International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Digital Image Forgery Detection with Motion Blur as Cue: A Survey

Pornima M. Birajdar[1], N.G. Dharashive[2]

[1]SRTM University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

[2]SRTM University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

Abstract: ***The extensive availability of sophisticated image editing tools has rendered it relatively easy to produce fake images for malicious purposes in various fields. Image splicing is one of the forms of image forgery and Image splicing detection has been considered as the most challenging problem in passive image authentication. Image forgery affects the characteristics of images such as blurriness, sharpness, noise etc. Introduction of artificial blur while image splicing is very common practice used to reduce degree of discontinuity to hide splicing effects. Using blur estimation blur consistency pattern of an image can be found. Blur factor can be used to detect any splicing possibilities in the image to decide whether it is authentic or forged. The survey covers various image forgery detection techniques with blur as cue.***

Keywords: Image forgery, Blur, Motion blur estimation, Splicing detection.

1. Introduction

Today's technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago. Web based large amount of digital contents such as image, video, audio have been the most popular service on internet. However the widespread availability of photo manipulation software has made it effortless task for illegal duplication and tampering of distributed content on internet which may cause some troubles or some economic loss to digital content provider. For example, [1] the image in Figure 1, this photograph was widely circulated via e-mail, supposedly having been obtained from a camera found in the debris of the World Trade Center buildings after the attacks of September 11, 2001. The approaching aircraft in the background seems to imply that this image was captured mere seconds before the impact. However, this image is clearly fake. There are many clues within this photograph that help decide that it is a hoax. *A priori* knowledge may be employed to prove that this image is unauthentic. For example, geographical knowledge or information about the type of aircraft involved in the attacks can be used to dismiss this image as fake. Even in the absence of such knowledge, as the camera is focused on the person, the aircraft should have appeared blurred in the image, due to its speed. The complete absence of motion blur of aircraft in this image indicates a possible forgery.

Figure 1: Forged "Tourist Guy" image allegedly captured on September 11, 2001.

Thus, digital image forgery detection has recently received significant attention of the researchers. At least two trend account for this: the first accepting digital image as official document has become a common practice, and the second the availability of low cost technology in which the image could be easily manipulated. [2]Following are the digital image tampering techniques categories;

1. Copy and Move Forgery
2. Image Splicing
3. Image Retouching

Forgery detection techniques for each of these categories can be implemented with two approaches: Active approach makes use of prior information associated with the problem image for forgery detection. Passive approach is more challenging for forgery detection as neither any visual clues nor any prior information is available with the problem image indicating the tampering.

Source identification, forgery detection, and detection of computer generated images, are some of the problem areas in blind image forensics. Image splicing detection methods can be region based and edge based. [3]Set of image forensic tools can be roughly grouped into five categories as shown in Table 1.

Table 1: Set of image forensic tools.

Techniques Based on	*Factors Considered*
Pixel	Statistical anomalies introduced at pixel level
Format	Lossy compression scheme, JPEG quantization, Double JPEG, JPEG blocking
Camera Response Function (CRF)	Artifacts introduced by camera lens, sensor, color filter array.
Physics	Light direction 2D, 3D, lighting environment
Geometric	Measurement of object in the world and their positions relative to camera.

The paper contributes how blurring can be used to detect image forgery.

2. Related Work

2.1. Motion Blur

Blur is one kind of opacity in an image, so it is focused for image forgery (splicing) detection. Motion blur occurs in image due to camera shake or fast moving subjects during image capturing. Primarily considering magnitude and direction of blur, artificial blur can be generated. Blur operation is used often to reduce the degree of discontinuity to hide splicing effects or to give real situation effect using artificial blur. Artificial blurring changes the blur consistency pattern of original image and identifying blur inconsistencies in whole forged image can aid to detect image forgeries.

An image can have different types of blurs such as Defocus blur, Motion Blur, Out-of-focus blur. Blur can be introduced in a region or at the edges, therefore different techniques detecting blur inconsistencies are categorized as Edge based, Region based, Edge-cum-Region based. [4]Motion blur retains some information about motion. There are various motions of blur like space invariant, linear, rotational, space variant, affine motion from blur. For image splicing detection with motion blur as cue, blur estimation of an image is essential and which can be computed using various blur detection techniques like DCT (Discrete Cosine Transform), Wavelet transform, Radon transform, Cepstral method. Some examples of motion blur and defocus are represented in Figure 2.

