ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Review On Different Image Splicing Techniques

Manisha Pansare, Prof. Suchita Walke, Prof. Vanita Mane

M.E. Student, Department of Computer Engineering, YTCEM, Bhivpuri Road, Mumbai, India

Assistant Professor, Department of Information Technology, YTCEM, Bhivpuri Road, Mumbai, India

Assistant Professor, Department of Computer Engineering, RAIT, Nerul, Navi Mumbai, India

ABSTRACT: The digital images are being used over the past few years to spread a message. Hence the need of image authentication is increased. Preserving image authenticity is very complex because image editing software is easily available. Since photo manipulation software is easily available, has made it unprecedentedly easy to manipulate images for malicious purposes. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. Image splicing or image composition is the one of the most common forms of digital image or photographic manipulation operation. Image splicing is a process that crops and pastes regions from same or separate sources to produce composite image called spliced image. This type of forgery is a challenging issue from tamper detection point of view. In this paper, we analyze the image forensic techniques for detecting digital image splicing using 3-D lighting environments and detecting discrepancies in motion blur.

KEYWORDS*:* Image Forensic, image forgery, image splicing, image forgery detection, motion blur Estimation, passive method

I. INTRODUCTION

Digital Image Forensics is a rising branch of image processing. It deals with the authentications and integrity of the images [1]. One of the important tasks of image forensics is image tampering or forgery detection. Tampering means to interfere with something to make unauthorized alterations or cause damage. Since the low-cost hardware and software tools are easily available, makes it easy to create, alter, and manipulate digital images with no obvious clues [2].Such software can do an alteration in digital image by modifying the blocks of an image without showing the effect of the modification which cannot be noticed by human eyes easily in the forged image [4]. Hence it is possible to distinguish whether a given digital image is original or a fake version. Since the digital images are used in many social areas like newspapers, magazines, websites and televisions, digital images are important tool for communication and courts where they are used as evidence, the digital image forgery detection is very important field in image processing.[3]

Applications of Digital Image Forensic

- Digital forensics is used in both criminal law and investigation of private information.
- Digital Forensic examines the images on online social networks like websites etc.
- Used for detecting tampering or forged image.
- Image forgery detection system is very important in many fields to protect copyright and prevent forgery or alteration of images which is applied in various areas like digital forensic science, journalism, scientific publications, surveillance systems, multimedia security etc.

Classifications of Approaches

Digital image forgery detection techniques are basically classified into two approaches such as active and passive approach. [2]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Active Approach

An active approach consists of adding image details in order to describe digital tampering such as name, date, signature, etc. It requires a special hardware implementation to mark the authentication of the digital image.

Techniques of Active Approach

a. Watermarking

Watermarking is used to identify ownership of the copyright in image forgery detection .Watermark must be inserted while creating the image. Once the image/video is created, the watermark will be destroyed so that the authenticator can verify the originality of contents. [2]

b. Digital Signatures

In digital signature the sender can electronically sign the data and the signature is electronically verified by the receiver. The sender owns a private key related to the public key that she has announced publically. To prove that the message is signed by the sender who claims to have sent the message, the receiver uses the sender's public key [2].

Advantage of Active Approach

- Less computational cost.
- Simple if prior information about original image is available.

Disadvantage of Active Approach

- This technique requires a prior knowledge about original image hence is not automatic. It requires some human involvement or specially equipped cameras.
- More than millions of digital images on social network without digital signature or watermark are present. In such scenario this approach could not be suitable to find the authenticity of the image [2].
- In digital signature scheme, for transmission of signature extra bandwidth is needed.

Passive Approach

Passive approach finds the duplicated objects and the amount and the location of forgery in forged images without need of original image, hence is automatic. It depends on traces left on the image by different processing steps while manipulating image. Most of the existing techniques extract features from image and select a suitable classifier and then classify the features. The main objective of passive detection technique is to classify a given image as original or tampered.

Techniques of Passive Approach

1) Pixel-based techniques that detect statistical inconsistencies introduced at the pixel level;

2) Format-based techniques that is based on representing the image as DCT blocks, and quantizing the resulting coefficients. This quantization is the source of the lossy compression in this technique.

3) Camera-based techniques that use the artifacts introduced by the camera lens, sensor, or on-chip post-processing;

4) Physically based techniques that detect anomalies in the three-dimensional interaction between physical objects, light, and the camera;

5) Geometric-based techniques that measures the objects in the world and their positions relative to the camera [3].

