INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Survey of Image Forgery Detection Technique Based on Color Illumination Using Machine Learning Approach

K.Sharath Chandra Reddy
Research Scholar
CBS Group of Institution, Jhajjar, Haryana

Tarun Dalal
Assistant Professor (CSE Department)
CBS Group of Institution, Jhajjar, Haryana

***Abstract:** In ancient times, images were used very rarely & there was a possibility of less amount of forgery or no forgery in images. It requires much knowledge to create a forged image earlier. Nowadays, Images have gained a very vital importance in our daily life and it is not very difficult to make forged images because of the availability of powerful digital image editing software's that does not require any expert knowledge. So, it becomes very easy to create a tampered image. As a result we have to prove the authenticity of an image. In this paper we have discussed about one of the most common forms of image forgery which is image splicing and other forms. We discussed about various existing forgery detection methods and techniques based on color illumination & machine learning approach which results in automatic decision making. We have also discussed about the existing work drawbacks and the possibility of future improvements.*

***Index Terms**— Forgery, Tampered Image, Image Splicing, color Illumination.*

1. INTRODUCTION

Images have become a powerful tool for communication nowadays as they are used every day in newspapers, magazines, websites and advertisements and provide various information. As the use of images are increasing day by day but trust in images is decreasing day by day. Creating a fake image from original image is known as Image forgery and to check whether the image is original or fake is probably termed as Image forgery Detection. Moreover, digitally manipulated images can trigger off major controversies. Hence, there is a need for more sophisticated and mathematically sound techniques that can perform this task of classification of the image into real ones and digitally manipulated ones.
There are basically three main types of image forgery-

1. Image Retouching-

Image Retouching is very common and least-harmful kind of digital alteration. Instead of completely changing the subject of the photo, retouching is enhancement or reduction of certain features in the image (see Figure 1). The most common users of this technique are magazines or other photo-heavy publications. By altering the images used on their covers or in their articles, such publications can make the subjects of the photos seem more attractive and encourage buyers to purchase the publication, disregarding the ethical problems of such an action [1].

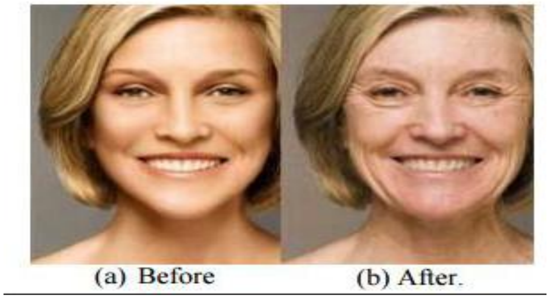


Figure 1. Image retouching forgery

2. Image Splicing

Image Splicing is also known as Image Composition. Image Splicing is very harmful as compared to Retouching. Creating a completely new image occurs by copying a part from one image and pasting to another one [2].In Figure 2 there is an insertion of a breaching Great White Shark into the base image of the helicopter rescue. In addition, the base image is rotated to make the image more convincing, and certainly more dramatic and memorable

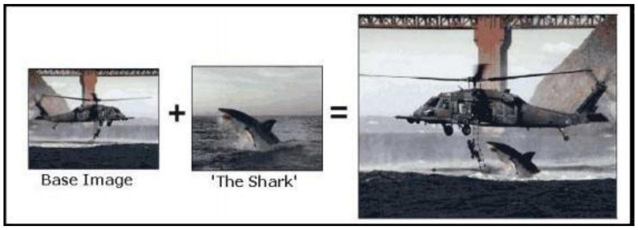


Figure 2: Image splicing forgery

3. Copy-Move

Copy-move is again similar to the previous category. Unlike Image Splicing, a copy of a region of an image is pasted in the same image. The difference lies in using the base image itself as both source and recipient of the copied portion. The primary objective of copy-move forgery is to either add or hide objects in a digital image. Blurring along the border of the pasted regions makes the editing less obvious, eliminating irregularities that could show the picture as tampered [3]. Figure 3, shows an image subjected to a copy-move forgery, as well as the original source image. The smoke from the picture on the left, copied and pasted multiple times, enhances the size and visual effect of the smoke cloud.

