Survey on Fake Image Detection Using Image Processing

Ms. Shalet Xavier[1] Ms.Steffy Francis[2] Ms.Vidhu Valsan A[3] Ms.Sheethal MS[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Sahrdaya College of Engineering and Technology, Kodakara, Thrissur, Kerala, India, Pin: 680684

Abstract— To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed image is a significant problem in authentication, which requires the development of new and efficient protection measures. The paper mainly deals with the detection of morphed images. In this digital world we come across many image processing software that produce doctored Images with high sophistication, which are manipulated in such a way that the tampering is not easily visible to naked eye. There is a need for developing techniques to distinguish the original images from the manipulated ones, the genuine ones from the doctored ones. There are number of ways of tampering an Image, such as splicing two different images together, removal of objects from the image, addition of objects in the image, change of appearance of objects in the image or resizing the image. In this paper, we present a software-based fake detection method that can be used in systems to detect different types of fraudulent activities. This Image Morphing detection technique detects traces of digital tampering and implemented using image processing with Demosaicing Algorithms. The objective of the proposed system is to enhance the security of image frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. And also it helps to differentiate the original and manipulated images and to trace the area morphed.

Key words: Image Detection, demosaicing technique

I. INTRODUCTION

In this digital world we come across many image processing software that produce doctored Images with high sophistication, which are manipulated in such a way that the tampering is not easily visible to naked eye.Image morphing has been the subject of much attention in recent years. There are various powerful tools available in market for Image morphing. Morphing technique continues to advance and many programs can automatically morph images that correspond closely enough with relatively little instruction from the user. This has led to the use of morphing techniques to create slow-motion effects where none existed in the original film or video footage by morphing between each individual frame by the technology called optical flow technology. Morphing has also seen as a transition technique between one scene to another in television shows, even if the contents of the two images are entirely different

Digital images are playing every important role in our daily life; the digital images are omnipresent right from the cover pages of journals, newspapers, magazines etc. to evidences in court rooms, teaching aids etc. Images are used everywhere either as a personal memory evidences or for official purposes .Recently, the low cost camera, sophisticated high end image processing, computer graphics software, made editing and manipulated images become easier, hence there is essential to detect the forgeries in the images. There are many types of forgeries such as morphing, copy move, compositing, retouching, etc. The image compositing is more popular one. There are some possible methodologies for identifying whether the image is manipulated or not. Image can be authenticated by Digital watermarking. Motivated by the fact that 2/3 color samples of a common photo are reconstructed by a demosaicing technique consisting of only a few formulas and this large population of reconstructed samples provides a good basis of reliable statistical characterization of the applied demosaicing technique. In this paper, we aim to accurately estimate the demosaicing formulas for diversified demosaicing algorithms. Our proposed framework employs a partial second-order image derivative correlation model, which detects both the intra-color channel and the cross-channel demosaicing correlation. A reverse classification scheme is incorporated to precisely classify the demosaiced samples into small categories, which best reveal the original demosaicing grouping. Compared with an existing method, our estimated demosaicing formulas regenerate the demosaiced samples from the sensor samples with significantly improved accuracy. Our reduced set of demosaicing features also perform significantly better in identification of 16 demosaicing algorithms in the presence of common camera post-demosaicing processes. For real applications including camera and RAW-tool identification, large-scale tests show that our proposed features achieve nearly perfect identification performances based on the cropped image blocks.

II. LITERATURE REVIEW

A camera is a trustworthy device and photos traditionally imply truth. Nowadays, this has been severely challenged. The advances of digital technology have given birth to numerous low-cost yet powerful tools which enable easy image creation, modification and distribution. Consequently, image forgery becomes commonplace in Internet and other mass media. This has brought up new challenges concerning authenticity and integrity of digital images. In recent years, passive image forensics has become a booming research area to mainly address photo-authentication related challenges such as image source identification, tampering discovery and steganalysis. Compared to active image forensic methods which require information hiding (e.g. watermarking and steganography), passive image forensics are based on detection of intrinsic image regularities or tell-tale artifacts leftover due to specific tampering operations. Since available digital images usually do not carry a watermark, much wider applications can be expected for passive image forensic approach . The different regularities are associated with different origins and their detections are useful in various forensic tasks. For instance, the work in extracts photo-response non-uniformity (PRNU) sensor

