International Journal of Emerging Trends in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2, Issue 3(May-June 2015), PP 91-95

Digital Image Forensics

Prof. B P Dharaskar[1], Prof. G J Tripathi[2], Prof .S R Dhabarde[3]
[12]*(Department of CSE. Priyadarshini Indira Gandhi College of Engineering/ RTMNU, India)*
[3]*(Department of CSE. Priyadarshini Indira Gandhi College of Engineering/ RTMNU, India)*

Abstract:- Digital visual media represent nowadays one of the principal means for communication. Lately, the reliability of digital visual information has been questioned, due to the ease in counterfeiting both its origin and content. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. In this paper, we discuss several techniques for identifying digital image source and forgeries detection.

Keywords: - CFA, CMOS, CCD, DIF, FPN, PRNU

I. INTRODUCTION

Images and videos have become the main information carriers in the digital era. The expressive potential of visual media and the ease in their acquisition, distribution and storage is such that they are more and more exploited to convey information, even sensible. As a consequence, today images and videos represent a common source of evidence, both in every-day life controversies. The simplest video in TV news is commonly accepted as a certification of the truthfulness of the reported news. Together with undoubted benefits, the accessibility of digital visual media brings a major drawback. Image processing experts can easily access and modify image content, and therefore its meaning, without leaving visually detectable traces. Moreover, with the spread of low-cost, user friendly editing tools, the art of tampering and counterfeiting visual content is no more restricted to experts. As a consequence, the modification of images for malicious purposes is now more common than ever. Digital Image Forensics is that branch of multimedia security that aims at contrasting and exposing malicious image manipulation.

II. ROLE OF DIGITAL IMAGE FORENSICS IN MULTIMEDIA SECURITY

Digital Image Forensics (DIF) is a quite recent discipline, it is tightly connected with a number of different research fields. DIF inherits its goals and attitude from classical (analog) forensic science and from the more recent field of computer forensics. Forensic disciplines in general aim at exposing evidence of crimes; to do so, they have to deal with the burglars' ability in either hiding or possibly counterfeiting their traces. In digital imaging both the acquisition process and the tampering techniques are likely to leave subtle traces. The task of forensics experts is to expose these traces by exploiting existing knowledge on digital imaging mechanisms. For better grasping the mission of image forensics investigators, it might be useful to explore the relationships between DIF and other multimedia security-oriented disciplines. Image processing for forensics shares indeed several challenges and similar techniques with digital watermarking and Steganography.

i) Digital watermarking consists in hiding a mark or a message in a picture in order to protect its copyright.

ii) Steganography consists in communicating secretly via some media (in particular images and videos). The choice of the cover is not really important here. Also, one can assume that the stego-picture will not undergo photometric or geometric attacks among the transmission. The main point for two persons who communicate some information using this technology is to be not detected by a third party. However, Digital Image Forensics has a very precise role among multimedia security disciplines: authenticating images for which no reference is known and no previous integrity protection has been set and to detect forgery in an existing image.

III.IMAGE SOURCE DEVICE IDENTIFICATION [2]

Introduction:-

In tracing the history of an image, identifying the device used for its acquisition is of major interest. In a court of law, the origin of a particular image can represent crucial evidence; the validity of this evidence might be compromised by the (reasonable) doubt that the image has not been captured from the device it's claimed/supposed to be acquired with, as in the case of video-surveillance material or covert videos. Helpful clues on the source imaging device might be simply found in the file's header (EXIF) or by checking (if present) a watermark consistency. However, since this information can be easily modified or removed, it cannot always be used for forensics purposes. As a consequence, blind techniques are preferred for the **acquisition device identification**. Blind image forensics techniques take advantage of the traces left by the different processing steps in the image acquisition and storage phases. These traces mark the image with some kind of camera fingerprint, which can be used for authentication.

The techniques presented in the following retrieve information on the source device at two different levels. As a first attempt, they try to distinguish between different camera models. On a second, more informative and challenging level, the goal is to distinguish between single devices, even different exemplars of the same camera model. To illustrate clearly the identification steps in the image acquisition and storage processes. In reviewing existing techniques, I would like to warn the you that no direct performance comparison is available between different methods. It is our belief, though, that this useful tool will be soon exploited by the community to have a clearer view on the state of the art of acquisition device identification methods.

