A Comprehensive Study of Passive Digital Image Forensics Techniques based on Intrinsic Fingerprints

Ajit Singh
Department of Computer Science & Engineering,
BPS Mahila Vishwavidyalaya, Khanpur Kalan
Sonipat, India

Jyoti Malik
Department of Computer Science & Engineering,
BPS Mahila Vishwavidyalaya, Khanpur Kalan
Sonipat, India

ABSTRACT
Over the past decade digital images has become a very popular way to communicate, store and process information. With the rapid advancement and easy availability of technology, there is a flood of devices that are able to capture, store and create digital images. Over the past years image processing techniques have been developed that makes it really easy to tamper images. From journalism to social media edited images are appearing everywhere with increasing frequency. Authentication of images is very necessary as visual data effects what people perceive and believe. Digital image Forensics is an emerging field that uses intrinsic and extrinsic methods to authenticate digital images. Passive techniques extract and analyze inherent patterns introduced by various image processing steps and use these artifacts to associate the image with source device as well as to detect tampering of the digital images. This paper gives an overview of passive techniques of Digital Image Forensics which are based on intrinsic fingerprints inherent in digital images**.**

Keywords
Digital Image Forensics, Digital Watermarking, Forgery detection, Intrinsic Fingerprints, Passive Blind Image Forensics, Source Identification.

1. INTRODUCTION
A picture can tell a thousand words i.e. Images are more influential than words. Digital images are now ubiquitous from multimedia phones to online news sites and magazines. Due to the rapid growth of technology digital imaging devices have reached the common masses in form of cheap digital cameras and mobile; even there are graphic software that let us create synthetic digital images. It is infact very difficult to tell which image is captured by camera and which image is created by a graphic software. Although it seems to be a good thing that now everybody can capture, store and process digital images; there is also a downside that technology is degrading our trust in pictures even published in newspapers and popular magazines because there tons of image editing softwares that let us change the content of digital image very easily and unnoticeably.

Image tampering is not new; it has always been around even at the time of analog images. But image tampering has evidently increased in past years because in the past to edit images taken by traditional analog film camera required a skilled photographer and hours of work in dark room but today anybody can manipulate digital images very easily using softwares like adobe Photoshop and Picasa. Image tampering ranges from innocent manipulation for quality enhancement(changing brightness, contrast adjustment, removing noise) to malicious editing such as sewing together two images, pasting part of an image to other image. Apparently seeing is no longer believing. So a technology is needed to authenticate images to bring back the lost trust in visual media. This need becomes more evident in cases where visual data is used as evidence and effects the masses like in case of journalism. In July, 2012 news corporation 'Sunday Times' published a manipulated and old photograph of missile testing with the title "Iran Issues Stark Threat to Israel" which caused a sensation. The original photograph was taken in 2008 and had three missile in the image whereas in the doctored image four missiles were shown[10].

Digital Image forensics[1-3] is a new emerging field that deals with authentication of digital images. It provides tools and techniques that extracts intrinsic and extrinsic patterns embedded within the image to create history of images. This field stems from existing multimedia security related domains such as steganography and digital watermarking. Digital Image forensics makes use of image analysis and processing tools to recover information about image's history. There are some inherent patterns that embeds in the image during various phases of image capturing or creation(synthetic), image processing, image compression and image storing; Digital Image Forensics exploits these properties to resolve various issues regarding image authentication and integrity assessment. The main issues regarding image authentication and assessment of integrity of digital image are if the image is captured by camera or generated by graphic software[4], source camera identification[5-6] and differentiate between original and manipulated image[7].

The rest of the paper is organized as follows section II discusses the various categories of Digital Image Forensics. Section III describes the concept of passive digital image forensics. Section IV summarizes the major contributions in the field of DIF for source identification and forgery detection. passive Digital Image forensics techniques for image authentication and tampering detection are reviewed in section V and VI respectively. Section VI draws the concluding remarks and challenges of passive digital image forensics.