(a)

(b)

Figure 2: Types of blur (a) Motion blur and (b) Out of focus blur

2.2. Motion Blur Estimation

Motion blur consists magnitude and direction in an original image. Blur operation reduces the joint consistency of color channel in the image. Most of the image forgery detection methods based on blur inconsistencies use blur estimation metric to measure the amount of blurriness in the tampered image. To assess image quality by human himself is a time consuming, inconvenient, and expensive process. There is a need to automate image quality assessment methods. Image quality assessment techniques are perceptual and non perceptual. Perceptual technique predicts image quality in terms of blurriness amount whereas non perceptual predict automatically. Non perceptual technique ensures assessment accuracy but with more time complexity.

[5]To extract motion blur parameters, convert blurred image into frequency domain. Periodic patterns in frequency domain estimates the motion blur parameters. The point spread function (PSF) has two important parameters, i.e., motion direction and motion length. The estimation of these parameters is important splicing detection. Wavelet transform is more effective to detect edges than other edge detection techniques as it uses horizontal, vertical and diagonal coefficients at different scale to detect edges. The Harr Wavelet Transform (HWT) discriminates different types of edges as well as can recover sharpness from the blurred version image. It also determines whether an image is blurred or not and to what extent if it is blurred. Gradient vector based PSF estimation is used for out of focus blurred images. The motion blur detection scheme using support vector machine (SVM) can classify the digital image as blurred or sharp. Statistics of the natural scenes and adopted multi-resolution decomposition methods can be used to extract motion blur features to train and test probabilistic support vector machine. In cepstrum domain, motion blur can be separated from blurred image using motion blur parameters. Radon transform is used to search characteristics of motion blur in cepstrum domain. Motion blur is estimated using cepstrum, Radon transform, Hough transform, or Wavelet transform.

Figure 3: Direction of Motion Blur

2.3. Image Splicing Detection

An overview of image forgery detection technique is as shown in figure 4, where input image is divided into blocks and block wise blur is estimated, variation in blur metric parameter segments the forged region.

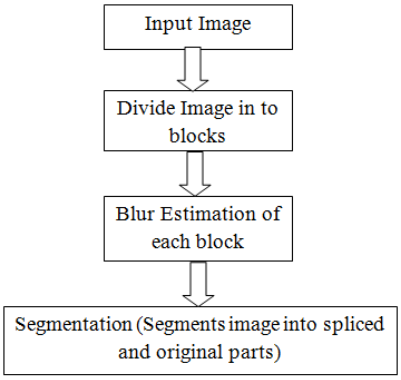

Figure 4: Overview of Image Forgery Detection

There are various methods for image splicing detection with blur as cue. Author of [1] proposed effective image splicing detection model based on discrepancies in motion blur, where image is subdivided into blocks, for each block motion blur parameter is estimated, and segmentation separates spliced region in the image. Spectral matting of component of the image which estimates motion blur effectively detects splicing forgery and gives better inconsistent region interpretation for user. The limitation of this method is, it is slower than DCT based technique and requires more number of steps. Restoration of a degraded image from motion blurring is highly dependent on the estimation of the blurring kernel. Most of the existing motion deblurring techniques model the blurring kernel with a shift-invariant box filter, which holds true only if the motion among images is of uniform velocity.

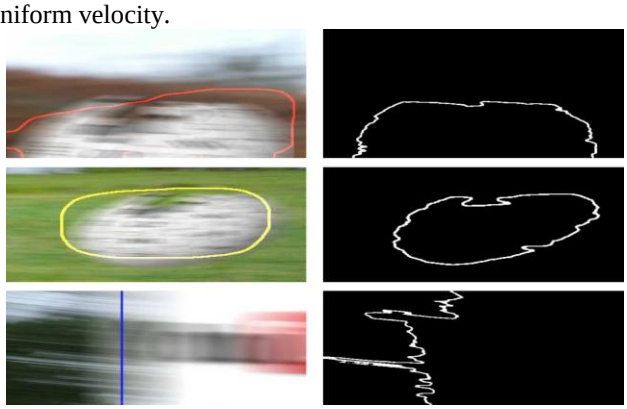

Figure 5: Detection of spliced blurred regions. Left column: Forged images with segmentation outputs. Right column: Ideal segmentations