Advantage of passive approach

- Passive approach overcomes the disadvantage of active approach by creating the pre-existing images

Disadvantage of passive approach

- This approach is complex because it is based on the assumption that digital forgeries may leave no visual clues to indicate tampering, so they require different statistics of an image.

Types of Digital Image Forgery

The digital image forgeries are classified into following major categories. [2]

1. Copy-Move (cloning)
2. Image Splicing
3. Image Retouching

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

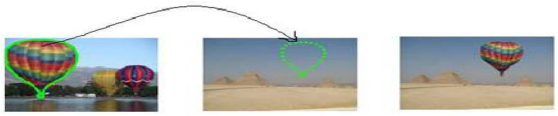
Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

4. Morphing

II IMAGE SPLICING

Image splicing is a one of the most common form of digital image manipulation or image forgery. Image splicing is a common type to create a tampered image where some regions from one image are copied and pasted into another image which produces composite image called spliced image; cut and join two or more snaps of pictures. This type of forgery is a challenging issue from tamper detection point of view. The complicated forgery may include some post-processing like blurring, JPEG compression, etc. that performs the forgery detection very hard. Hence image splicing can be defined as the process that crops and paste regions of an image from same or separate sources.



a. Source image b. Target image c. Composite image

Fig.1 Process of Image Splicing Forgery [1]

As shown in fig.1, by coping a spliced portion from the source image (a) into a target image (b). One can create a composite picture (c) or scenery to defraud others with the help of state-of-art image editing software. The non-professional users can do splicing very easily.
Existing methods for detecting splicing images are classified as below: boundary based and region based methods.

The boundary based methods find the unexpected transient at the splicing boundaries, e.g. sharp transition.

The region based methods depend on a generative model of the image and it uses the changeable system parameters estimated from the modified and the original regions to identify the forgery. For images obtained with digital cameras, the generative models try to model lighting, optical lens characteristic, sensor pattern noise, and post-processing algorithm, such as colour filter array interpolation.

III. LITERATURE REVIEW

Method used by [6] is based on Human Visual System Model and uses edge sharpness measure and visual saliency as forensic cue. It is convenient to locate splicing boundaries but needs training for users.
Method used by [7] is based on neighbor bit planes and used binary texture characteristics within bit planes for forensic cue. It is better for both stronger and weaker level manipulation but requires various image forensic detectors
Method used by [8] uses inconsistencies in lighting as cue. It is better for outdoor images.
Method used by [10] is based on specular highlights that appear on eye and used Inconsistencies in shape, color and location as cue. It is applicable to arbitrary objects but determines the direction of light source within one degree of ambiguity.
[11] is based on transition between illuminants of color. It uses disturbed illuminants. It is best for identifying image authenticity but requires original image for comparison process.
[12] is based on consistency checking of camera characteristics among different areas of image. It provides high performance but rate of detection of splicing is not to the expected level.
[13] judges lightning conditions of digital composite image in 3-D environment. It is very powerful in tampering analysis. It is not applicable to an arbitrary head pose.
[14] is based on discrepancies in motion blur. It uses inconsistencies in motion blur estimation through image gradients. It needs very less human intervention, improves robustness and efficiency If the segmentation of an image not done properly then rate of detection is less

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

IV. IMAGE SPLICING TECHNIQUES

A. Exposing Digital Forgeries from 3-D Lighting Environments

While creating a new image by combining multiple images, it is too difficult to exactly match the lighting conditions. Also it is difficult to visually judge inconsistencies in lighting and shadows in a photograph [13].We describe how to calculate the full 3-D lighting environment in images of persons. To extract the required 3-D surface, the 3-D models are fit to an image of a person's head and automatically align this model to an arbitrary head pose. This 3-D approach removes the uncertainties in the earlier 2-D lighting techniques, and hence useful for a more powerful forensic analysis.

a) 3-D Model Estimation

The model was obtained by collecting a set of 3-D laser scanned faces and by projecting them into a lower-dimensional linear subspace. By the linear combinations of the resulting linear basis, new faces are modeled. The 3-D model parameters can be estimated by using a pair of frontal and profile view or from only a single frontal view. Several trusty points on the face (11 on the frontal view and 9 on the profile view), are selected to estimate the 3-D model automatically. [13]

Shown in Fig. 2(a)-(b), is a frontal and profile view with the selected trusty points. The estimated model is shown in Fig. 2 (d)-(f), which can be seen to be in good with the original head poses shown in panels (a)-(c).

