http://dx.doi.org/10.14257/ijsip.2016.9.2.35

A Survey of Digital Image Tampering Techniques

Nishtha Parashar[1], Nirupama Tiwari[2], Deepika Dubey[3]
[1,2,3]Computer Science & Engineering Dept., SRCEM, Banmore
nishtha2909@gmail.com[1], girishniru@gmail.com[2], deepika.sa1304@gmail.com[3]

Abstract

Due to powerful computers and advanced photo-editing software tools the manipulation of images has become an easy task. Confirming the authenticity of images and detecting tampered regions in an image without any knowledge about the image content is an important part of the research field. An effort is made to survey the recent advancements being made in the field of digital image forgery detection and thus passive methods for forgery detection are being presented. Blind or passive methods do not require any explicit former information about the image. In the first part, various image forgery detection techniques are classified and then an overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed

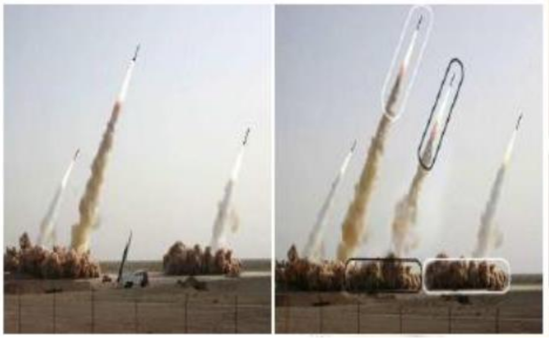
Keywords: *passive/blind forgery detection techniques, dyadic wavelet transform, image tampering, copy-move forgery*

1. Introduction

The present day digital revolution has changed the format of accessing, manipulating and sharing information, however these developments have also given rise to different security issues. Complex digital technology and various photo-editing software like Adobe Photoshop *etc*. are universal and have made the task of forging images a common practice.

Complex digital technology and different photo-editing software, such as Adobe Photoshop, are universal and thus have made the process of manipulating images to create forgeries a fairly common practice. As a result, trust in digital imagery has been eroded.

An example of digital forgery was seen in a Tunisian newspaper in which a photo was altered duplicating the crowd to appear large [9]. Another example as shown in Figure 1 displays the altered photograph released by Iran showing four missiles instead of three [2]. This tampered image was also being published by various western media including The New York Times. The research in this thesis attempts to address this need and provide some insight into this challenging problem.



(a) Original Image (b) Forged Image

Figure 1. Example of Copy-Move Forgery[2]

ISSN: 2005-4254 IJSIP

2. Image Tampering

Image tampering is defined as “adding or removing important features from an image without leaving any obvious traces of tampering” and thus image tampering is considered as intentional manipulation of images for malicious purposes [5]. There are various techniques for counterfeiting images and these can be classified into three broad categories.

Copy-Move attack, also called Cloning, is a technique in which instead of having an external image as the source, it uses portion of the original base image as its source. Therefore, the source and the destination of the modified image originate from the same image. Photoshop Clone Stamp Tool can be used to achieve such type of forgery. Blurring is usually applied along the border of the modified region to reduce the effect of irregularities between the original and pasted region.

The second type of image tampering techniques is known as Image-Splicing, which is a technique that involves a composite of two or more images which are combined to create a fake image. Thus, by sticking together photographic images a spliced image is being obtained.

And the third category of image tampering technique is known as Image-Retouching in which certain features of image are being enhanced or reduced in order to make the image more attractive. Thus, this type forgery is considered less harmful and is used mostly by the magazine editors.

3. Techniques to Counter Attack Forgery

To detect above mentioned digital forgeries in images two principle approaches are taken into account namely, **Active approach** and **Passive approach.**

In active approach, during the creation of images pre-processing techniques like watermark embedding or signature generation are applied which limit the use of images in general. However, there are millions of digital images on internet which are without any digital watermark or signature. In this context *active approach* could not be used to find the authenticity of the image.

Therefore unlike the active approach, the passive approach does not need any embedded watermark or digitally generated signature. Mainly three techniques are widely used to tamper digital images namely Copy-Move, Splicing and Retouching as shown in Figure 2.