2. CATEGORIES OF DIGITAL IMAGE FORENSICS
Blind and Non blind DIF: The techniques of investigation can be blind or non blind. The blind techniques investigate the image when the original image is not available whereas the non-blind technique compares the case image with the original image. Detecting the traces of forgery is quite easy task when the original image before alteration is available but usually its not the case. In most of the cases only the case image is available and the investigation is done blindly using fingerprints extraction generated during different phases of image processing. The non-blind approach can be further

categorized in intrusive and semi-intrusive. In intrusive analysis the analyst has the device and information of each input and output signals generated by each component of the device as well as the different parameters used in image creation while in the semi-intrusive approach analyst has access to the source device but as a black box. The analyst does not has access to the parameters and processing techniques[18].

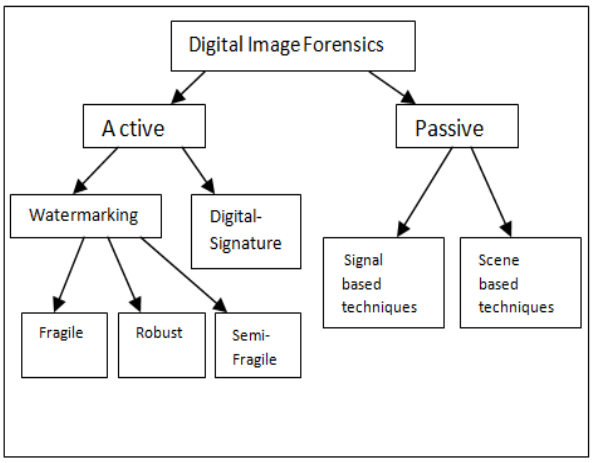

Figure 1: Categories of DIF

Active and Passive image forensics: DIF itself can be categorized into active and passive image forensics. Active techniques interfere with the image generation phase. The active techniques interfere in the image generation phase and intentionally modifies the image to leave behind identifying trails. It can serve two purposes first of which is to authenticate the image source and second is to prove integrity of the image. To achieve the first purpose a robust watermark or digital signature is added to the image which remains intact even when the image undergoes various processing operation like compression rotation, scaling and even attack. The watermark is a private data that is embedded into digital signals using a secret encryption key and to authenticate the source of the image the watermark and digital signature can be extracted using decryption process and the secret key. This method is used for copyright protection of images[11-13,19,27].

Another type of active technique is adding a fragile or semi-fragile watermark to the image. A fragile watermark doesn't survive the image processing steps and gets distorted when any processing operations are applied. To detect tampering watermark is extracted from the image and compared with original watermark. If watermark is same as original image is authentic and original else image is assumed to be tampered[26].

The passive techniques consider image generation as a read-only process and don't interfere in the process. Passive DIF techniques can be broadly categorized into Signal based DIF techniques and Semantic based techniques. Passive techniques that rely on inherent traces or fingerprints that are embedded during various phases of image processing are signal based DIF techniques. Whereas the scene based techniques analyses the scene and the semantics of the scene deployed in the digital image and detect anomalies based on interaction between physical objects like shadow and lightning [1].

Passive Digital Image forensics combines the principles of blind investigation with passive techniques of Digital Image forensics. It analyses digital image to extract traces to associate image with the source and to access image integrity. Development of efficient and robust passive Digital Image forensics techniques is being emphasized because most camera devices doesn't employ cryptographic or watermarking algorithms. So digital images are being produced without any attention toward authentication and integrity protection of digital data which leads to rely on passive techniques to access integrity and authenticity of digital images[8,9].

3. CONCEPT OF DIGITAL IMAGE FORENSICS

The passive techniques of image forensics depends upon the fact that the various processing steps during image acquisition, storage and post processing operations leave identifying traces of those operations providing a unique fingerprints to track the history of the image. These fingerprints can be used for various forensic purposes from source identification to tampering detection.

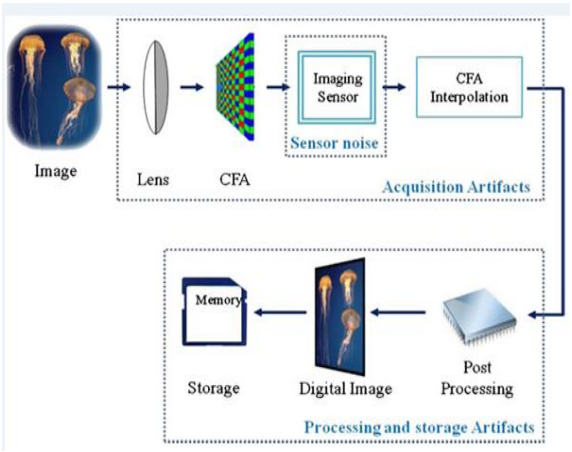

Fig 2: Digital Image Lifecycle (Source: [2])