noises for individual camera identification and tampering detection. The work in estimates the demosaicing parameters for non-intrusive component forensic analysis on different camera models. Our proposed framework employs a partial second-order image derivative correlation model, which detects both the intra-color channel and the cross-channel demosaicing correlation. A reverse classification scheme is incorporated to precisely classify the demosaiced samples into small categories, which best reveal the original demosaicing grouping. The simulation results show that our proposed demosaicing features confidently outperform 2 existing demosaicing detection methods in identifying 16 demosaicing algorithms in the presence of various common post-demosaicing processes. Our proposed features are also highly effective in distinguishing different post-processes and are more sensitive to small scenery variations.[1]

Image morphing techniques can generate compelling 2D transitions between images. However, differences in object pose or viewpoint often cause unnatural distortions in image morphs that are difficult to correct manually. Demosaicing of Color Filter Array Captured Images Using Gradient Edge Detection Masks and Adaptive Heterogeneity-Projection based on spectral-spatial correlation, a novel adaptive heterogeneity-projection with proper mask size for each pixel is presented. Combining the extracted gradient/edge information and the adaptive heterogeneity-projection values, a new edge-sensing demosaicing algorithm is presented. Based on 24 popular testing images, experimental results demonstrated that our proposed high-quality demosaicing algorithm has the best image quality performance when compared with several recently published algorithms. It presents a new approach to extract more accurate gradient information on mosaic images directly. In what follows, the luminance estimation technique for mosaic images is first introduced. Then, combining the luminance estimation technique and Sobel operator , our proposed new approach to extract more gradient information on mosaic images is presented. [2]

A novel manipulation detection framework for image patches using a fusion procedure, called FusionBoost, in conjunction with accurately detected derivative correlation features. By first dividing all demosaiced samples of a color image into a number of categories, we estimate their underlying demosaicing formulas based on partial derivative correlation models and extract several types of derivative correlation features. The features are organized into small subsets according to both the demosaicing category and the feature type. For each subset, we train a lightweight manipulation detector using probabilistic support vector machines. FusionBoost is then proposed to learn the weights of an ensemble detector for achieving the minimum error rate. By applying the ensemble detector on cropped photo patches from different image sources, large-scale experiments show that our proposed method achieves low average detection error rates of 2.0% to 4.3% in simultaneously detecting a large variety of common manipulation attempts for image patches from several different source models. Our framework shows good learning efficiency for highly imbalanced tasks. In several patch-based detection examples, we demonstrate the efficacy of the proposed method in detecting image manipulations on local patches.[3]

In this digital world we come across many image processing software that produce doctored Images with high sophistication, which are manipulated in such a way that the tampering is not easily visible to naked eye. The authenticity of a digital image has become a challenging task due to the various tools present in the photo editing software packages. There are number of ways of tampering an Image, such as splicing two different images together, removal of objects from the image, addition of objects in the image, change of appearance of objects in the image or resizing the image. This Image Morphing detection technique detects traces of digital tampering in the complete absence of any form of digital watermark or signature and is therefore referred as passive. So there is a need for developing techniques to distinguish the original images from the manipulated ones, the genuine ones from the doctored ones. In this paper we describe a novel approach for detecting Image morphing. The new scheme is designed to detect any changes to a signal. We recognize that images from digital cameras contain traces of re-sampling as a result of using a color filter array with demosaicing algorithms. Our results show that the proposed scheme has a good accuracy in locating tampered pixels.[4]

