fixed size image blocks to yield a reduced-dimension representation. Duplicated regions are again detected by lexicographically sorting and grouping all of the image blocks. Authors of [3] used the principle component analysis (PCA) and represented each block of size 16× 16 as a feature vector of length 32, and lexicographically sorted the vectors in O(32× k lgk) [15] time. Their method was robust to compression up to JPEG quality level 50.

Both the DCT and PCA representations are employed to reduce computational complexity and to ensure that the copy move detection is robust to minor variations in the image due to additive noise or lossy compression [10].

A simple method was proposed by authors in [4] to detect copy move forgery by block matching in spatial domain. The input image of size a×b is divided into ‗n' blocks of size m×m pixels by moving the block point to point on the image. Each block is iteratively compared to every other block in the image. In case of complete match both blocks are marked as copied. In case of copy detection, the adjacent neighbours of the marked blocks are then compared. The algorithm confirms the manipulation if at least three blocks in the adjacent neighbourhood of the both marked blocks is exact match of each other [4].

In another passive approach by G. Li in [5] applied DWT to the given image, and used SVD on fixed-size blocks of low-frequency component in wavelet sub-band to yield a reduced dimension representation, then lexicographically sorted the SV vectors to detect duplicated image blocks. The sorting time was reduced to O(8k lgk) [15] using this method.

An approach based on the application of wavelet transform that detects and performed exhaustive search to identify the similar blocks in the image by mapping them to log-polar coordinates and using phase correlation as the similarity criterion was proposed by A. N. Myna et al. [6].

Copy move forgeries are also carried out with copying the portion of the image and rotating or scaling it, before pasting it on the same image. H. Huang et al. [7] first extracted scale invariant features transform SIFT descriptors of an image, which are invariant to changes in illumination, rotation, scaling etc. Owing to the similarity between pasted region and copied region, descriptors are then matched between each other to seek for any possible forgery in images.

Hwei-Jen Lin et. al. [15] proposed a method for detecting copy-move forgery over images tampered by copy-move. The given image is divided into overlapping blocks of equal size, for resisting against various modifications and improving the efficiency for sorting feature vectors, they represented each block B of size b × b (= 16×16) by a 9-dimensional feature vector vB = (x1, x2, …, x9). Firstly, the block B is divided into four equal-sized sub-blocks, S1, S2, S3, and S4, as shown in Figure 3 [15].

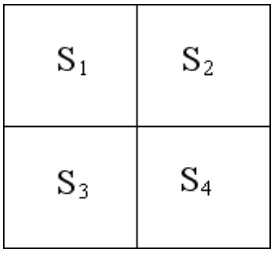
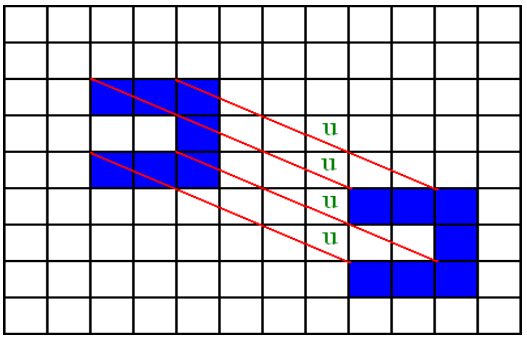


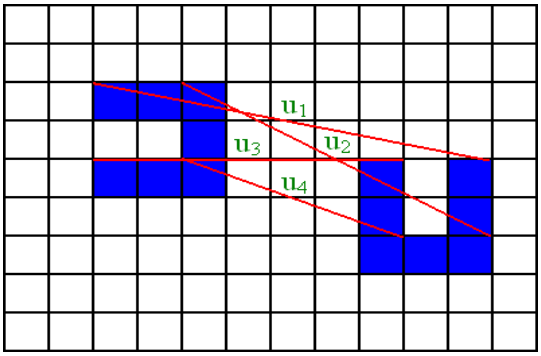
Fig. 3: Block B [15]

The feature vectors are then extracted which store integers. As a result efficient radix sort algorithm is used to perform lexicographical sorting over these vectors [15]. The difference (shift vector) of the Positions of every pair of adjacent feature vectors in the sorting list is computed. After evaluation of the accumulated number of each of the shift vectors, duplicated region is detected with presence of large accumulated number and thus all the feature vectors corresponding to the shift vectors with large accumulated numbers are detected, whose corresponding blocks are then marked to form a tentative detected result. The figure 4 [15] shows duplicated region with and without rotation. Final results are obtained from tentative detected result by medium filtering and performing connected component analysis.

Compared with other methods, employing the radix sort makes the detection much more efficient without degradation of detection quality. The total time for sorting the feature vectors was reduced to O(9k). According to their experimental results, the scheme performed well when the degree of rotation was 90, 180 and 270 degree. But the method failed to detect all copied region of smaller size. Although duplicated regions with rotation through some fixed angles can be detected, the method does not deal with rotation arbitrary angles.



(A)



(B)

Figure 4: (A) Duplicated regions form several identical shift vector u. (B) A region is copied, rotated through 90 degrees, and pasted to another region[15].

Fourier-Mellin Transform (FMT) was used by Bayram [8] to extract features from the image blocks. These features were not only robust to lossy JPEG compression, blurring, or noise addition, but also known to be scaling and translation invariant. They used lexicographic sorting method and compared the robustness of their features with the ones utilized in [2], and [3]. Counting bloom filters, instead of lexicographic sorting was experimented to reduce the sorting time. In their paper, the authors showed that their technique was robust to compression up to JPEG quality level 20 and rotation with 10 degree and scaling by 10%.