All these steps add imperfections to the final output image. These imperfections or artifacts vary from device to device and form a unique fingerprint that can be used to track the source device as well as tampering detection. These artifacts are caused due to device imperfections such as lens distortion, chromatic aberrations, sensor imperfections, CFA interpolation and other processing steps such as lossy compression. The presence of these artifacts and distortion in these artifacts gives clue about image's originality and integrity[2].

4. PASSIVE IMAGE FORENSIC TECHNIQUES FOR SOURCE IDENTIFICATION

The first issue that arises is Source Identification. Source identification sometimes is of prime concern when the knowledge of the device that captured the image is itself an evidence. Another concern related to source identification is to differentiate between synthetic and natural images. Images captured by a digital camera are termed as natural images and images created by a computer graphics software are synthetic images. With the advent of graphics softwares it is possible to create images that are just alike as that of images captured by a digital camera.

Several approaches are available for source device identification of a particular test image at hand that uses

intrinsic fingerprints imprinted inside a digital image. These intrinsic features are basically imperfections that are introduced in the image during various operations. Some major approaches that are being used for source camera identification or discrimination between synthetic and natural image are based on sensor imperfections such as pixel defects and sensor noise, chromatic aberrations, photo response non uniformity, lens radial distortion and CFA interpolation pattern.

Source identification approaches

Approach based on Sensor noise: Sensor noise is additive noise caused by sensor imperfections. Sensor noise is made up of two factors fixed pattern noise and PRNU. There are basically two types of sensor technology used in digital camera devices CMOS(Complementary Metal Oxide Semiconductor) and CCD(Charged Coupled Device). These are made up of silicon chips and these silicon chips has large number of photo detectors on them. These photo detectors are pixels; these pixels capture light by converting photons and electrons. The in non homogeneity in the silicon chip and size variations in pixels which are rectangular in shape due to imperfections in the manufacturing process cause slight variations in the quantum efficiency of the pixels. These variations in the ability of converting photons into electrons(quantum efficiency) is termed as Photo Response Non Uniformity. PRNU is prevailing part of sensor noise. This PRNU which embeds into the image as a weak noise signal now act as an unintentional watermark and survives through various processing steps such as lossy compression. This PRNU can be estimated from the images and used to establish originality and integrity of digital images.

Jessica Fridrich proposed a model based on PRNU of image sensors that can be used for various important digital forensics tasks such as device identification and association, creating history of operations of a digital image and image forgery detection. The model involved capturing the differences among the pixels in a matrix same size as of the image sensor itself for an image sensor. This matrix form the fingerprint of the camera device[17]. Approach based on sensor noise has the advantage that the sensor noise pattern does not change from picture to picture i.e. it is content independent.

Lukas et al. highlighted that images captured by a particular camera inhibits a unique statistical characteristics introduced owed to the medium or high frequency content of the photograph. This unique sensor noise pattern can be uniquely mapped to a source digital camera using the reference error pattern which is calculated by averaging noise pattern calculated using denoising process over a number of images captured by that particular camera[16].

This approach is also used to efficiently discriminate between images captured by a digital camera and computer generated images. The approach exploits the basic principle that computer generated images fundamentally from camera images. As is has been established that the sensor used in a digital camera has imperfections and the sensors deployed in a digital camera inherently embeds sensor noise to the digital image during image acquisition step which is not the case with the computer generated images. This sensor pattern noise leaves a unique signature in the image that is not present in the synthetic images[5]. Although every camera has a unique noise pattern but the pattern noises of different cameras have some common statistical properties that are not present in computer generated images and can be used to classify the images between natural and synthetic images. Similarly the images generated by different computer graphics software will exhibit common properties that will not be present in images captured by cameras[16].