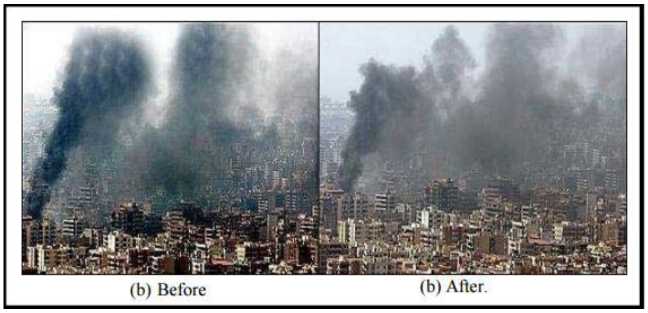
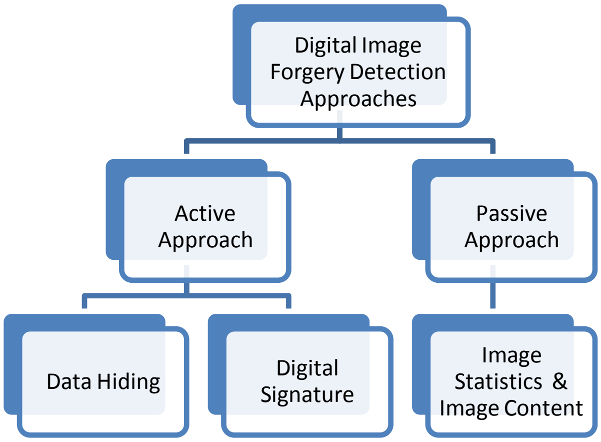


Figure 3: Copy-move forgery

IMAGE FORGERY APPROACHES


Digital Image Forgery Detection Approaches
Active Approach
Passive Approach
Data Hiding
Digital Signature
Image Statistics & Image Content

There are basically two approaches of digital image forgery detection-

1. **Active Approach-**This approach consists of :-
   - Data hiding: In this approach, it adds secondary data into an image. Digital watermarking is a common example of this. In this, digital watermark is inserted at source side and verify that at detection side. The main drawback of this method is that watermark must be inserted at the time of recording, which requires specially equipped digital camera.
   - Digital signature.: In this approach, unique feature of image is extracted and Corresponding signature created at the source side. This signature is then used for verification at the detection side.[4]

2. **Passive Approach**
   - This approach does not need any prior information about image like it does not need any digital signature generated or watermark embedded in advance. This is the main advantage of passive methods. [4]
   - This techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.
   - Detecting the changes in statistical properties and is known as digital image forensics.

IMAGE FORENSIC TOOLS

1. Pixel-based techniques-These techniques includes that tools which helps in detecting statistical anomalies introduced at the pixel level.
2. Format-based techniques- These techniques includes that tools which leverage the statistical correlations introduced by a specific lossy compression scheme.
3. Camera-based techniques- These techniques includes that tools which exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing.
4. Physically based techniques- These techniques includes that tools which explicitly model and detect anomalies in the three dimensional interaction between physical objects, light, and the camera.

5. Geometric-based techniques- These techniques includes that tools which make measurements of objects in the world and their positions relative to the camera.[5]

LITERATURE REVIEW

Digital forgery is now a nightmare to individuals (e.g. fake images of celebrities and public figures), societies (fake images targeting religion or race), journalism, scientific publication etc. [6]. According to a survey, Flickr has some 350 million photographs with more than 1 million added daily (record 2007) and Facebook has more than 50 million cumulative upload of images (record 2010) [6]. The maintenance of such a large amount of digital data has become critical, complex and challenging.

In the recent years many forgery detection methods and techniques are proposed. Digital watermarking is one effective tool for providing image realism and source details. Forgery detection is also offered by these digital watermarks. A number of watermarking techniques have been proposed. One uses a checksum on the image data which is embedded in the least significant bits of certain pixels [3]. Others identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image and adding a maximal length linear shift register sequence to the pixel data [6]. Watermarks can be generated by modulating JPEG coefficients, or can be relied on image, using independent visual channels. Some watermarks are designed to be invisible, which can be blend in with camera or noise. Watermarks which are visible also do exist.

Weiqi Luo [6] proposed an algorithm to extract image features by using seven characteristics features computed from the statistical analysis of pixels in an image block. The first three features are the average of red, green, and blue components respectively and the other four features are computed based on the division of that block into two parts in 4 directions: horizontal, vertical, and two diagonal directions. To obtain the correct matching, the main shift vector which has the highest frequency of occurrence is also defined. It gives low computational complexity and more robust against various post region duplication image processing graphics operations.

Li, Hancheng Zhu et al. [7] have used a vector with seven elements to describe the feature of each small blocks, a 9- dimensional vector is also introduced in to solve the problem with a fixed angle rotation on the copied regions. Elements of this vector are calculated based on the intensities from four equal-sized sub-blocks on each block. The first element is the average intensity, the next four elements are ratios of average intensities and the last four elements are differences of average intensities. A radix sort algorithm is applied to perform lexicographical sorting on these vectors and a forgery manipulation is also detected. The rotation with fixed angle can be detected but not with arbitrary angles by this methods.

Hieu Cuong Nguyen et al. [8] proposed Radon transformation to extract the features and use phase correlation to detect the pairs of matching vectors. The proposed method is well performed for the forged images which the rotation angle of the copied region is less than 4o, has Gaussian noise addition with a SNR greater than 35dB and smaller block size 8x8 pixels.

