Review of Image Splicing Forgery Detection Techniques

PNRL Chandra Sekhar[1], Dr. T N Sankar2
1 Research Scholar, 2 Professor
Dept of CSE, KL University, Vijaywada
[1]pchsekhar@hotmail.com, [2]tnshankar2004@kluniversity.in

***Abstract*--** With the growing usage of internet in daily life along with the usage of powerful image editing software tools in creating forged images effortlessly, making us lose the trust in the authenticity of the images. More than a decade an extensive research is going on in the field of Image forensics aims at restoring trustworthiness in images by bringing various tampering detection techniques. In this regard, we attempt to survey various techniques found particularly in Splicing Image Forgery Detection. We summarize both features based as well as camera characteristics based techniques over the recent years.

***Index Terms*--** Image splicing, Copy-Move Forgery, Re-sampling, Passive techniques.

I. INTRODUCTION

Today's world is living in the remarkable era of visual imagery which made it possible to access, process and share information very easily. Historically we had confidence in the integrity of this imagery however; the rapid growth of technological advancement in digital technology in terms of powerful algorithms, tools such as Photoshop, CorelDraw for manipulating digital images brought with major security challenges that rise question in this trust. Name a few particularly from magazines to fashion industry in terms of media outlets, scientific magazines, political campaigns, courtrooms, photo hoaxes that reached our inbox, doctored photographs etc are appearing with a growing frequency and sophistication. Then it becomes very difficult to discriminate which is authentic or manipulated or doctored image.

In general image forgery is the manipulation of digital images either in terms of destroying or inserting some information in the images. An example of such forged image is shown in Figure1. An American diplomat John Forbes Kerry with Jane Fonda, an Hollywood actress speaking to a crowd at an anti-Vietnam peace rally [1]. This is a manipulated image by a hoaxer in trying to raise a question about John Kerry's patriotism.

Figure 1: Example of image forgery John Forbes Kerry with Jane Fonda

This manipulation of images is going on from the past and even accepted in areas like the forensic investigation, Information Technology, medical Imaging, Journalism, Intelligence service etc.[2] Nowadays organizations interested in paperless work and e-government services resulting a huge amount of data stored in digital format and this gives rise to many challenges to secure authentic data. Unfortunately, the various collections of data like documents, files, voice data, and image data are all vulnerable to manipulation and doctoring. This gives rises to an interest among the research community in developing image forensics techniques towards identifying the trust of digital images. Over the past decade, the image forensics emerged to help in restoring the lost trust to digital images.

The rest of the paper organized as follows: In section II the classification of Image forgery is discussed, in section III various forgery detection techniques are discussed followed by a summary of splicing image forgery techniques are given in section IV and ends with conclusion in section V.

2. CLASSIFICATION OF IMAGE FORGERY

In literature,researchers classified Image Forgery in following ways [4]. Copy-Move or region duplication forgery is the most common image tampering technique used because of its simplicity and effectiveness. In this type, part of the original image is copied or moved to a destined location for pasting in order to hide certain details as well as duplicate parts of an image as given in figure2. Textured regions are used as ideal parts for copy-move forgery since textured areas has similar color and noise variations to that of an image which is unperceivable to human eye looking for inconsistencies in image statistical properties.

Figure 2: Copy-move Image forgery

Image splicing involves replacing of image fragments from one or more different images into another image in order to produce a fake image as shown in figure3. This is one of the simple and commonly used tampering techniques. When splicing is performed carefully, the borders between the spliced regions can visually be imperceptible. However, splicing disturbs the higher order Fourier statistics such as the bi-spectrum.

