IMAGE SPICING FORGERY DETECTION

1SIDDHI GAUR, 2SHAMIK TIWARI

1M.Tech, 2Assistant Professor, Dept of CSE, Mody University of Science and Technology, Sikar,India
E-mail: 1siddhi.gaur14@gmail.com, 2shamiktiwari.cet@modyuniversity.ac.in

Abstract - Images nowadays are often used as validate proof for any crime and it will create issue if these images do not remain real. This leads to the issue of Image Forgery. Image Forgery means manipulation of the digital image to hide some important or useful information of the image. There are instances when it is hard to identify the modify region from the actual image. Further, it can be either active (intrusive) or passive (blind or non-intrusive). In active approach, it detects the forgery by validating the integrity of a pre-embedded (i.e. by a camera) signature or watermark. In passive approach, we do not need to embed any information. They depend on the original characteristics of the image, which let them to be widely used. This paper discusses about the image forgery detection and different forgery detection techniques namely image splicing forgery detection techniques.

Keywords - image forgery detection; intrusive, non-intrusive, image splicing forgery detection techniques

I. INTRODUCTION

Today we are living in digital world where most of the images are stored and captured in digital nature due to very low cost of digital cameras and storage, very high quality of images and ease of manipulating the images with powerful image editing tools. Also, many advance image editing tools are available online and offline with very cost effective alternatives. The ease of use and accessibility of software tools and low-cost hardware, makes it very simple to forge digital images leaving almost no trace of being subjected to any kind of tampering. As such we cannot take the authenticity and integrity of digital images for granted [1]. This type of the forgery is increasing day-by-day.

Digital images are being used as a means of pictorial information in daily newspapers and magazines as evidence in courts of law, and in the medical diagnose field. Moreover, with the spread of low-cost user friendly editing tools the art of tampering, content is no more restricted to experts. As a result, the modification of images for malicious purposes is now more common than ever.

Based on the above reasons, it is important to develop a credible method to detect a digital image is tempered, so called digital image forgery. The image forgeries can hide or add an important object in an original image to misguide the court of law. Image forensic has an important role where the authenticity of images is important in our daily and social life.

Digital Image Forgery Detection is an very important field in Image Processing, because digital images are used in many social areas like in courtrooms where they are used as evidences[2]. In information route like newspapers, magazines, websites and television, digital images are powerful tool for communication. Unfortunately, it is easy to use computer graphics, image editing software and image processing techniques to manipulate the images. These manipulated images create some unwanted problems in information routes.

The rest of the paper is structured as follows. Section 2 describes various digital image forgeries and the state of art passive methods to authenticate digital images. Section 3 tells about the related work. Finally we conclude in section 4.

II. CLASSIFICATION OF IMAGE AUTHENTICATION TECHNIQUES

The authenticity of digital images safety is a very major problem and it has increased some time ago. Many techniques have been developed for validation of the authenticity of digital images. These techniques can be described as active (intrusive) approach and blind or passive (non-intrusive) approach. The active techniques can be classified into two categories.

A. Active Approach

In this active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. However, in practice this would limit their application.

Types-  
1) Watermark-
In Watermarking, as a security structure is embedded into the image, it is such a method of active tampering detection, but the most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection. Digital watermarking techniques makes the assumption that a digital watermark also known as authentication code has been inserted at the source side into the image, and this code is being used for verifying the authenticity of the digital
information at the time of detection. They undergo the same manipulations as the image as most often these watermarks are not separable from the image content they are embedded in. The drawback involving this approach of the techniques is that at the time of recording the image, the code must be inserted into the image, or later by authorized person, which usually requires specialized camera and/or subsequent processing of the image. Another limitation is that they might result in the degradation of the image. The digital signature approach mainly involves the extraction of unique features from the image at the source, and encoding them to form digital signatures. At a later time these signatures are used for the verification of these images. The usages of techniques involving these approaches also suffer the same limitations as the watermarking techniques.

B. Passive Approach
Passive image forensics is usually a very great challenge in image processing techniques. The passive approaches since they do not have any prior information about the image features are also known as blind approaches. These methods use the image only for validating the authenticity or integrity of the image. Using the passive approach, image forensic techniques works on the assumption that although these forgeries leave no tampering traces visually, they might alter the statistical properties, often referred to as the digital fingerprints of the image that characteristic the life cycle of the image from its acquisition to its processing. The alterations to the image, results in the distortion of these fingerprints, thereby giving inconsistencies of the image. In order to detect the tampered regions, if any the passive techniques apply techniques for the verification of these inconsistencies in the image.

