International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 152 – 155

Review of Digital Image Forgery Detection

Jigna J. Patel
Ph. D Research Scholar
Computer Engineering Department
Dr.S & S.S.Ghandhy Government Engineering College,
Surat.
jigna2012me@gmail.com

Dr.Ninad Bhatt
Professor & Head
Electronics and Communication Department
C.K Pithawalla College of Engineering Technology,
Surat.
ninad.bhatt@ckpcet.ac.in

Abstract: Forgery in digital images can be done by manipulating the digital image to conceal some meaningful or useful information of the image. It can be much difficult to identify the edited region from the original image in various cases. In order to maintain the integrity and authenticity of the image, the detection of forgery in the image is necessary. Adaption of modern lifestyle and advanced photography equipment has made tempering of digital image easy with the help of image editing soft wares. It is thus important to detect such image tempering operations. Different methods exist in literature that divide the suspicious image into overlapped blocks and extract some features from the images to detect the type of forgery that exist in the image. The image forgery detection can be done based on object removal, object addition, unusual color modifications in the image. Many existing techniques are available to overcome this problem but most of these techniques have many limitations. Images are one of the powerful media for communication. In this paper a survey of different types of forgery and digital image forgery detection has been focused.

Keywords: *Cloning, Splicing, Retouching, Morphing, Copy-Move Forgery*

*****

I. INTRODUCTION

Digital image forgeries are common nowadays as many picture editing soft wares are easily available and the use of digital images has become much popular among common men. Also digital cameras and computers has become cheap and easily available to people, so visually identifying forgeries is difficult for humans .One cannot identify whether the image is original or manipulated. Images can be manipulated by deleting a part of image or hiding some region in the image or by modifying the image to misrepresent the image information. Such vulnerabilities decreases the credibility and authenticity of digital images .As images can be used in some very important areas such as medicine, astronomy, surveillance, etc. therefore image should be it is necessary to recognize this type of doctored images. Various algorithms are proposed in recent years to detect image forgery. They can be classified into two categories: active and passive or blind algorithms. In active approach, watermark or digital signature is embedded into the image. Embedding watermarks in the image requires specially equipped cameras, so, the use of this method in practice is very limited. In contrast to this, the passive techniques do not need to embed any watermark in the image or no digital signature is required to be generated.

In passive approaches detection of duplicated objects is done in forged images without need of original image watermark. Detection of forgery depends upon the evidence of traces left on the image by different processing steps during image manipulation. The amount and location of forgery in the image can also be determined with passive approach.

It can be further classified into two approaches:

Image source identification- where it can identify the device that has been used for capturing the digital image. It can identify whether the image is computer generated or digital camera image but the location of forgery in image cannot be determined.

Tampering detection- It detects the tampering done in the image deliberately for malicious purposes.

Passive approaches for image forgery detection can further be divided into five categories:-

1.Pixel-based techniques

It detects the statistical anomalies that are introduced in the image at the pixel level.

These techniques can further be categorized as cloning, resampling, statistical and slicing.

2.Format-based techniques

It leverage the statistical correlations introduced by a specific lossy compression scheme in the image

It can be further classified into JPEG Quantization, Double JPEG, and JPEG blocking. It detects forgery even in compressed image.

 ISSN: 2321-8169
152 – 155

3.Camera- based techniques-

It exploits the artifacts introduced in the image by the camera lens, sensor, or on-chip post-processing. The detection technique includes chromatic aberration, color filter array, camera response and sensor noise which detects traces of tampering introduced at various stages of imaging process.

4.Physical environment-based techniques

It can explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera;

These techniques can further be classified as: Light Direction 2D, Light Direction 3D, and Light environment.

5.Geometry-based techniques

It makes the measurements of objects in the world and their positions relative to the camera to detect the forgery in the image.

Principal points and Metric measurements are example of this technique.

Advantage of passive approach for image forgery detection:

The images which are already forged can be catered using passive approach while in active approach it cannot gain any profit.

Disadvantage of passive approach:

In this technique assumes that tempering cannot be visually recognized, so they require different statistics of an image. Therefore this technique is complex.

I. TYPES OF DIGITAL IMAGE FORGERIES

Digital image forgery can be divided into five categories:-

1. **Copy-move (cloning) forgery :**

In this type of forgery, image is manipulated by copying a part of image and pasting it into another part of the same image.