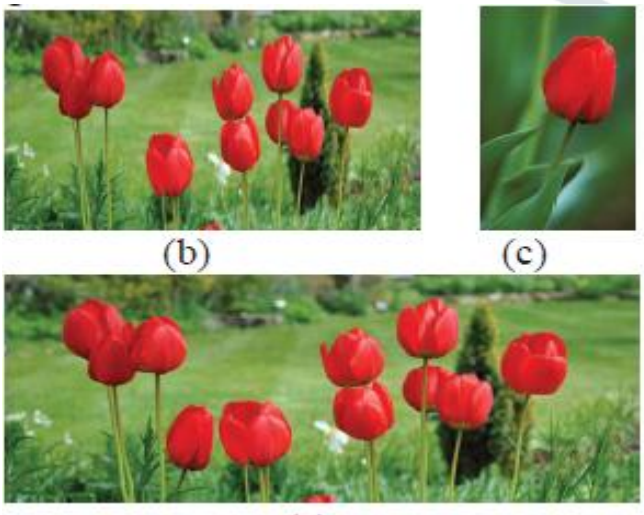

Figure 3: Splicing Image forgery

Image Re-sampling involves in creating a high quality forged image by applying some transformations like rotation, scaling, stretching, skewing, flipping etc in order to produce a convincing composite between two objects of different dimensions as shown in figure4. This process requires resample the original image onto a new by introducing specific periodic correlations between neighboring pixels.

Figure 4: Re-sampling image forgery

3. IMAGE FORGERY DETECTIONTECHNIQUES

Image forgery detection aims at verifying the authenticity of a digital image [4]. The authentication can be classified into i) Active and ii) Blind or passive approaches as shown in figure (5). The Active approach includes techniques like digital signatures or watermarking wherein a known authentication code was embedded into the image either at the time of creation or just before it can send through an unreliable public channel. The authenticity can be verified by the presence of the code with the inserted original code. However, this method requires special hardware or software to insert the authenticated code in the image before the image is being used. Whereas, Blind or passive forgery techniques uses the received image only for assessing its authenticity or integrity without using any external signature or watermark of the original image. The forgery images do not leave any visual clues to indicate tampering but leave changes its underlying statistics

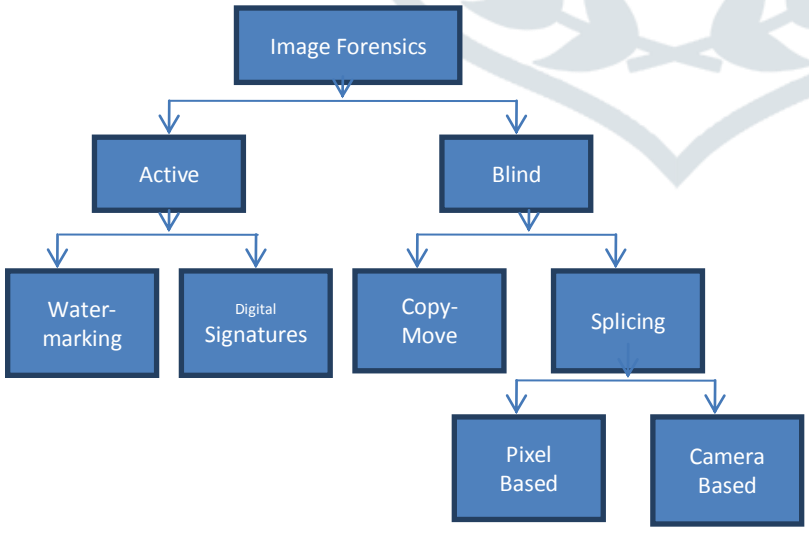

Figure 5: Classification of Image Forensics

image forensic techniques classified as pixel-based techniques – which detects any statistical anomalies found in the image at pixel level, format-based techniques - which detects any statistical correlations by a specific lossy compression technique, camera-based techniques - which identifies the different artifacts produced using the camera lens, sensor, or on-chip post processing operations, physical based techniques - which are due to anomalies between objects, camera and light and geometric-based techniques – based on measurements of objects with its relative position of camera [3].

4. SPLICING IMAGE FORGERY DETECTION TECHNIQUES

Image splicing is a technique in which crops and pastes regions of the image from the same or different image. This is a fundamental step used in digital photomontage, which is very popular in digital image content editing. It is also referred as paste-up produced by sticking the images together using available digital software tools such as Photoshop. The spliced image used in many ways such as news reports, photography contest, key proof in the academic papers, and so on, which could bring certain negative influences. As the digital images become more vulnerable to malicious tampering compared to their non-digital counterparts naturally it becomes an important and challenging research area in order to determine the authenticity of an image and detecting tampered parts of an image. The following are various techniques found in the literature and we classify them as illumination color estimation, inconsistency in image noise levels, statistical properties inherent in the source image (camera characteristics) and other feature based methods.