Principle:-

When capturing a digital image, multiple processing steps are performed prior to the storage. The Light enters the imaging device through a system of optical lenses, which conveys it towards the imaging sensor. The imaging sensor is the heart of every digital camera, and it is composed of an array of photo detectors, each corresponding to a pixel of the final image, which transform the incoming light intensity into a proportional voltage. Most cameras use CCD (Charged Coupled Device) sensors, but CMOS (Complementary Metal Oxide Semiconductor) imagers can also be found. To render color, before reaching the sensor the light is filtered by the Color Filter Array (CFA), a specific color mosaic that permits to each pixel to gather only one particular light wavelength (i.e. color). The CFA pattern arrangement depends on the manufacturer, although Bayer's filter mosaic is often preferred. As a result, the sensor output is a mosaic of e.g. red, green and blue pixels arranged on a single layer. Before the eventual storage, additional processing is performed, such as white balance, gamma correction, and image enhancement. Finally, the image is recorded in the memory device. Also in this case the format can vary, but a common choice is JPEG. The described image acquisition pipeline is common for most of the commercially available devices; nonetheless, each step is performed according to specific manufacturer choices, and hence might depend on the camera brand and model. This variation can be used to determine the type of camera from which a specific image was obtained. Indeed, each stage in the pipeline can introduce imperfections in the final image or characteristic traits: lens distortion, chromatic aberration, pixel defects or CCD sensor imperfections, statistical dependencies related to proprietary CFA interpolation algorithms and other intrinsic image regularities which leave tell-tale footprints. These artifacts are statistically stable and can be considered as a signature of the camera type or even of the individual device. In addition, some techniques focus on statistical regularities in the image such as color or compression features. Each of the techniques presented in the following section has been proved to be effective to some extent in identifying the acquisition device. However, the scope of most of them is limited to the discrimination between different camera models. Sensor imperfections seem to be at this stage the only traits able to distinguish between different exemplars of the same camera model. Therefore, recent studies mostly concentrate on exploiting sensor imperfection. *C.*

Forensics methods for image source identification:-

1. Identification through artifacts produced in the acquisition phase.

Due to each lens and image geometries and to the design of the camera, lenses produce distortions (aberrations) in the captured images. Radial distortion for example deforms the image so that straight lines in object space appear as curved lines.

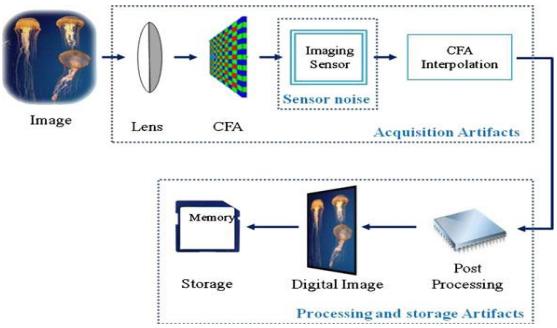


Fig1: A schematic view of a standard digital image acquisition pipeline.

Choi et al. propose to analyze this kind of lens aberration as a fingerprint to identify the source camera. The authors find the distortion parameters of a camera using Devernay's line extraction method, to then measure the error between the distorted line segment and the corresponding straight lines. The estimated parameters can be used to train a classifier to distinguish among images captured by different cameras. The method achieves good discrimination rates among different models of cameras but no proof of robustness is given for distinct exemplars of the same model.

Identification through sensor imperfections.

Imaging sensors have been shown to introduce various defects and to create noise in the pixel values. The sensor noise is the result of three main components, i.e. pixel defects, fixed pattern noise (FPN), and Photo Response Non Uniformity (PRNU). Pixel defects include point defects, hot point defects, dead pixels, pixel traps, and cluster defects, which reasonably vary across different sensors, independent on the specific camera model. Geradts et al. in attempt at reconstructing pixel defects patterns. The authors propose to determine pixel noise by taking images with black or green background with 12 different cameras and then comparing the defect points which appeared as white. Their experiments show that each camera has distinct patterns of defect pixels also across the same model; nonetheless, the impact of defect pixels closely depends on the content of the image. Furthermore, some camera models do not contain any defectives pixels or they eliminate it. Therefore, this method is not applicable to every digital camera.