There are at least two similar regions in a tampered region due to region duplication.

Fig.1. copy-move attack [1]

Fig.1 shows copy-move attack where left side shows original image which contains three rockets and right side shows forged imaged with four rockets. [1]

2. **Image Splicing:**

In this type of forgery fragments of same or different images are combined to produce a single forged image without further post processing such as smoothing of boundaries among different fragments.

Fig.2 Image Splicing [1]

Fig. 2 shows image splicing where different elements from multiple images (right) are juxtapose in a single image (left) to create forgery. [1]

3. **Image Retouching:**

In this type of forgery image is enhanced by performing slight changes in the image or reducing certain features in the image. Various image editors are used which can change the background, fill some attractive colors, and work with hue saturation for toning and balancing of the image.

Fig.3 Image Retouching [1]

Fig. 3 shows an example of image retouching, where real face is on the right and left shows the retouched version of it. [1]

4. **Morphing:**

In this type of forgery one image is transformed into another through a smooth transition between two images. Transformation is done by cross-dissolving two images.

Fig.4.Morphing[1]

Morphing is shown in Fig.4 where left and right images are the original image and middle one is the morphed image. [1]

5. **Enhanced:**

In this type of forgery image is manipulated by several enhancement operations (like changing color in the image, blurring the background of the image etc.) are performed over the image to make objects more visible.

Fig.5 Enhanced Image [1]

The original image shown is upper left corner of Fig. 5, followed by various enhancements such as color change, blurring of background and finally the enhanced image on the lower right corner. [1]

II. RELATED WORK

In 2011, Najah Muhammad et al[2],proposed an efficient non-intrusive method for copy-move forgery detection that can effectively detect tampering on the image and does not require any knowledge about the camera and also does not need a large number of images for the decision making process. They used DyWT decomposition of the image for extracting the smoothed and the high frequency versions of each segment. However they have tested their algorithm for images where the background is simple and images having complicated background and texture are not used by them.

In 2014 Shahana N Youseph et al[3], presented a new method for detecting forged images of humans using the illuminant color Estimation. Author has mainly focused on common form of image manipulation such as image splicing. They generated a map of estimated illuminant color from illuminant color estimation using Pixel and Edge based methods. The authors used Canny edge detector to obtain edges of illuminant map for the extraction of shape features using HOG Edge descriptor. Histogram of oriented gradients and color moments features were tested separately by the author with different illuminant estimation methods and combination of these two features was used by them for forgery detection. Combined HOG Edge and color features had given more accuracy than the methods that use shape and color features separately. Accuracy was estimated by them using SVM Classifier. The Combined feature extraction with weighted gray edge testing process had given them 74% of accuracy.

In 2014, Davide Cozzolino et al[4],proposed image forgery localization by a fusion of camera –based, feature-based and pixel-based techniques. This technique proposed by them detects the forgery present in the image by detection of the Photo Response Non Uniformity (PRNU) noise which is present in all pristine images produced by the camera but absent in tampered areas. They had used SVM (Support Vector Machine) classifier and an index-SDH (Sum of Distancesfrom the Hyperplane) to obtain better results.

In 2016, Yuan Rao et al [5], proposed a new image forgery detection method based on deep learning technique, which utilizes a convolutional neural network (CNN) to automatically learn hierarchical representations from the input RGB color images. CNN proposed by them is specifically designed for image splicing and copy-move detection applications. Instead of a random strategy, the weights at the first layer of their network were initialized with the 30 basic high-pass filters used in spatial rich model (SRM) for image steganalysis, which helps to efficiently suppress the effect of complex image contents and accelerate the convergence of the network. They have carried out extensive experiments on several public datasets which demonstrates the superior performance of the proposed by them.

In 2016, Ira Tuba, Eva et al [6], proposed an algorithm for digital image forgery detection that deals with the situation when some object, together with its shadow, is copied and pasted to some other location in the same or different image. They have used local binary patterns from shadow and adjacent non-shadow regions and features extracted from their histograms where energy and entropy

proved to be the most discriminative. Authors have used uniform pattern LBP(local binary pattern)as texture feature .They have tested this method on some benchmark forged images and compared with other approaches from literature where it proved to be successful in detection of this type of forgery. However, the limitation of the method is that it can only be used for regions that include shadow.