The multimedia applications are rapidly increasing. It is essential to ensure the authenticity of multimedia components. The image is one of the integrated components of the multimedia. In this paper ,we designing a model based on customized filter mask to ensure the authenticity of image that means the image forgery detection based on customized filter mask. We have satisfactory results for our dataset. Image compositing is most popular image forgery. The figure 1 shows the creation of image compositing. The photo compositing is the result of cutting and joining a two or more photographs with seamless transition without leaving any visual clues about the joining from other photographs. The image compositing is also known as photomontage and image splicing. The image compositing detection assumes that the image scene authenticity properties and conditions such as illuminations, object surface properties, shadow, noise, inter-reflections. Perspective and projective views etc. are rare and difficult match in a composite image. The image composite detection techniques are able to detect the above inconsistent properties in different parts of the same images, the image edges, boundaries and colors, and image qualities may be affected by image compositing. The image forgery can be identified by the specific patterns relating to image attributes which disturbed by the forgery operations. Particularly image composting is created by the two or more images sources, naturally all the different images are taken from the different devices and at different world view conditions. The host image conditions are expected to reflect in image portions of the altered images. The abrupt and unnatural luminance levels, colors and edges are able to detect the image forgeries.[5]

Image processing is often not necessary for image manipulation detection. For instance, a picture supposed to be taken in India that shows the China monument in the background will be suspect by inspection. Detection of incongruous textural features, however, may require substantial image processing. The manipulation are sometimes not noticeable by human eye, they do affect the

statistics of the image, because of detection of tampering is possible. Thus it becomes very important to develop efficient techniques which may detect these forgeries which are addition of an object in image, removal of object from image and change of appearance of the object in image. The process of Image morphing detection can involve several works. These work include, but are not limited to, evaluation of image structure issues include discovery of artifacts consistent with image manipulation or degradation, metadata analysis, and indications of provenance and Image content issues include continuity issues, evidence of manipulation, evidence of staging, and misplacing. There are several possible techniques for detecting manipulation in the source of a digital image. Image can be authenticated by Digital watermarking. Digital watermarking has two classes of watermarks, fragile and robust. Robust watermarks techniques are designed to be detected even after attempts are made to remove them. Fragile watermarks techniques are used for authentication purposes and are capable of detecting even minute changes of the watermarked content. But, neither type of watermark is ideal when considering "information preserving transformations (such as compression) which keep the meaning or expression of the content and "information altering" transformations (such as feature replacement) which modify the expression of the content.[6]

Fig. 1: When demosaicing is performed with linear interpolation, the original green pixels have higher variance than the interpolated green pixels. The spatial pattern of variances is the basis for detecting the presence of demosaicing. The green photosites pixel values in the Bayer array are IID with variance σ2, the above image shows the variance from which each pixel value is drawn.

Nowadays Digital images are manipulated due to the availability of the image processing and editing softwares. Using these softwares we can add or remove important features from an image without leaving any obvious traces of tampering. In this paper we discuss on the detection of a special type of digital forgery that is copy-move attack in which part of the image is copied and pasted and also investigate the problem and describing an efficient and reliable detection method . The method may successfully detect the forgerd part even when the copied area is enhanced to merge it with the background and when the forgerd image is saved in lossy format, such as JPEG. To tamper an analogue video, one can easily digitize the analog video stream, upload it into a computer, perform the forgeries, and then save the result in the NTSC format on an ordinary videotape. Digital watermarks have been proposed as a means for fragile authentication, content authentication, detection of tampering, localization of changes, and recovery of original content. While digital watermarks can provide useful information about the image integrity and its processing history, the watermark must be present in the image before the tampering occurs.In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. Textured areas, such as grass, foliage, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily understand any suspicious artifacts. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image.[7]

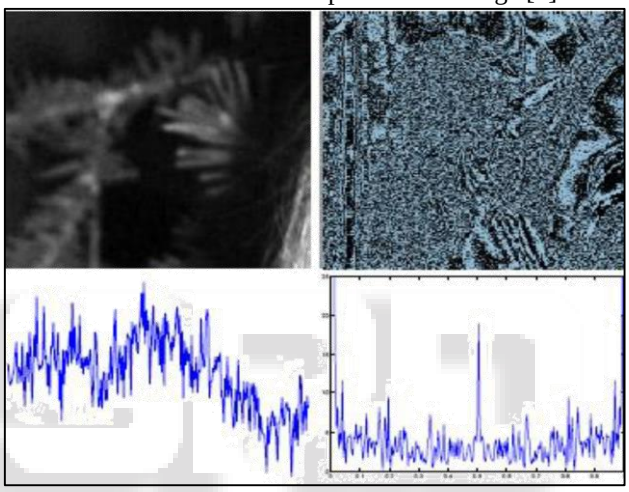

Fig. 2: Distinguish between images containing noise with large energy across the frequency spectrum and true demosaicing signals generated by our algorithm. Bottom Left: The signal , which represents an calculation of the variance along each image diagonal. Bottom Right: The spectrum of , represents the characteristic peak at.

