Survey of Digital Image Tampering Techniques

Yash Parashar
Research Scholar, M.tech (Computer Science& Engineering)
ITM Group of Institutions, Gwalior (M.P.), India.

Shirish Mohan Dubey
Asst. Professor, Department of Computer Science and Engineering
ITM Group of Institutions, Gwalior (M.P.), India.

Abstract – In this time of modern technology the manipulation in the digital image is very easy and common as well. An image can be tampered easily with the help of photo editing software like Photoshop in a very advanced way. The motive of this research is to detect and confront the authenticity of the image, and if the image has been forged or tampered then detecting the tampered region of the image. We put our efforts to make a survey about the recent achievements and discoveries in the field of digital image forgery detection and hence, we are going to present the passive method of image forgery detection. First we will get the overview or introduction to detect the various types of image forgery and then we will come to the introduction of passive image authentication. It will also present the overview of previously existing passive image forgery detection or also known as blind image forgery detection.

Index Terms – Digital Image, Forgery Detection.

1. INTRODUCTION

In this present day, it will not be wrong to say that this is the era of science and the new discoveries are taking place every single day. In the digital world of photography various powerful camera instruments with high resolution lenses are providing the results exceed - expectation. To filter those captured images for better quality some advanced tools and software are being used such as Adobe Photoshop. With the help of these software the editing in the image and carrying out the changes and manipulation becomes far easier. The major drawback of this is that we can lose the integrity and the authentication of the original images. The contents of the real image can be easily changed [1]. The impact of these software is that we are losing our trust in the digital image world or it has been faded.

There are numerous examples such as; there was an image of a newspaper in which there was the duplicity of the crowd had been displayed to appear larger. We can see another example in figure 1. An altered photograph was released by Iran. There were only 3 missiles in the original but in the alteration it becomes 4. This altered image of missile was published in the various cities including New York. The research which we are proposing in this thesis is to help us in the addressing of forgery in this challenging environment.

(a) Original Image (b) Forged Image

Figure 1 Example of copy-move forgery [11]

2. RELATED WORK

S. Ryu, M. Lee and H. Lee [2], 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.

Yongzhen Ke Qiang Zhang et.al [9] proposed in this research a method for the detection of image forgery by the detection of inconsistency in the variation of image noise on the saturation component of HSV colour space. From RGB colour space image is converted into HSV colour space. Various sizes of blocks are created by dividing images and then adding white Gaussian noise on the randomly cropped 100 forged images at various locations from the image for every size. The best results were achieved by noise estimation for image blocks having size 32 x 32. Yet noise estimation for 16 x 16 and 64x 64 pixels images proved to be poor.

Vijay Anand et.al [11] proposed a method of the combination of scale in variant feature transform (SIFT) and Dyadic

Wavelet Transform (DyWT) for the detection of copy move image forgery. First we apply the DyWT to the forged image. It divides the image or sub bands it in four major components LL, LH, HL, and HH. Now to extract the features of the image we apply the SIFT on the LL part of the image which contains the maximum information of the image. To locate the tampered region on a given image the descriptor vector is obtained with the help of these key features and hence the similarities are identified between them. However there is a disadvantage associated with this method. It is not robust to the angles which define the orientation of camera axis for the image

Mohammad Farukh Hashmi et.al [14], proposed a method to detect copy-move forgery in images. Image is decomposed using DWT into four sub-bands then, SIFT is applied on LL part only and descriptor vector is found for given key features. To check whether image is forged or not a match between various descriptor vectors is made.

Ghulam Muhammad et.al [12], suggested blind technique for the detection of copy move forgery in images via un-decimated dyadic wavelets. Due to shift invariant nature, the dyadic wavelet transform (DyWT) is more suitable for data examinations compare to discrete wavelet transform or DWT. The image is disintegrated into LL1 and HH1 sub bands. Then together the sub bands are divided into overlying blocks and similarity between the blocks are calculated. The main idea of this process is that the similarity between the copied and the moved blocks from the LL1 sub band must be high, while that in the HH1 sub band should be low due to noise variation in the moved block.

Vincent Christlein et.al [15], proposed a rotation-invariant selection method, which is called as Same Affine Transformation Selection (SATS). It provides the benefits of the shift vectors at an only slightly increased computational cost and can handle rotation directly. Also, 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. The main idea is to explicitly estimate the rotation and scaling parameters from a few blocks, being expressed as an affine transformation matrix.

3. IMAGE TAMPERING

To edit the important contents of the original image like to add some contents from different images and to delete or erase some content of the original image is considered as image tampering. It is being used very commonly all over across the world. It can be categorized in various forms but there are three major categories in which they can be classified.