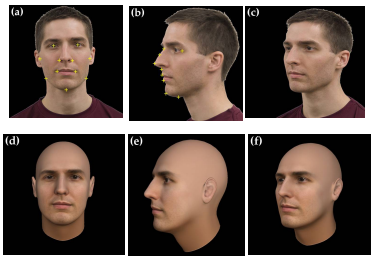


Fig2 Shown in panels (a) and (b) are a frontal and profile view used to estimate a 3-D head model (the +'s denote the manually selected trusty points). The estimated model is shown in panels (d)-(f) with head poses corresponding to panels (a)-(c). [13]

b) 3-D Model Registration

After the estimation, the 3-D model is registered to the face being analyzed. The objective function over the camera intrinsic and extrinsic parameters is maximized that aligns the 3-D model to the image of the face. Specifically, we consider the rotation matrix R, translation vector $\vec{t}$, focal length f and camera center (c_x, c_y) that maximizes the correlation between the image $I(\cdot)$ and the rendered model $I_m(\cdot)$:

$$(R, \vec{t}, f, c_x, c_y) = (x, y) * I_m(x, y) \qquad (1)$$

where $*$ denotes correlation, the spatial coordinates of the rendered model $I_m(.)$ $(x = x_s / s \text{ and } y = y_s / s)$ are given by:

$$\begin{pmatrix} x_s \\ y_s \\ s \end{pmatrix} = \begin{pmatrix} f & 0 & c_x \\ 0 & f & c_y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} R & \vec{t} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \\ 1 \end{pmatrix} \qquad (2)$$

and (X, Y, Z) are the 3-D coordinates of the face model. The error function in Equation (1) is maximized as follows.

First approximately The 3-D model is manually rotated to align it with the image $(\cdot)$. Minimum three corresponding points are selected on the model and image such as the center of each eye and base of the nose, from which the optimal translation is evaluated using standard least-squares. A brute force search that maximizes equation (1) is performed by considering the three rotation parameters, focal length, and camera center. At each iteration, the translation vector is estimated as described above. To reduce the lighting effects, a high-pass filter is applied to both the image $(\cdot)$ and rendered model $I_m(.)$ before computing the correlation in equation (1). After the model estimation and registration, 3-D surface normals and then corresponding intensities are used to estimate the lighting environment. [13]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

B. Displaying Digital Image Forgeries by Discovering Inconsistencies in Motion Blur

This approach is based on the method of spectral analysis of image gradients. The image gradients of a blurred image in the spectral domain display some periodic characteristics which are correlated with the amount and direction of motion blur present.

The suspected image is divided into overlapping blocks and the motion blur for each block is estimated. This is followed by a post processing step of smoothing the blur estimates and upsampling to the size of the image. The regions of the image which show inconsistent blur are then segmented from the image and displayed to the user. The author has also developed a BEM to provide robust segmentation, in the case of little perceptible blur. The presence of low blur is determined by using a perceptual blur metric. [14]

Blur Estimation

The widely recognized cepstral method is used to estimate motion blur. Instead of using the cepstrum directly, the spectral characteristics of the image gradients are used. The suspected image is divided into overlapping blocks and the motion blur for each block is estimated. This is followed by a post processing step of smoothing the blur estimates and upsampling to the size of image. The regions of the image which show inconsistent blur are then segmented from the image and displayed to the user. The presence of low blur is determined by using a perceptual blur metric. [14]

A flowchart outlining the steps in this technique is shown in Fig. 3

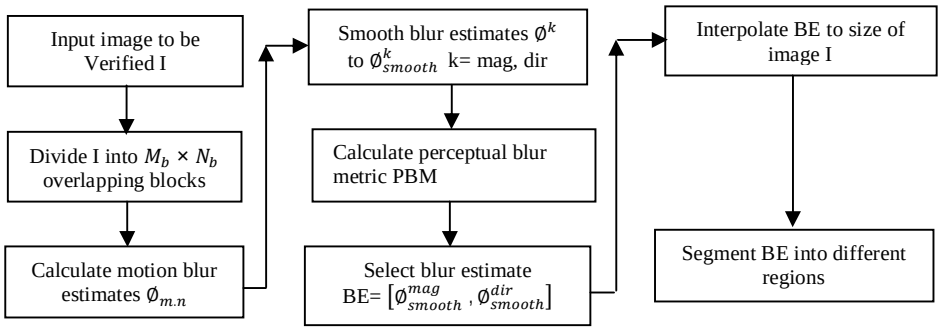


Fig 3 Flowchart for forgery detection technique using motion blur. [14]