There are several different types of forgeries being applied to images, some of which commonly used are the copy-move forgery, image splicing, image retouching, forgeries using JPEG compression properties, using lighting inconsistencies, projective geometry and transformations, chromatic aberration, color pixel array and inter-pixel correlations, noise variations, sharpening and blurring etc.

Types-
There are several types of digital forgery. Each instance falls into one of three major categories, depending on the process used in the image’s creation. These groups consist of Image Retouching, Image Splicing, and Copy-Move.

1) Copy-move Forgery
Copy-Move is a special type of image manipulation technique in which a part of the image itself is copied and pasted into another part of the same image wherein a part of the image is being copied and pasted to another part of the same image[3]. The copy move forgery is popular as one of the difficult and most commonly used kind of image tampering technique. In this technique, one needs to cover a part of the image in order to add or remove information. In the Copy-Move image, manipulation technique a part of the same image is copied and pasted into another part of that image itself. In a copy-move attack, the intention is to hide something in the original image with some other part of the same image [4]. The example of Copy-Move type is as shown in below figure 1 below. The original image contains only three missiles and its Copy-Moved version on the right has four missiles.

![Fig.1.Example of Copy-Move Attack on Image](image)

2) Image Retouching
Retouching is defined as hanging the image on a whole. For example by adding onto brightness, creating noise, creating clarity onto the base images etc. It is considered to be the very less harmful kind of digital image forgery than other types present. In case of image retouching, original image does not significantly changes, but there is enhancement or reduces certain feature of original image. This technique is popular among magazine photo editors. This type of Image forgery is present in almost all magazine cover that would employ this technique to enhance certain features of an image so that it is more attractive. Actually, the fact is that such enhancement is ethically wrong. In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative 6]retouching [5]. Image is carried out to either reduce or improve certain features of the image. Retouching may require rotation, scaling, or stretching of an image before combining it with other image.

3) Image Splicing
Image Splicing is defined as a paste-up produced by sticking together photographic images. This technique for making forgery images is more aggressive than image retouching. Image splicing is fundamentally simple process and can be done as crops and pastes regions from the same or separate sources.

Image splicing is a common type to create a tampered image where a region from one image is copied and pasted into another image which produces composite image called spliced image; cut and join two or more
snaps of pictures. The complicated forgery may include some post-processing like blurring, JPEG compression, etc. that performs the forgery detection very hard. Examples include several infamous news reporting cases involving the use of faked images. Fig. 2 below shows how to create forge Image; by copying a spliced portion from the source image into a target image. The left picture is the base image and the right one is the spliced image as in that case some cropped image is pasted over the base image and new image is generated.

III. IMAGE SPICING

Image Splicing is a common form of digital image manipulation or image forgery. It is one such type of tampering; also called as image composition. The basic definition of image splicing is a process that crops and paste regions from same or separate sources. The following figure 3 shows one of the example form of image splicing process and its steps[6].

![Image Splicing](image_splicing.png)

**Fig.3. The steps of image splicing, f(x,y) and g(x,y) are original images, h(x,y) is a part of f(x,y) which is insert into g(x,y) and generate spliced image I(x,y). Perhaps f(x,y) and g(x,y) is the same image.**

As shown in above figure 4, by copying a spliced portion from the source image (4a) into a target image (4b). One can create a composite picture (4c) or scenery to cheat others with the help of start-of-art images editing software [6], even non-professional users can perform splicing without much difficulty.

IV. LITERATURE REVIEW

Zhehua and Guoping proposed an automatic detection framework to identify a spliced image, which is fully based on Human Visual System model in which visual saliency and fixation are used as a forensic cue [7]. This technique provides a convenient way to locate splicing boundaries, but this system needs some training for users.

Servinc and Ismail proposed a method based on the neighbor bit planes of the image. The basic idea is the correlation between the bit planes as well as the binary texture characteristics within the bit planes will differ between an original and a spliced image, which is considered for detecting splicing [8]. This method provides better performance at both stronger and weaker level of manipulation, but in order to identify the spliced image this method requires various image forensic detectors.

Farid method consider the fact that while creating a digital composite image the matching of lightning conditions of digital image is difficult between the individual photographs[9], this inconsistencies in lighting can be used as a factor for detecting digital tampering. But the main drawback with this approach is it is not applicable for indoor images.

Alin and Farid proposed a method to detect the spliced image by detecting traces of resampling. When creating digital forgeries, it is often necessary to scale, rotate or distort a portion of an image. This process involves resampling the original image onto a new lattice, which resampling rates used for exposing digital forgeries [10]. This method offers a complementary approach to authenticating digital images, but it’s only applicable for uncompressed TIF &JPEG image with minimal compression.