Seung-Jin Ryu [9] proposed a detection method of copy-move forgery that localizes duplicated regions using Zernike moments. Since the magnitude of Zernike moments is algebraically invariant against rotation, the method can detect a forged region even though it is rotated. They have proposed copy-rotate- move (CRM) detection scheme for a suspicious image. To extract feature vectors of a given block, the magnitude of Zernike moments is calculated. The vectors are then sorted in lexicographical order. The similarity of adjacent vectors investigated. Finally, the suspected regions were measured by Precision, Recall, and F1 – measure [9]. The proposed method was appropriate to identify and localize the CRM region even though the region had been manipulated intentionally. However, in spite of an algebraic invariant of rotation, detection errors occurred due to the quantization and interpolation error. Their method is still weak against scaling or the other tampering based on affine transform.

From the research related to copy move manipulation detection we can summarize the important steps to configure the copy move detection Technique. They are as follows:

1. The tampered image which is the input image to the detection system is first divided into overlapping blocks of equal size.
2. These blocks are then represented in form vectors by feature extraction of each block. For feature extraction we have seen different approaches such as DCT[3], PCA[3], SVD[5], DWT[1,5], FMT[8], SIFT[7] and many more.
3. Further they are lexicographically sorted to locate the manipulated region in the image due to copy move by obtaining a match.

Depending upon the number blocks, the methods used to represent these blocks in form of (feature) vectors, no. of vectors and the different sorting methods used, the computational time varies for different approaches.

IV. CONCLUSION

With continuous development in Image editing software, doctored photographs are appearing with a growing frequency and sophistication. Therefore there is an urgent need to develop computational efficient techniques. As Copy-Move forgeries is the most common image manipulation, the detection technique for the same is necessary. As discussed in this we have come across many passive approaches made to detect copy move forgery, some have made significant progress in detection, but there are yet many challenges where the images are manipulated by adding noise, by compressing, by rotation, by retouching or scaling the image. We have discussed the progress of copy move manipulation techniques. With growing curiosity in copy move manipulation, more exploration is required in this area.

REFERENCES

[1] Yagiz Sutcu, Baris Coskunand Husrev T. Sencar, Nasir Memon. ‗Tamper detection based on regularity of wavelet transform coefficients' International Conference on Image Processing ICIP 2007.

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

[3] A.C. Popescu and H. Farid, ―Exposing digital forgeries by detecting duplicated image regions,‖ Dept. Comput. Sci., Dartmouth college, Tech. Rep. TR2004-515, 2004.

[4] Copy-Move Forgery Detection Algorithm for Digital Images and a New Accuracy Metric, Tehseen Shahid, Atif Bin Mansoor.

[5] 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.

[6] 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, 2007, pp. 371-377.

[7] W. Luo, J. Huang, and G. Qiu, ―Robust detection of region-duplication forgery in digital images,‖ in Proc. Int. Conf. on Pattern Recognition, Washington, D.C., 2006, pp. 746–749.]

[8] Sevinc Bayram, Taha Sencar, and Nasir Memon, ―An efficient and robust method for detecting copy-move forgery,‖ in Proceedings of ICASSP *2009*, 2009.

[9] 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

[10] Hany Farid' Image Forgery Detection A survey' IEEE Signal Processing Magazine march 2009, Digital Object Identifier 10.1109/MSP.2008.931079

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

[12] P. Meerwald and A. Uhl, ―A Survey of Wavelet-Domain Watermarking Algorithms,‖ in Proceedubgs of SPIE, Electronic Imaging, *Security and Watermarking of Multimedia Contents*, Vol. 4314, 2001, pp. 505-516.

[13] M. S. Wang and W. C. Chen, ―A Majority-Voting based Watermarking Scheme for Color Image Tamper Detection and Recovery‖, *Computer Standards & Interfaces*, Vol. 29, Issue 5, 2007, pp. 561-570.

[14] P. L. Lin, C. K. Hsieh, and P. W. Huang, ―A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery, *Pattern Recognition*, Vol. 38, Issue 12, 2005, pp. 2519-2529.

[15] 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.

[16] B. Mahdian and S. Saic, ―Detection of copy move forgery using a method based on blur movement invariants,‖ Forensic Sci. Int., vol. 171, pp. 180–189, 2007.

[17] S. Katzenbeisser and F. A. P. Petitcolas, Information Techniques for Steganography and Digital Watermarking. Norwood, MA: Artec House, 2000.

[18] H. Gou, A. Swaminathan, and M. Wu. Noise features for image tampering detection and steganalysis.In IEEE International Conference on Image Processing, San Antonio, TX, 2007.

[19] J. He, Z. Lin, L. Wang, and X. Tang. Detecting doctored JPEG images via DCT coefficient analysis.In European Conference on Computer Vision, Graz, Austria, 2006.

[20] [Y-F. Hsu and S-F. Chang. Image splicing detection using camera response function consistency and automatic segmentation. In International Conference on Multimedia and Expo, Beijing, China, 2007.

[21] M.K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting. In ACM Multimedia and Security Workshop, New York, NY, 2005.

[22] M.K. Johnson and H. Farid. Detecting photographic composites of people. In 6th International Workshop on Digital Watermarking, Guangzhou, China, 2007.

[23] M.K. Johnson and H. Farid. Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security, 3(2):450–461, 2007.