Source identification using properties of the imaging device.

Exploiting the digital image acquisition process is not the only way to identify the source of an image: post-processing performed in the storage phase can also produce interesting cues. Kharrazi et al. Propose to use a set of image features to characterize a specific digital camera, assuming that the image can be affected by color processing and transformations operated by the camera prior to the storage. The authors study statistical properties of the image organized into two groups: color-related measurements, such as average pixel value, RGB pairs correlation, neighbor distribution center of mass, energy ratio and wavelet domains statistics, and image quality features. Supported by a SVM classifier, this approach shows an effective result on low compressed images taken by different camera models. However, this technique can only be applied on images depicting similar content.

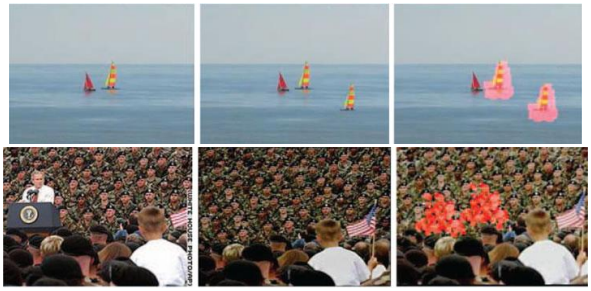
IMAGE TAMPERING [1]:-

Introduction:-

According to the Oxford dictionary, the verb to tamper literally means "to interfere with something in order to cause damage or make unauthorized alterations". In the context of digital imaging, tampering recalls the intentional manipulation of images for malicious purposes: as images are natural carriers of information, image manipulation is denoted as tampering when it explicitly aims at modifying the semantic meaning of the visual message. The story of image forgery dates back to the early twentieth century to support political propaganda actions. With the increasing use of visual content as a message conveyer, tampering techniques developed accordingly. Furthermore, with the advent of digital imaging and photo-editing software, image manipulation became affordable also for no darkroom experts, resulting in a general lack of reliability of digital image authenticity, not only in investigative activities, but, more in general, in the media and information world.

Short summary of the most common tampering techniques:-

1. Deleting undesired objects from an image is one of the most straightforward methods to alter its meaning. In such circumstances, forgers need to "fill" the region of the image from which the object has been removed. A typical solution in this case is to copy a portion of the same image and replace with it the void left from the deletion (copy-move technique). Of course, the same approach can be used to replicate objects instead of deleting them, as shown in the images of Fig. 4. To better hide this operation to the human eye, the forger can perform geometric transforms on the region to be copied, such as rotation or scaling. Furthermore, to produce a smooth transition between the (original) surround and object removal can be also achieved by means of in-painting techniques. Inspired by real techniques for painting restoration, in-painting methods fill the holes left by object removal by exploiting the information preserved in the regions surrounding the gaps.



Forgeries using multiple images as source for tampering.

The insertion in an image of material originally coming from another source is one of the most powerful tools to overturn the message contained in visual media. Modern techniques and editing software allow easy creations of image composites obtaining results that are hardly detectable by the human eye. Blending and matting techniques are again applicable to mask the boundaries of the spliced regions and to give the image a more uniform aspect.

IV.CONCLUSION:-

Thus we conclude that the field of DIF is brand new field and yet new tools, techniques are discovered by the researchers.

REFERENCES:-

[1] Photo tampering throughout history. http://www.cs.dartmouth.edu/farid/research/digitaltampering/.
[2] Digital image forensics: a booklet for beginners. Judith A. Redi & Wiem Taktak & Jean-Luc Dugelay. Published online: 24 October 2010. Online http://www.springerlink.com
[3] The Oxford dictionary online. http://oxforddictionaries.com/