Illumination color Estimation - in identifying the authenticity of a digital image illumination inconsistencies are potentially effective for splicing detection among other telltale signs. This is due to proper adjustment of the illumination conditions is hard to achieve while creating a forged image.

In [12] developed a physics based on illuminant color model for detecting the difference in the local image regions. The authors used illumination map based on distance measure to estimate the results thereby employing in forensic analysis. This technique requires user intervention. [13] Used inconsistencies of the illuminant color in the object region in order to detect the region splicing forgeries based on local illumination estimation. They proposed to combine five low-level statistics-based algorithms to estimate illuminant of each horizontal and each vertical band. For further development, [14] presented a new technique to detect forged images of people using the illuminant color. They estimated illuminant color using a statistical gray edge method and a physics-based method which exploits the inverse intensity-chromaticity color space. HOGedge algorithm is used to combine texture and edge based cues and used machine learning late fusion. Thereby reduce user intervention to minimal.

Forgeries based on inconsistency in image noise levels – noise that exists in images can be used to improve accuracy in detecting spliced image regions. It is evident that each image obtained by a digital camera prone to contains certain type of noise which may happen during to process of photons comes into the sensor until the camera output the image.

In [15] a blind forgery detection method based on local noise inconsistencies to detect small regions corrupted by local noise is proposed. The method uses the high pass diagonal wavelet coefficients at the highest resolution with non-overlapping blocks. The image segmented on the basis of homogeneity condition into several homogenous sub-regions using simple region merging algorithm in order to detect spliced forgery. The methods work well on the image where there is homogeneous noise level but fail when the authenticated image contains the same. As an improvement in [16] authors proposed an effective method based. First, the image is divided into non-overlapping blocks and clustering applied to make them clean and tampered blocks. The detected suspicious regions are further segmented to refine noise estimation and finally applied classification to obtain the final result. To improve the results further the author estimate local noise variances by segmenting the image into regions with significantly different noise variances. Simple k-means clustering algorithm applied and then post-processing steps on detected regions to refine the result. In [17] an automated technique is proposed to detect spliced forgery in raw images. They used the relative consistency of noise parameters by looking at image inconsistencies from quad-tree decomposition to detect the potential sliced images. An efficient technique is proposed in [18] to detect region splicing. The technique is based on observed projection kurtosis concentration phenomenon. The

noise statistics estimation is an optimization problem with a closed-form solution. All these techniques based on noise discrepancies in a single scale. Taking the advantage of multi-scales as an indicator for detecting spliced image forgery [19] proposed a technique where the image segmented into super-pixels of multiple scales and then noise level function applied on each individual scale. Those segments which are not constrained by the noise level function are further processed by Optimal Parameter Combination Searching algorithm in order to mark the spliced regions.

Author	Year	Method	data set	works well on
Babak et al.	2009	local noise standard deviation	Columbia	homogeneous noise levels
X Pan et al.	2012	Inconsistency in image noise levels	Columbia, UCID	higher noise variances & larger regions
S Lyu et al.	2014	projection kurtosis concentration	Columbia, UCID	simple and specific statistical aberration by additive noise
Chi-M P et al.	2016	OPCS	own dataset	spliced area with different noise variance, different size and different no of spliced objects

Table1: Comparison of noise based techniques

Statistical properties inherent in the source image - the consistency of inherent physics-based attributes among different parts of a single image such as natural scene related, imaging device properties such as camera characteristics can be used in detecting forged regions of an image.