Preeti Yadav et al. [9] introduced an improved algorithm by applying DWT into an image to reduce the dimension representation. The feature vectors will be extracted from the small overlapping blocks of the compressed image and sorted lexicographically to find the duplicated blocks. The detection was carried out on the lowest level image representation and also proved best performance on small size copy move forgery, detected the multiple Copy-Move forgery with lower computational complexity.

Johnson et al. [10] proposed a method which describes how composites can be detected by estimating a camera's intrinsic parameters from the image of a person's eyes .In authentic images, the principal point is near the center of the image. When a person is translated in the image as part of creating a composite, the principal point is moved proportionally. The major sensitivity with this technique is in extracting the elliptical boundary of the eye. This process will be difficult for low-resolution images.

Riess and Angelopoulou et al. [11] introduced method which uses physics-based illumination cues to image forensics. They examined inconsistencies in specularities based on the dichromatic reflection model. Specularity segmentation on real-world images is challenging.

Therefore, it requires manual annotation of specular highlights. A second drawback of this approach is that it relies on the presence of specularities on all regions of interest making them difficult to deploy in many real world scenarios.

Takai Niinuma et al. [12] proposed a novel method for estimating parameters of light sources. Their key idea is in introducing the notion of difference sphere that are acquire by differencing two image regions of the reference spheres. They show that separate identification of multiple combined light sources is facilitated through an analysis of gray level contours on the difference sphere. In a forensic scenario, however, the conditions for image capturing cannot be controlled. Thus, one cannot assume to have such gray spheres placed in the scene under investigation.

Gholap and Bora [13] proposed a method, where color mismatches among objects are considered for forgery detection. While creating a Spliced image from a number of images, it becomes very difficult to match the color of one object with reference to the other. In the proposed method, the color mismatch is decided by estimating the illuminant color of different objects in the image and illuminant color is estimated in every specular highlight region. A specular highlight is the bright spot of light that appears on shiny objects when illuminated. Then illuminant colors were plotted in r-g plane by straight dichromatic lines. If these lines intersect points of different regions were not close to each other, it is considers as a forged image.

Tiago and Christian et al. [14] Proposed a method that exploits subtle fakeness in the color of the illumination of images .The technique used is machine-learning based and requires minimal user interaction. This technique is applicable to spliced images only. To achieve this, they combined information from physics and statistical-based illuminant estimators on image regions of similar material. From these illuminant estimates, they extract texture- and edge-based features which are then provided to a machine-learning approach for automatic decision-making. In order to describe the edge information, they proposed a new algorithm based on edge-points and the HOG descriptor, called HOG edge.

Reshma P.D and Arunvinodh C [15] describes a technique for detecting digital image forgery using illuminant color. In this paper, they presented an improved forgery detection method that makes use of machine learning classifiers. Training images texture and gradient features extracted and train the classifier with these features. Then classifier tests the image and made accurate. The main advantage of this work is that it completely avoids user interaction and provides a crisp Statement on the authenticity of the image.

Pravin et al. [16] proposed method to detect motion blur inconsistencies using spectral matting to help splicing detection. They also developed a new measure to do inconsistent region segmentation in images that contain small amounts of blur.It has been proved an effective method than other existing blur based techniques.

Zhipeng et al. [17] provides another method to detect image tampering. It detects global or local blur manipulation using no-reference image quality metric. It extracts image features from MSCN(meansubtractedcontrastnormalized) coefficients of different regions to quantify tampered regions. But it does not work good for images with poor resolution.

COMPARISON:

Author	**Techniques**	**Advantages**	**Disadvantages**
Weiqi Luo & et al.	Copy Move Forgery	Gives low computational complexity and more robust against various post region duplication image processing graphics operations.	
Li, Hancheng Zhu et al.	Copy Move Forgery	robust not only to the traditional signal processing operations, but also to the rotation and	when the region is rotated by general angles, it is difficult to detect the forgeries.