Block-Level Analysis

If an image is artificially motion-blurred spliced region, it is impossible to obtain multiple blur models for the whole image from its gradients, mainly when the blurs are too much similar to each other. Hence, we propose estimating the blur at a local level allowing for different blur models to be estimated, without being lost in noisy data at a global level. The image I is divided into $M_b \times N_b$ overlapping blocks $b_{m,n}$, $m = 1$ to M_b ,n= 1 to N_b, and the motion blur estimate$\emptyset_{m.n}$ for each block is calculated. $\emptyset_{m.n}$ is a two-dimensional vector$[\emptyset^{mag}_{m,n}\ \emptyset^{dir}_{m,n}]$ which consists of the motion blur estimate magnitudes and directions. The image subdivision has two main benefits: 1) Motion blur can be estimated at a number of points, instead of just a single estimate for the entire image, with improved resolution, and 2) By allowing for simpler calculations, space-invariance of motion blur can be assumed over each block. [14]

Smoothing

The elements of the motion blur estimates $\emptyset_{m.n}$ can be represented in magnitude and direction estimate matrices $\emptyset^{mag}_{m,n}$ and $\emptyset^{dir}_{m,n}$, respectively, each of size $M_b \times N_b$, i.e.,

$$\emptyset^k = \begin{pmatrix} \emptyset^k_{1,1} & \emptyset^k_{1,2} & \dots & \emptyset^k_{1,N_b} \\ \emptyset^k_{2,1} & \emptyset^k_{2,2} & \dots & \emptyset^k_{2,N_b} \\ \vdots & \vdots & \vdots & \\ \emptyset^k_{M_b,1} & \emptyset^k_{M_b,2} & & \emptyset^k_{M_b,N_b} \end{pmatrix} \text{ k=mag,dir} \quad (3)$$

Since $\emptyset_{m.n}$is calculated independently for each block $b_{m,n}$, we perform a smoothing to correct for small variations in the estimated blurs. We smooth both the magnitudes and the directions of the estimates:

$\emptyset^k_{smooth} = \emptyset^k * h^k$, k = mag , dir

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Where $\emptyset_{smooth}^{k}$ represent the respective smoothed estimate and is the smoothing filter involved. A disk filter was used. Smoothing allows the local estimates to vary in a short manner, which results in better segmentation of the image in subsequent steps. [14]

Blur Estimate Measures

In few images certain regions appear to have little perceptible motion blur, we propose using the gradients of I along with the motion blur estimates$\emptyset_{smooth}^{mag}$, generating a new blur estimate measure (BEM), to improve robustness:

$$\text{BEM}(m,n) = \frac{\nabla I.w_{i,j}}{\emptyset_{smooth}^{mag}(\text{m,n})} \qquad (4)$$

Where $w_{i,j}$ is a neighborhood window placed at the center (i, j) in pixel coordinates of every block $b_{m,n}$ of the image I and of the same in size as the block. As stated above, equation (4) distinguishes between the cases where presence of little motion blur due to better focusing and where there is presence of a small amount of motion blur due to the lack of enough texture to give notable information about the motion blur present. Hence by considering only the magnitudes of the motion blur as the direction estimates are perpendicular to the image gradients. Similar to $\emptyset^{k}$ in (3), $\text{BEM}(m,n)$ can be arranged in an $M_b \times N_b$ matrix BEM , as $\emptyset_{m,n}^{K}$ and $\text{BEM}(m,n)$are calculated block-wise. [14]

Interpolation

The motion blur estimates are then upsampled to the size of using bicubic interpolation, in order to have an estimate of the blur at each pixel. The accuracy of the estimate depends on the amount of upsampling done. Bicubic interpolation provides better results than nearest neighbor (which gives a blocky segmentation) and bilinear interpolation (whose segmentation still has a few jagged edges that could be adequate for certain applications). [14]

Segmentation

The image is segmented into two regions that manifest different motion blurs which is achieved by thresholding the upsampled using Otsu's method. This method also gives an effectiveness metric which is used to discard images with consistent directions and/or magnitudes are shown in their motion blur estimates and hence cannot be segmented effectively. The result of segmenting the magnitude and direction of the estimates provides us with an indication of regions with dissimilar motion blur.