Digital Photo images are everywhere, on the covers of magazines, in newspapers ,in courtrooms ,and all over the internet. In this paper we propose methodologies to identify such unbelievable photo images and also identify forgerd region by given only the forgerd image. Formats are additive tag for every file system and contents are relatively expressed with extension based on most popular digital camera uses JPEG and other image formats like png, bmp,etc. We have designed algorithm to find the abnormal anomalies and identify the forgerd regions. Different keywords are using this purpose such as Digital image, Forgery region, Copy-move Copy-create. Composition is experimented by the Photographers, i.e., combining multiple images into one. Digital images offer many attributes for tamper detection algorithm to take advantage of specifically the color and brightness of individual pixels as well as an image's resolution and format. This paper focuses on images saved in the JPEG format. Other fundamental properties of any digital forgery are used to develop additional detection technique such as direction filter, which is used to detect the forgery region . Photo image forgery is classified in to two

categories. The first class of image forgeries includes images tampered by copying one area in an image and pasting it onto another area. It is called as Copy-Move Forgery or Cloning. The second class of forgeries is copying and pasting areas from one or more images and pasting on to an image being forged. [8]

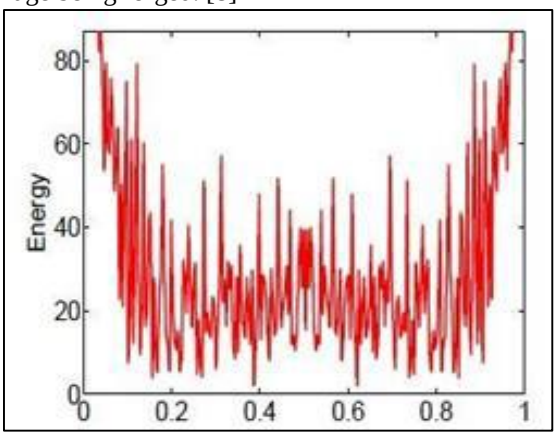

Fig. 3: PRCG Image example.performance curves are generated.

Image Forgery is defined as adding or removing important features from an image without leaving any obvious traces of tampering. Further, it can either be intrusive (active) or non-intrusive (blind or passive). In 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. Watermarking is such a method of active tampering detection, as a security structure is embedded into the image, but most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection. Signature is such a method of active tempering detection, in which signature is embedded into the image as a security means. Passive image forensics is usually a great challenge in image processing techniques. It includes the concept of Copy-Move Forgery, Retouching and Image Splicing. 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.Retouching is defined as hanging the image on a whole. For example by adding onto brightness, creating noise, creating clarity onto the base image etc.Image-splicing is defined as a paste-up produced by sticking together photographic images. 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 is 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.[9]

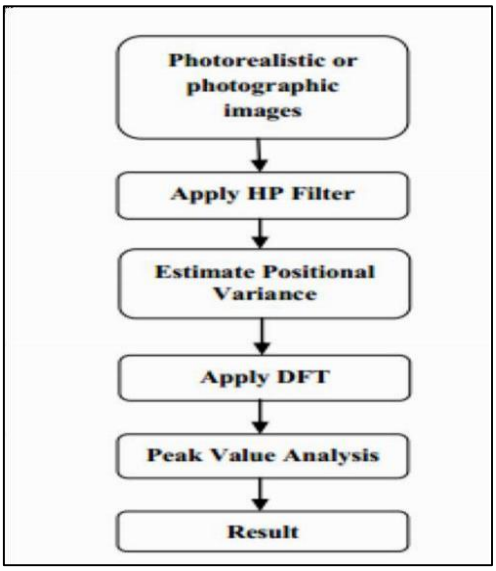

Fig. 4: Flow diagram for Photo Morphing Detection. First photographs from digital cameras or computer generated images are given to high pass (HP) filter. Then HP Filter is applied, and then the Positional Variance of each diagonal is calculated. Then analyzed, indicating the presence of demosaicing in the image.