		flipping.	
Preeti Yadav et al.	Copy-Move forgery based on Discrete Wavelet Transform	Has lower computational complexity because detection is first carried out on lowest level image representation	Low performance when large size coy move forgery.
Gholap, Bora et al.	Exploiting Color mismatches among the objects in the digital image & color mismatch is based on estimated illuminant color in every specular highlight region & illuminant estimation is done through PCA.	Experimental results suggest good performance of the proposed method on images which Show the specular highlights.	This method is not suitable for images containing Human skin as the bunch of human skin colors lies near that of illuminant color.
Tiago and Christian et al.	A semiautomatic method For the minimization of user interaction of an illuminant-based tampering decision-Making.	The proposed method requires only a less amount of human interaction and provides a crisp statement on the authenticity of the image.	Although promising as forensic evidence, methods that operate On illuminant color are inherently prone to estimation errors.
Reshma P.D and Arunvinodh C	Detecting digital image forgery using illuminant color (SVM Classifier).	It completely avoids user interaction and provides a crisp Statement on the authenticity of the image.	
Pravin kakar et.al	Based on spectral matting	•Simple and speedy segmentation to detect inconsistent regions efficiently •estimates the motion blur effectively. •detects splicing forgery •Better inconsistent region interpretation for user	More number of steps are involved
Zhipeng et.al	MSCN coefficients	Good for detecting guassian blur and blur operation by mean filter	•Not good for images with poor resolution. •Cannot detect guassian blur with sigma 0.1

CONCLUSION

In recent years, there is a significant improvement in the field of image forgery detection. But, in spite of this improvement and higher number of methods, we still can see a lot of drawbacks and imperfections of the existing methods. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem. Thus to solve this problem recently some more techniques were presented and new techniques will be developed to make better and harder to detect fakes (for exposing photographic frauds). In this paper we have discussed different methods of detection for digital image forgery as well as illumination inconsistencies and illuminant map. From survey of all papers, we found that inconsistencies in lighting method use the direction of the incident light for exposing digital forgeries. For the future work we suggest to work over improved new method with efficient skin detection methods.

REFRENCES

[1] S.Shaid."TypesofImageForgery."Internet:http://csc.fsksm.utm.my/syed/research/image-forensics/11-types-of-imageforgery.html, Feb.08, 2010 12:17 [Dec. 4, 2012].

[2] Z. He, W. Sun, W. Lu, and H. Lu. "Digital image splicing detection based on approximate run length," Pattern Recogn .Lett., vol. 32, pp. 1591-1597, 2011.

[3] B. L. Shivakumar and Lt. Dr. Santhosh. "Detecting copy-move forgery in Digital images: A survey and analysis of current methods," Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.

[4] BASE PAPER REFERENCE.

[5] Deshpande, Pradyumna, and Prashasti Kanikar. "Pixel Based Digital Image Forgery Detection Techniques." International Journal of Engineering Research and Applications (IJERA) 2.3 (2012): 539-54.

[6] Luo, Weiqi, Jiwu Huang, and Guoping Qiu. "Robust detection of region-duplication forgery in digital image." Pattern Recognition, 2006. ICPR 2006. 18th International Conference on. Vol. 4. IEEE, 2006.

[7] Leida Li, Shushang Li, Hancheng Zhu, “An efficient scheme for detecting Copy-Move forged images by local binary patterns”, Journal of Information Hiding and Multimedia Signal Processing, Vol. 4, No. 1, pp. 46-56, January 2013.

[8] Hieu Cuong Nguyen and Stefan Katzenbeisser, “Detection of Copy- Move forgery in digital images using Radon transformation and phase correlation”, IEEE Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeu, 2012.

[9] Preeti Yadav, Yogesh Rathore, “Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform”, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 04 April 2012.

[10] M. K. Johnson and H. Farid, “Detecting photographic composites of people,”in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.

[11] C. Riess and E. Angelopoulou. Physics-Based Illuminant Color Estimation as an Image Semantics Clue. In: Proceedings of the 16th IEEE International Conference on Image Processing(Page: 689 Year of Publication: 2009 ISBN: 978-1-4244-5653-6).

[12] T. Takai, K. Niinuma, Difference Sphere: An Approach To Near Light Source Estimation Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,(Page: 98 Year of Publication: 2004 ISBN: 0-7695-2158-4)

[13] S. Gholap and P. K. Bora, Illuminant colour based image forensics, in Proc. IEEE Region 10 Conf. 2008, pp. 1–5. [9] C. Riess and E. Angelopoulou, Scene illumination as an indicator of image manipulation,Inf. Hiding, vol. 6387, pp. 66– 80, 2010

[14] Tiago and Christian et al Exposing Digital Image Forgeries by Illumination Color Classification. IEEE Transactions on Information Forensics and Security (Page: 1182 – 1194)Year of Publication: 2013.

[15] Reshma P.D and Arunvinodh C, “IMAGE FORGERY DETECTION USING SVM CLASSIFIER”, IEEE International Conference on Innovations in Information, Embedde and Communication Systems (ICIIECS), 2015.

[16] Pravin Kakar , Sudha Natrajan, Wee Ser,“Exposing Digital Image Forgeries by detecting Through discrepancies in Motion Blur” in IEEE Transactions On Multimedia ,Vol.13,No.3,June 2011.

[17] Zhipeng,Chen,Yao and Rongrong Ni, “Forensics blurred images based on no-reference image quality assessment” in IEEE, 2013.