In [20] proposed a method based on identifying the consistency of camera characteristics among various area of an image. On a segmented image, from each area a camera response function (CRF) is estimated using geometric invariants from LPIP's. CRF cross fitting scores and area intensity features are computed and given to SVM-based classifier. A

Author	year	method	data set	performance
Yu-Feng Hsu et al.	2007	CRF& LPIP	own dataset	Precision-70% Recall 70%
Zhenhua Qu et al.	2009	HVS	Columbia	96.33% accuracy
H.R. Chennamma	2010	consistency of lens radial distortion	Columbia	86% accuracy
Pravin K et al.	2011	spectral analysis of image gradients	own dataset	93.43% accuracy

Table2: Comparison of Statistical properties of source image

machine learning algorithm based on human visual system (HVS) model is proposed in [21]. High correlation between spliced borders and the first few fixation points obtained by edge sharpness used as visual cues. The visual fixation prediction algorithm is proposed to detect spliced images with visual cues. The limitation is that the edge sharpness cues used in this method will fail when concealing measures, such as blur, is applied. To improve further [22] proposed a method

based on an intrinsic camera parameter lens radial distortion for detecting spliced image forgery where the degree of lens radial distortion across the image is used as evidence for splicing. The algorithm measures lens radial distortion of the image using line-based calibration. The method works well for splicing of images when straight edges are there but the poor quality image will generate perturbations along with straight lines which results wrong estimation of radial distortions. In [9] Used inconsistency in the blurriness and direction of motion blur. This method cannot discriminate motion and out-of-focus blur. It can only usedfor linear motion blur and cannot be applied to the more complicated motion blur kernels.

Other Featurebased techniques - in general, any feature based techniques follows a 4 step process. Image pre-processing mainly to enhance the structural changes occurred due to forgery. Feature extraction where compute the specific representation of data that can highlight relevant information. To reduce complexity, eliminate some insignificant features before classification. Classifier selection and modeling to identify an appropriate classifier and then train set of images and fine-tune the parameters. Classification discriminates the given image and classifies them into two either authentic or forged. Commonly used classifiers as SVM [5-8], KNN[23], Naïve Bayes[24], ANN[10].

Author	year	method	data set	performance
Amani A.A et al.	2013	LBP & DCT	CASIA v1.0	97%
Yujin Z et al.	2013	MBDCT &Kernal PCA	Columbia	90.46%
Saurabh A et al.	2015	Entropy & LPQ	CASIA v2.0	98.33%
Ce.Li et al.	2015	QDCT	DVMM	93.42%

Table3: Comparison of feature based techniques

In [5] proposed a technique based on features extracted from the chromatic channel. After chrominance component is extracted, the image divided into overlapping blocks and LBP calculated for each block and transformed each block into 2D DCT. Standard deviations corresponding DCT coefficients of each block are used as a feature vector. A different perspective method is proposed in [7] where first multi-block discrete cosine transform (MBDCT) applied to input images and apply the multi-resolution LBP operator on the magnitude components of 2D array DCT components. Kernel Principal Component Analysis (Kernal PCA) is used to reduce the dimensionality of the feature vector. In [6] authors applied multi-scale entropy filter on chrominance components Cb and Cr of the input images followed by LPQ operator. The Feature vector is obtained by calculating the histogram of LPQ of the image with size 256. Owing to their effectiveness and simple-ness Markov features [8] extracted from both DCT and DWT domains. AEM_EDW is used to make the computational complexity more manageable.

5. CONCLUSIONS

In this review, we presented a summary study of various splicing image forgery detection techniques. The spliced images are produced from different images there by the discrepancies of the image features or camera characteristics are the main source in detecting the forged regions of the images. Among the pixel-based and statistical based techniques we classify further into illumination color estimation, statistical characteristics of the image, noise inconsistency and finally presented other feature based methods. There may be several techniques found in the literature but, each one has its limitations. Image forensics is a burgeoning research field and despite the limitations, it promises a significant improvement in forgery detection with competition among forgery creators and detectors.

REFERENCES

[1] K L Fonda, Kerry, And P Fakery, "The Washington Post," P- A21, Feb. 2004.

[2] M A Qureshi, M Deriche, "A Review On Copy Move Image Forgery Detection Techniques", 11th IEEE International Multi-Conference On Systems, Signals & Devices (SSD), 2014

[3] H Farid, "Image Forgery Detection A Survey," IEEE Signal Processing Magazine, Vol. 26, No. 2, Pp. 16-25, Mar 2009.

[4] G K Birajdar, V H Mankar, "Digital Image Forgery Detection Using Passive Techniques: A Survey", Digital Investigation (10) 2013 @Elsevier.