In [4], S. Dai and Y. Wu has been proposed segmentation of an image into various regions depending on the estimated blur model of each pixel. This model gives different motions from blur like space variant, space invariant, linear, non linear, rotational, local. H.Ji and C.Liu, [6] presented a spectral analysis of image gradients, which leads to a better configuration for identifying the blurring kernel of more general motion types (uniform velocity motion, accelerated motion and vibration) and hybrid Fourier-Radon transform to estimate the parameters of the blurring kernel with improved robustness to noise over available techniques. W.Wang and F. Zeng have presented a technique for detecting spliced blurred images through blind image restoration. This technique first estimates the blur parameters from the cepstrum of suspected image, then restores the given image based on constructed blurring kernel. D.Hsiao and S. Pei[7] introduced the method of DCT coefficient and optimal morphological operation to detect blurred region. The digital forensic to detect content tampering is a typical application of safety digital content management. Based on the edge processing and analysis using edge preserving smoothing filtering and mathematical morphology, blur edge detection scheme is proposed by L.Zhou, D.Wang *et*[8]. X.Wang and S.Peng [9] proposed Defocus model to detect defocus inconsistencies. It is robust in photofinishing and scanning. M.P.Rao *et*[10] proposed a passive method to automatically detect image splicing using blur as a cue. Specifically, they addressed the scenario of a static scene in which the cause of blur is due to hand shake. Existing methods for dealing with this problem work only in the presence of uniform space-invariant blur. In contrast, their method can expose the presence of splicing by evaluating inconsistencies in motion blur even under space-variant blurring situations.

3. Conclusion

In this paper we have presented review approaches which use discrepancies in motion blur to detect image forgeries. To accomplish this, primarily blur estimation amount is considered. Such motion blur is estimated using different blur estimation metrics. Considering this blur as cue, forged region in image is segmented. But above mentioned

techniques have some limitations that may be challenge for researchers explore new ideas and provide new solutions.

References

[1] Pravin Kakar, Sudha Natrajan, Wee Ser, " Exposing Digital Image Forgeries by detecting discrepancies in Motion Blur" in IEEE Transactions On Multimedia, June 2011, Vol.13.
[2] T Qazi, K Hayat, I Khan, " Survey on blind image forgery detection" in IET Image Process., 2013, Vol. 7, pp. 660–670
[3] Hany Farid, "Image Forgery Detection" in IEEE SIGNAL PROCESSING MAGZINE , March 2009.
[4] S. Dai and Y. Wu, "Motion from blur, " in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2008, pp. 1–8.
[5] Shamik Tiwari, V. P. Shukla , Ajay Kr. Singh , " Certain Investigations on Motion Blur Detection and Estimation"
[6] H. Ji and C. Liu, "Motion blur identification from image gradients, " in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2008, pp.1–8.
[7] D. Hsiao and S. Pei, "Detecting digital tampering by blur estimation, " in Proc. 1st IEEE Int. Workshop Systematic Approaches to Digital Forensic Engineering, 2005, pp. 264–278.
[8] L. Zhou, D. Wang, Y. Guo, and J. Zhang, "Blur detection of digital forgery using mathematical morphology, " Lecture Notes Computer. Sci., 2007, vol. 4496, pp. 990–998 .
[9] Xin Wang , Bo Xuan , Si-long Peng , "Digital Image Forgery detection based on the consistency of defocus blur" in IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.
[10] M.P.Rao, A.N.Rajgopalan, "Harnessing Motion Blur to Unveil Splicing", IEEE Transactions on Information Forensics And Security, April 2014 VOL. 9.

Author Profile

P.M. Birajdar received the B.E. degree in Computer Science and Engineering from M.S. Bidve Engineering College in 2009. Now, she is pursuing Master's in Engineering (Computer Science and Engineering) from M.S. Bidve Engineering college, Latur , SRTM University Nanded, Maharashtra..

N. G. Dharashive received the B.E. and M.E. degrees in Computer Science & Engineering from M.B.E.Society's College of Engineering, Ambajogai in 2001 and from Government College of Engineering, Aurangabad in 2011, respectively. He is pursuing Ph.D in Image Processing from S.R.T.M.University, Nanded (M.S.). He is now with M.S.Bidve Engineering College, Latur (M.S.) as Assistant Professor since 2002.