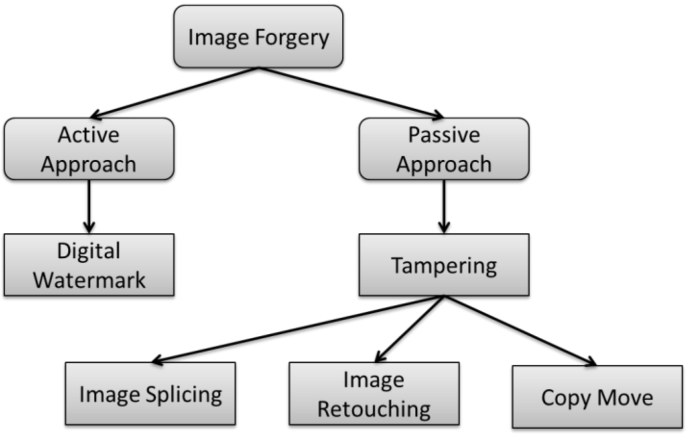


Figure 2. Classification of Image Forgery

4. Literature Survey

Akhilesh Kumar Yadav *et. al*., [7] introduced a method for detecting copy-move forgery which is one of the difficult types of forgery This method is good at some manipulation/attack like JPEG compression, rotation, Gaussian noise, smoothing, scaling etc. The image is partitioned into blocks and exact matches are made between patterns of different blocks and then results are calculated using Discrete Wavelet Transform (DWT).

Yongzhen Ke, Qiang Zhang *et. al.*, [14], in this paper, a detection method is proposed to effectively locate image forgeries by detecting inconsistency of image noise variance on the saturation component of HSV color space. The image is first converted to HSV color space from RGB color space. Then, the images were divided into blocks of different sizes and 100 forged images were randomly cropped at different locations from the images for each size and white Gaussian noise was added. The evaluation results demonstrate that the noise estimation for image blocks with size of 32×32 achieve the best results. However the drawback was that the noise estimation for 16x16 and 64x64 pixels images was poor.

Vijay Anand *et. al.*, [17] proposed dyadic wavelet transform (DyWT) in combination with scale invariant feature transform (SIFT) to detect copy-move forgery. Firstly, DyWT is applied on the given test image which decomposes the image into four sub-bands LL, LH, HL, HH. Then, to extract the features of the image SIFT is applied on the LL part only as it contains the maximum information. Using these key features the descriptor vector is obtained and similarities are find out between them in order to find the tampered region on the given image. The drawback of this method is that it is not robust to the angles defining the camera axis orientations for image.

Jian Wu *et. al.*, [18] has provided a comparative and systematic analysis of SIFT and its family, including PCA-SIFT, GSIFT, CSIFT, SURF and ASIFT. The performance is measured and time consumption is calculated in different situations. The results concluded that each algorithm has its own advantages.

Nirupma Tiwari *et. al.*, [8] proposed a method for tampering detection in which the original image is divided into overlapping blocks and for each block number of connected components are calculated. By calculating the difference between vectors of the original and tampered image the location of tampering is detected and measured. However the drawback of this method is that it is applicable on similar sized square images only. In future it can be extended to different sized images.

Ghulam Muhammad *et. al.*, [18], proposed a blind method for copy move image forgery detection using undecimated dyadic wavelets. Due to shift invariant nature, the dyadic wavelet transform (DyWT) is more appropriate for data analysis than discrete wavelet transform (DWT). The image is decomposed into LL1 and HH1 subbands. Then both the subbands are divided into overlapping blocks and similarity between the blocks is calculated. The key idea of this method is that the similarity between the copied and moved blocks from the LL1 subband should be high, while that in the HH1 subband should be low due to noise inconsistency in the moved block.

Pradyumna Deshpande and Prashasti Kanikar [13], introduced two important techniques for pixel based forgery detection. A technique for copy-move forgery detection is discussed. But this approach takes into account only shifting of copied regions. So, another technique is discussed for fast-copy-move detection.

In the first technique DWT transformation is being applied and then the image is divided into sub-images. The shifted region is located by comparing the pixels. However no noise is detected and no filtration is applied. And thus, the first algorithm for copy-move is effective for detection when the region is pasted without any change (scaling or rotation) to another location in the image.

In the second technique first the image block is subdivided and then processed. The feature vectors are compared It takes more issues like rotation and noise removal under consideration and achieves a very good detection rate.