- Copy-move
- Image Splicing
- Image Retouching

Copy-move – This attack is also known as cloning. In this process some specific portion of the image has been replaced by some different portion of the image. It creates the duplicity of the content in the image. With the help of 'Clone Stamp tool' of Photoshop such type of forgery can be easily achieved.

Image splicing – In this process the various contents of the different images are put together in a single image. This technique of splicing the different images and putting it all together is called image splicing.

Image retouching – The process of image forgery is generally used for making the image attractive by altering the contrast, brightness, levels etc. it is considered as very less harmful as compared to the others and mostly used in magazines.

4. METHODS TO COUNTER ATTACK FORGERY

To detect the previously mentioned forgeries in the digital image there are two approaches which are being used.

The active approach works over the images during the creation of the image and authenticated with the help of watermark or the generation of the signature. But this approach cannot fulfil the expectations because there are millions of images available on the internet without any watermark or signature. So in these cases this approach cannot work to discover the authenticity of the image.

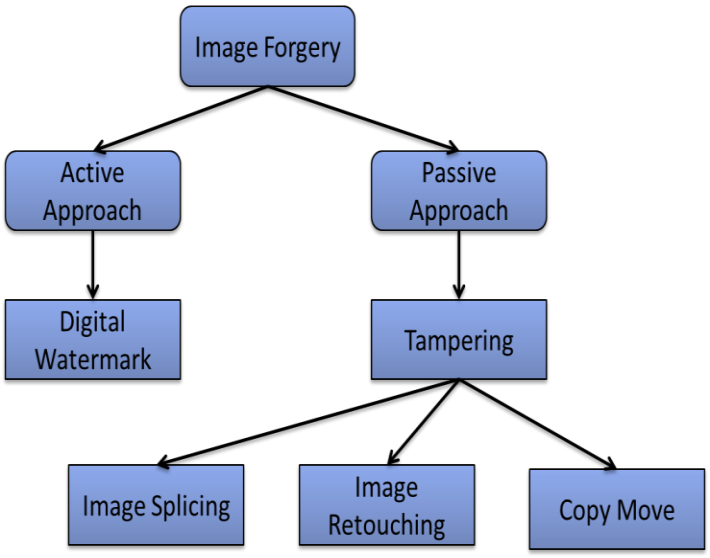

Figure 2 Classification of Image Forgery.

5. CONCLUSION

Herein this paper we review and analyze various techniques to identify forgery in image. The techniques or method deliberated above are beneficial for sensing forgeries based on cut and paste. 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] Ms.P.G.Gomase, Ms. N.R. Wankhade, "Advanced Digital Image Forgery Detection: A Review", International Conference on Advances in Engineering & Technology, 2014, pp. 80-83.
[2] S. Ryu, M. Lee, H. Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments" in Proc. Int. Workshop Information Hiding, Springer , 2010, pp. 51–65.
[3] Cao Y, Gao T, Fan L, Yang Q., "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images", Forensic Sci Int. 2012 Jan.
[4] 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.
[5] Farid, H. and A. Popescu, "Exposing Digital Forgeries by Detecting Traces of Resampling."Proceedings of the IEEE Transactions on Signal Processing. (In Press). 2004.
[6] Fridrich, J., J. Lukas, and D. Soukal, "Detection of Copy-Move Forgery in DigitalImages." Proceedings of DFRWS 2003. Cleveland, OH, August 2003.
[7] Christlein V, C Riess, E Angelopoulou, "On Rotation Invariance in Copy-Move Forgery Detection ", IEEE International Workshop on Information Forensics and Security (WIFS), 2010.
[8] 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.
[9] 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.
[10] S. Ryu, M. Lee, H. Lee, "Detection of Copy-Rotate-Move Forgery using Zernike Moments," in Proc. Int. Workshop Information Hiding, Springer , 2010, pp. 51–65.
[11] 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, 2014, pp. 530–542.
[12] 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.
[13] Jian Wu, Zhiming Cui, Victor S.Sheng, Pengpeng Zhao, Dongliang Su, Shengrong Gong, "A Comparative Study of SIFT and its Variants", Measurement Science Review, Volume 13, No.3, 2013.
[14] Mohammad Farukh Hashmi, Aaditya R. Hambarde, Avinash G. Keskar, "Copy Move Forgery Detection using DWT and SIFT Features", IEEE, 2013.
[15] Christlein V, C Riess, E Angelopoulou, "On Rotation Invariance in Copy-Move Forgery Detection ", IEEE International Workshop on Information Forensics and Security (WIFS), 2010.