III. IMAGE PROCESSING

In imaging science, Image Processing is processing of images using mathematical operations by using any form of signal processing for which the input is an image, a series of images, or a video, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Images are also processed as three-dimensional signals where the third-dimension being time or the z-axis. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images is referred to as imaging. Closely related to image processing are computer graphics and computer vision. In computer graphics, images are manually made from physical models of objects, environments, and lighting, instead of being acquired from natural scenes, as in most animated movies. Computer vision, on the other hand, is often considered high-level image processing out of which a software intends to decipher the physical contents of an image or a sequence of images

IV. CONCLUSIONS

In this survey article, we have reviewed over nine papers in the literature of image demosaicing and forgery. The majority of existing demosaicing algorithms exploit the spectral correlation by sequential strategies - i.e., the luminance channel is recovered first and then chrominance channels are reconstructed based on the full-resolution luminance image. Spatial adaptation based on local deterministic or statistical has shown critical to the performance of various demosaicing techniques. Our comparative studies with very best demosaicing algorithms

have demonstrated the importance of jointly exploiting spatial and spectral correlations especially for images with high-saturation and varying-hue. We have also observed that even ad-hoc fusion by averaging different demosaiced images could lead to further improvement. There are three directions along which further studies are definitely needed. First, demosaicing of images with weak spectral correlation remains a challenging task. Our understanding about the tradeoff between spatial and spectral correlation is still primitive though some attention has been paid to this issue by one group of contributing authors to this session. Last but not the least, the performance evaluation of demosaicing algorithms needs more careful investigation. Complementing the current proposed approach to identify different image software processing pipelines, additional features such as sensor noise pattern are needed in identification of individual cameras of the same model. Further investigation effort also includes verifying the effectiveness of our proposed demosaicing features on the camera models of non-Bayer CFAs.

ACKNOWLEDGMENT

The authors would like to thank the referees for their valuable comments which helped improve the quality of the paper greatly.

REFERENCES

[1] Hong CAO, student member, IEEE, and Alex C. KOT, Fellow, IEEE, "Accurate Detection of Demosaicing Regularity for Digital Image Forensics",
[2] Kuo-Liang Chung, Senior Member, IEEE, Wei-Jen Yang, Wen-Ming Yan, and Chung-Chou Wang, "Demosaicing of Color Filter Array Captured Images Using Gradient Edge Detection Masks and Adaptive Heterogeneity-Projection", IEEE Transactions On Image Processing, VOL. 17, NO. 12, DECEMBER 2008
[3] Hong Cao, Member, IEEE, and Alex C. Kot, Fellow, IEEE, "Manipulation Detection on Image Patches Using FusionBoost", IEEE Transactions On Information Forensics And Security, VOL. 7, NO. 3, JUNE 2012
[4] Nilesh P Ghatol, Rahul Paigude, Aniket Shirke "Image Morphing Detection by Locating Tampered Pixels with Demosaicing Algorithms", International Journal of Computer Applications (0975 – 8887) Volume 66– No.8, March 2013
[5] Shrishail Math , R.C.Tripathi "Images Image composite detection using customized", International Journal of Computer Graphics & Animation (IJCGA) Vol.1, No.3, October 2011
[6] Mr. Vinayak K. Shingote, Prof. Ruhi Kabara, "Image Authentication by Detecting Demosaicing ", IJARCCE *Vol.* 4, Issue 5, May 2015
[7] Jessica Fridrich, David Soukal, and Jan Lukáš Detection of Copy-Move Forgery in Digital Images "",SUNY Binghamton, Binghamton, NY 13902-6000
[8] S.Murali1 , Govindraj B. Chittapur2 , Prabhakara H. S 1 and Basavaraj S. Anami3, "Comparison and analysis of photo image forgery detection techniques" , International Journal on Computational Sciences & Applications (IJCSA) Vo2, No.6, December 2012
[9] Hany Farid, "Image Forgery Detection", IEEE Signal Processing Magazine [16] MARCH 2009