[5] Aa Alahmadi, M Hussain ; Hatim A ; Ghulam M ; George B, "Splicing Image Forgery Detection Based On DCT And Local Binary Pattern", Global Conference On Signal And Information Processing (Globalsip), 2013 IEEE

[6] Saurabh A, Satish Ch," Image Forgery Detection Using Multi-Scale Entropy Filter And Local Phase Quantization", Internation Journal Of Image, Graphics And Signal Processing, 2015.

[7] Y Zhang, Ch Zhao, Yiming Pi, Shenghong Li1, Shilin W", Image-Splicing Forgery Detection Based On Local Binary Patterns Of DCT Coefficients", Security And Communication Networks, Published Online In Wiley Online Library, 2013.

[8] Ce Li1,2(&), Qiang Ma1, Limei Xiao1, Ming Li1, And Aihua Zhang1," Image Splicing Detection Based On Markov Features InQDCT Domain", LNCS, Springer, 2015

[9]P.Kakar, N. Sudha, And W. Ser, "Exposing Digital Image Forgeries By Detecting Discrepancies In Motion Blur," IEEE Trans. Multimedia, Vol. 13, No. 3, Pp. 443–452, Jun. 2011.

[10] Zhang Z, Wang G, Bian Y, Yu Z,"A Novel Model For Splicing Detection", In IEEE 5th International Conference On Bio-Inspired Computing: Theories And Applications (Bic-Ta), 2010

[11] TuK.Huynh, KhoaV.Huynh, Thuong Le-Tien, SyC.Nguyen, "A Survey on Image Forgery Detection Techniques", International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF),2015.B. Su, S. Lu, And C. L. Tan, "Blurred Image Region Detection And Classification," In Proc. 19th Acm Int. Conf. Multimedia, 2011, Pp. 1397–1400.

[12] C. RiessAnd E. Angelopoulou, "Scene Illumination As An Indicator Of Image Manipulation," Inf. Hiding, Vol. 6387, Pp. 66–80, 2010.

[13] Yu Fan, Philippe Carré, Christine Fernandez-Maloigne" Image Splicing Detection With Local Illumination Estimation", ICIP 2015

[14] C. RiessAnd E. Angelopoulou, "Exposing Digital Image Forgeries By Illumination Color Classification", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 7, July 2013

[15] Xunyu Pan, Xing Zhang, SiweiLyu, "Exposing Image Forgery With Blind Noise Estimation", Thirteenth Acm Multimedia Workshop On Multimedia And Security, 2012

[16] Xunyu Pan, Xing Zhang, SiweiLyu, "Exposing Image Forgery With Blind Noise Estimation", IEEE International Conference On Computational Photography (ICCP), 2012

[17] Thibaut Julliand, Vincent Nozick And Hugues Talbot," Automated Image Splicing Detection From Noise Estimation In Raw Images", 6th International Conference On Imaging For Crime Prevention And Detection (ICDP-15)

[18] SiweiLyu ,Xunyu Pan And Xing Zhang, "Exposing Region Splicing Forgeries With Blind Local Noise Estimation", Springer, Int J Comput Vis,2014

[19] Chi-Man Pun, Bo Liu, Xiao-Chen Yuan, "Multi-scale noise estimation for image splicing forgery detection", Journal Of Visual Communication Image Representation, Elsevier, 2016.

[20]Yu-Feng Hsu And Shih-Fu Chang," Image Splicing Detection Using Camera Response Function Consistency And Automatic Segmentation", 2007 IEEE International Conference On Multimedia And Expo

[21] Zhenhua Qu1, Guoping Qiu2, And Jiwu Huang1," Detect Digital Image Splicing With Visual Cues", LNCS, Springer, 2009.

[22] H. R. Chennamma, LalithaRangarajan, " Image Splicing Detection Using Inherent Lens Radial Distortion", International Journal Of Computer Science, 2010

[23] FahimeHakimi, Zanjan, Iran Mahdi Hariri," Image-Splicing Forgery Detection Based On Improved LBPAnd K-Nearest Neighbors Algorithm", International Journal Of Electronics Information & Planning, 2015.

[24] Muratov O, Dang-Nguyen D-T, Boato G. De NataleFg," Saliency Detection As A Support For Image Forensics", 5th International Symposium On Communications Control And Signal Processing(ISCCP), 2012