In 2016, Ashwini V Malviya et al[7],proposed a method for detecting copy-move forgery or cloning. Authors proposed ACC (Auto Color Correlogram) which is a simple and a low complexity feature extraction scheme.It is effective in detecting multiple copy-move forgeries in same image.

In 2016 Tae Hee Park et al [8], proposed an image splicing detecting method using the characteristic function moments for the inter-scale co-occurrence matrix in the wavelet domain. Authors have constructed the co-occurrence matrices by using a pair of wavelet difference values across inter-scale wavelet subbands. Their method can be applied regardless of the color or gray image dataset using only luminance component of an image. Authors have proposed method achieves good performance in splicing detection. Results of experiments done by the authors showed that the detection accuracy was greater than 95 % on average with well-known four splicing detection image datasets.

In 2016,Vanita Agarwal et al[9] presented mirror-reflection invariant feature transform (MIFT),basically used for flipped images which creates descriptors that are invariant to flipping and proved it to be better than scale invariant feature transform (SIFT). Authors demonstrated on various databases such as MICC-F2000 and CASIA V2.0. From the experimental results, they found that MIFT works for almost all types of transformations including reflection.

In 2017,Bhavya Bhanu M P et al[10] presented a Copy-Move forgery detection technique using segmentation. For segmentation the authors have used (SLIC) is super pixel extraction (segmentation) method based on k-means clustering and SURF (Speeded Up Robust Features) for feature extraction. The technique proposed by them reduces time required for forgery detection and also reduces false positive rate.

III.CONCLUSION:

Digital images are being adopted in various areas as information providers. Therefore, the chances of tempering the images also increase as many software applications and image editing tools are easily available. Copy-move forgery is most common problem that is being faced in many areas. Several algorithms are designed and various techniques are adopted to detect the copy-move forgery. Block-based method or key point-based methods are commonly used for detection of copy – move forgery. Each of these methods have some advantages and disadvantages .Therefore new algorithms and methods that combines both the block based and the key point based methods can be developed which aims to improve the accuracy.

REFERENCES

[1] Rani Susan Oommen, Jayamohan M and Sruthy S," A Survey of Copy-Move Forgery DetectionTechniques for Digital Images", IJIET'2016.

[2] Najah Muhammad, Muhammad Hussain, Ghulam Muhammad, and George Bebis," Copy-move forgery detection using dyadic wavelet transform",IEEE'2011.

[3] Yuan Rao, Jiangqun Ni," Pixel and Edge Based Illuminant Color Estimation for Image
Forgery Detection", Elsevier'2015.

[4] Davide Cozzolino, Diego Gragnaniello and Luisa Verdoliva ,"Image forgery localization through the fusion of camera- based ,feature –based and pixel-based techniques", IEEE'2014.

[5] Yuan Rao and Jiangqun Ni,"A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images",IEEE'2016.

[6] Ira Tuba, Eva Tuba, and Marko Beko ,"Digital Image Forgery Detection Based on Shadow Texture Features", IEEE'2016.

[7] Ashwini V Malviyaa and Siddharth A Ladhakeb, "Pixel based Image Forensic Technique for copy-move forgery detection using Auto Color Correlogram",Elsevier'2016.

[8] Tae Hee Park, Jong Goo Han, Yong Ho Moon and Kyu Eom, "Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain", Springer'2016.

[9] Vanita Agarwal and Vanita Mane ,"Reflective SIFT for Improving the Detection of Copy-Move Image Forgery" , IEEE Computer Society'2016.

[10] "Copy-Move Forgery Detection Using Segmentation", Bhavya Bhanu M P Dr. Arun Kumar M N,IEEE'2017.

[11] Xu Bo, Wang Junwen, Liu Guangjie and Dai Yuewei ,"Image Copy-move Forgery Detection Based on SURF",IEEE Computer Society'2010.

[12] Harpreet Kaur and Kamaljit Kaur," Image Forgery Detection Using Steerable Pyramid Transform and LAB Color Space", IJARCSSE'2015.

[13] Ahmet Emir Dirik and Nasir Memon,"Image Temper detection based on demosiacing artifacts",IEEE'2009.

[14] Yanping Huang, Wei Lu, Wei Sun and Dongyang Long," Improved DCT-based detection of copy-move forgery in images",Elsevier'2010

[15] Hany Farid, Member, IEEE ,"Exposing Digital Forgeries from JPEG Ghosts".