The results from this simple segmentation can be refined by again employing an energy-based segmentation. The pixel intensities are considered in addition to the motion blur discrepancies, giving smoother boundaries, more likely to correspond to the actual boundaries of the spliced region. This assumes that the spliced region are with different intensity than its immediate background, which is sensible. Otherwise, the boundary of the inconsistent region would not be detectable at all, by any method. In order to accomplish such segmentation, we use the mean values of the motion blur estimates of the two regions obtained by Otsu's method and then find the Euclidean distance between this mean and the motion blur estimate at each pixel. Using graph cuts, the author finds a segmentation which minimizes the total cost consisting of the cost of assigning different adjacent region labels (based on the above Euclidean distance) and the cost of dissimilar neighboring pixel intensities.

The ideal segmentation is obtained by using supervised spectral matting in order to extract the spliced regions from the image and applying Otsu's method to this extracted matte. Obtaining such segmentation requires knowledge of the spliced region, making it useful only for evaluating splicing detection. The same ideal segmentation can be used for comparison with the energy-based segmentation approach as well, since supervised matting ensures that the extracted region's boundaries correspond very closely with the spliced object's boundaries. [14]

V. CONCLUSION

We have studied various passive techniques which can be used for the detection of forgeries like image splicing. Our first contribution is a method to detect splicing in images containing motion blur. We have studied a new technique for detecting small inconsistencies in motion blur in an image which can indicate possible tampering. We have studied the use of two methods spectral matting and image gradients in order to estimate the motion blur for our purposes. Within this technique, we have also studied a novel blur estimate measure in order to deal with the case of very little motion blur. In order to automate the decision of using this new measure or plain motion blur estimates, we have studied a no-reference perceptual blur metric that is applicable to directional blur. When creating a photographic fusion, it is difficult to match lighting conditions. Hence we have studied a technique for measuring lighting conditions in an image, and its use in detecting photographic composites. We studied how a 3-D lighting environment with a low- dimensional model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

is approximated and how the model's parameters from a single image are calculated. Inconsistencies in the lighting model are then used as proof of alteration.

REFERENCES

[1] P.Sabeena Burvin, PG scholar, J.Monica Esther, "Analysis of Digital Image Splicing Detection" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014)
[2] Harpreet Kaur, Kamaljit Kaur "A Brief Survey of Diff Techniques for Detecting Copy- Move Forgery" Volume 5, Issue 4, 2015
[3] Mohd Dilshad Ansari, S. P.Ghrera&VipinTyagi :"Pixel-Based Image Forgery Detection: A Review" IETE Journal of Education,
[4] Nikhilkumar P.Joglekar, Dr. P. N. Chatur"A Compressive Survey on Active and Passive Methods for Image Forgery Detection"International Journal Of Engg And Computer Science ISSN:2319-7242 ,Volume 4 , Page No. 10187-10190, Jan 15.
[5] Zhen zhang,ying zhou, jiquankang & yaan ren, "Study of digital image splicing detection", zhang zhen 660126.com, china.
[6] Zhenhua Qu, Guoping Qiu, and Jiwu Huang.(Jan 8-10-2009) "Detect Digital Image Splicing with Visual Cues", 11th International Workshop, IH 2009, Darmstadt, Germany.
[7] Bayram.S, I. Avcibas, B. Sankur, and N. Memon, (2005) "Image manipulation detection with binary similarity measures", in Proc. Eur. Signal Processing Conf. (EUSIPCO), vol. I, pp. 752–755.
[8] Johnson and Hany, (2005) "Exposing digital forgeries by detecting inconsistencies in lighting", in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, pp. 1–10.
[9] Hany Faridy and Alin C. Popescu, (Feb 2005) "Exposing Digital Forgeries by Detecting Traces of Re-sampling", Signal Processing, IEEE Transactions on (Volume:53 , Issue: 2).
[10] Johnson.M.K, (2007) "Exposing Digital Forgeries Through Specular Highlights on the Eye", 9th International Workshop on Information Hiding, Saint Malo, France.
[11] C. Riess and E. Angelopoulou, (2010) "Scene illumination as an indicator of image manipulation", Inf. Hiding, vol. 6387.
[12] Yu-Feng Hsu and Shih-Fu Chanhge, (2007) "Image Splicing Detection Using Camera Response Function Consistency and Automatic Segmentation", ICME, page 28-31, IEEE.
[13] Eric Kee and Hany Farid, (Dec 2010) "Exposing Digital Forgeries From 3-D Lighting Environments", Information Forensics and Security (WIFS), 2010 IEEE International Workshop.
[14] Pravin Kakar, N. Sudha, and Wee Ser, (Jun 2011) "Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur", IEEE Transaction on Multimedia, Vol. 13, No, 3.