Cao Y, Gao T and Fan L, Yang Q [15], proposed method of Circular Block with DCT which provides perfect detection of tampered region for uniform background images, non-regular duplicate regions, and high resolution images. Also it detect multiple copies - move. However the drawback of this method is that it has poor performance with poor image quality and is not robust to geometrical operations.

Vincent Christlein *et. al.*, [12], proposed a rotation-invariant selection method, which is called as Same Affine Transformation Selection (SATS). It shares the benefits of the shift vectors at an only slightly increased computational cost. As a by-product, the proposed method explicitly recovers the parameters of the affine transformation applied to the copied region. The results show that SATS outperforms shift vectors when the copied region is rotated, independent of the size of the image.

S. Ryu, M. Lee and H. Lee [16], proposed a copy-rotate-move (CRM) detection scheme based on Zernike moments which help in reduction of JPEG compression, blurring and additive white Gaussian noise. Also, method can detect forgery even on the rotated region since Zernike moments are algebraically invariant to rotation. However, the disadvantage of this method is that it is still weak against scaling and tampering based on affine transform.

5. Conclusion

In this paper we survey and analyse different techniques to detect forgery in image. The techniques discussed above are useful for detecting cut and paste type forgeries. Thus extensive survey is done in this paper to detect duplication in images and provides future enhancement directions in the area of image forgery detection.

References

[1] R. C. Gonzalez and R. E. Woods, “Digital Image Processing”.

[2] http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/

[3] Image Processing by Dr. Nidaa F Hassan.

[4] Ms. P. G. Gomase and Ms. N. R. Wankhade, “Advanced Digital Image Forgery Detection: A Review”, International Conference on Advances in Engineering & Technology-2014, e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 80-83.

[5] V. P. Raval, “Analysis and Detection of Image Forgery Methodologies”, International Journal of Scientific Research and Development 2013, vol. 1, Issue 9, **(2013)**.

[6] S. Ryu, M. Lee and H. Lee, “Detection of copy-rotate-move forgery using zernike moments”, in Proc. Int. Workshop Information Hiding, Springer, **(2010)**, pp. 51–65.

[7] A. K. Yadav, D. Singh and V. Kumar, “Forgery (Copy-Move) Detection In Digital Images using Block Method”, International Journal of Collaborative Research in Engineering Sciences, **(2014)** April.

[8] N. Tiwari, N. Hemrajani and M. K. Ramaiya, “A Novel Technique For Tampering Detection”, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN 2249-6831, vol. 3, Issue 3, **(2013)** Aug, pp. 341-346.

[9] Resmi Sekhar and Chithra A S, “Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images”, International Journal of Computer Applications March 2014, Volume 89 – No 8, March 2014.

[10] Farid, H. and A. Popescu, “Exposing Digital Forgeries by Detecting Traces of Resampling.”Proceedings of the IEEE Transactions on Signal Processing. (In Press). 2004.

[11] Fridrich, J., J. Lukas, and D. Soukal, “Detection of Copy-Move Forgery in DigitalImages.” Proceedings of DFRWS 2003. Cleveland, OH, August 2003.

[12] Christlein V, C Riess, E Angelopoulou, "On rotation invariance in copy-move forgery detection ", IEEE International Workshop on Information Forensics and Security (WIFS), 2010.

[13] Pradyumna Deshpande, Prashasti Kanikar, “Pixel Based Digital Image Forgery Detection Techniques” International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 539-543.

[14] Yongzhen Ke, Qiang Zhang, Weidong Min and Shuguang Zhang, " Detecting Image Forgery Based on Noise Estimation" International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.1 (2014), pp.325-336.

[15] Cao Y, Gao T, Fan L, Yang Q., "A robust detection algorithm for copy-move forgery in digital images", Forensic Sci Int. 2012 Jan.

[16] S. Ryu, M. Lee, H. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Proc. Int. Workshop Information Hiding, Springer , pp. 51–65, 2010.

[17] Vijay Anand, Mohammad Farukh Hashmi, and Avinash G. Keskar , "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods", Springer International Publishing Switzerland pp. 530–542, 2014.

[18] Ghulam Muhammad, Muhammad Hussain , George Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform",Elsevier doi:10.1016/j.diin. 2012.04.004.

[19] Jian Wu, Zhiming Cui, Victor S.Sheng, Pengpeng Zhao, Dongliang Su, Shengrong Gong, "A Comparitive Study of SIFT and its Variants", Measurement Science Review, Volume 13, No.3, 2013.