Alin and Farid again proposed an automatic method for detecting traces of digital tampering in lossless & lossy compressed image by using color Filter Array[11]. Most digital cameras employ a single sensor in conjunction with a CFA, where the missing color samples are interpolated from these recorded samples to obtain a three channel color image. This interpolation introduces specific correlations which are likely to be destroyed when tampering with a digital image. As such, the presence or lack of correlations produced by CFA interpolation can be used to declare it as a forgery. This technique works in the absence of any digital watermark or signature to authenticating digital images, but this will not be the case in practical.
Johnson and Farid proposed a method based on the specular highlights that appear on the eye are a powerful cue to shape, color and location of the light source [12]. Inconsistencies in these properties of light can be used as evidence of tampering. It can applicable to arbitrary objects, but this method only determines the direction to the light source within one degree of ambiguity.

Riers & Angelopoulou proposed illumination color as a new indicator to distinguish the original and manipulated image [13]. The basic idea is that if an image has been manipulated, the transition between the illuminants should be disturbed. The disturbed illuminants can be used as a best indicator for identifying image authenticity; but it requires the original image for comparison process.

Feng and chang proposed a fully automatic spliced image detection method, which is based on consistency checking of camera characteristics among different areas in an image [14]. From each area using geometric invariants camera response functions (CRF) is determined. The boundary between the authentic or spliced regions is segmented by classifiers. This method provides high performance, but the rate of detection of splicing is not to the expected level.

Chennamma & Lalitha proposed a detection method based on the spherical lens which introduces radial distortion [15]. This radial distortion parameter estimated and their consistency is verified for the detection of splicing. The efficiency of this method depends on the resolution of the images.

Eric and Hany put forth a method which estimates the lightning conditions of the digital composite image in 3-D environment and the same estimate is used as a evidence for detecting tampering [16]. This method is very powerful in tampering analysis.

Farid & Bravo proposed an automatic detection method for identifying faked pictures without the involvement of HVS (Human Visual System) [17], which shows the visual system is remarkably improper to detecting geometric inconsistencies in shadows, reflection and perspective distortion. But the process of detection is time consuming.

Xuemxin & Zhen locate the splicing area by exploiting illuminant color inconsistency [18]. This method detects image splicing and also locates the spliced region, is not applicable for indoor images and original image is necessary to find the duplication or manipulation.

Pravin, Sudha and Ser proposed a novel method for detecting image splicing using discrepancies in motion blur. In which they used motion blur estimation through image gradients in order to detect inconsistencies between the spliced region and rest of the image [19]. This method needs very less human intervention, improves robustness and efficiency.

Shinteng & Tsan proposed a fast and effective forgery detection technique for copy-move and image splicing forgery, which focuses on JPEG format image and detect both image forgeries [20]. This method is mainly used to find the Copy-and-Paste operation of image regions from one image onto another.

James F.O’Brien & Harry proposed a new forensic technique has emerged to detect geometric or statistical inconsistencies that result from specific forms of Photographic manipulation [21], but the human visual system is needed to identify the corresponding points on objects and it’s reflections.

Pan, Xing & Lyu describes a method based on the fact that the images from different origins tend to have different amount of noise introduced by the sensors [22]. They proposed an effective method to expose image splicing by detecting the inconsistencies in local noise variances. But the main this method is not able to detect the entire tampered region.

Kekre, Misha, Pallavi, Shede & Gupta proposed a new method based on image hashing, which is used to generate hash value for each image in the database [23], these hash values can be used for content based image retrieval, image database indexing, image authentication and also avoiding & mitigating the tampering of digital images. The only limitation of this technique is the original image is needed for find duplication.

Zahra Mohamadian and Ali Akbar pouyan proposed a method to detect forgery in digital images in uniform and non-uniform regions in which Zernike moments based detection approaches is used to detect flat copied regions [24]. If the images are rotated, scaled or distorted this method will fail to identify the forged image.

Munkhbaatar & Rhee proposed a blind forgery detection scheme using compatibility metrics based on edge blur and lightning directions [25]. The edge blur width is used to identify the discontinuities of edge in spliced image and the lightning directions are used to enlighten the image composition.

**CONCLUSION**

Nowadays image splicing image forgery is becoming a common way the anti-social people are using to create the fake photographs and misusing them. So it is necessary to identify such kind of image manipulations. So many researchers have already
been carried out on image splicing. But the existing methods of detecting image splicing undergo the following challenges: original image is essential for revealing tampering, forgeries with indoor image and image resolution. We have analyzed several methods proposed in research papers to detect image composition to insist the necessity for image splicing detection. This field is still growing and a lot of research is needed to make Digital forensic more promising.

REFERENCES