Approach based on CFA interpolation: In both CCD and CMOS cameras color filters are used. The color sensing elements are monochromatic in nature. Each element can capture one color component frequency out of the RGB bands. For each color component separate color array is needed but because of cost constraints the CCD color array is arranged in a pattern and acts like a mask in front of the sensor. The output image is a mosaic of red, green and blue color components. The missing RGB values are filled by applying weighting matrix operation on neighboring pixels. These interpolation operation generate a CFA pattern that acts like a fingerprint. Different camera manufactures uses different CFA interpolation algorithms. By extracting CFA artifacts from an image we can associate the output image to a source camera.

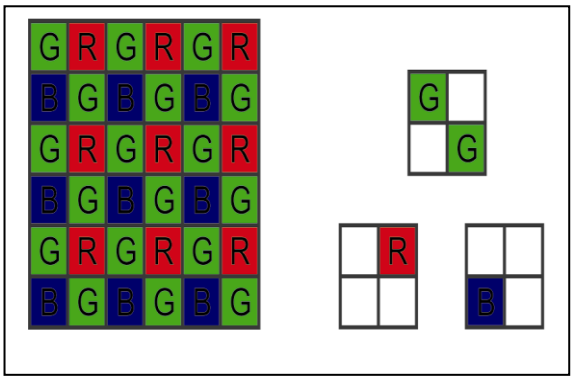

Fig 3: Missing values due to CFA (Source: [8])

Bayram et al. described an approach based on CFA(Color Filter Array) artifacts for source device identification. The author tested this approach for camera identification using interpolation correlation coefficients[14]. The approach although feasible but reliability drops as number of devices for associating the image increases. This approach doesn't work if when images are taken from different camera models from the same manufactures as being manufactured by same company similar CFA design and similar algorithm used for CFA interpolation.

Approach based on Pixel Defects: There are about a million pixels on the sensor chips of even the lowest quality image capturing device. A few of these pixels are defective. These pixels are usually dead pixels. These pixels can't capture the light in the image scene. These dead pixels are fixed for a particular camera and form a pattern. These dead pixels are visible when images are taken in black background. When images are enlarged all the working pixels are black but the defective pixels appear white because they can't absorb photons as shown in the image below. These errors form a pattern which can be used to relate the digital image with the source device. Each camera with the pixel defects produces same error pattern in each output image.

Z. J. Geradts et al. explained the approach based on pixel defects in CCD devices and tested the same for 12 different cameras. [20]. The approach although is quite robust but can't be used for camera devices that doesn't have pixel defects. Also when there is comparatively large number of devices there is quite a probability that two or more devices posses similar error pattern caused by pixel defects. Also this approach can't be used confidently because all the camera

device have built in mechanisms to compensate for these defects.

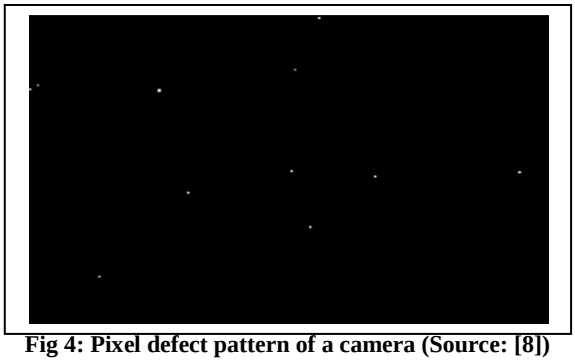

Fig 4: Pixel defect pattern of a camera (Source: [8])

Approach based on lens radial distortion: Due to flawed design and manufacturing processes most camera lenses produces distortions in the image. These defects are lens aberrations and most common lens aberration is radial distortion that makes straight line in the scene appear curved on the camera sensor. These aberrations form a fingerprint that varies in different devices and is forms basic concept of source identification using radial distortions[21].

For source identification distortion parameters are computed for different color bands and fed to classifier machine to associate the image to the source device.

5. PASSIVE IMAGE FORENSIC TECHNIQUES FOR TAMPERING DETECTION

Tampering is any processing operation that is applied on a multimedia object after has been created. Tampering can be innocent that doesn't changes the contents of the image but changes image's quality. Innocent tampering include various operation such as contrast adjustment, brightness adjustment, up-sampling, down-sampling, zooming, rotation etc. Whereas other type of tampering that aims to modify the contents of the image is malicious tampering. Malicious tampering includes operations such as cut-paste, copy-paste, region cloning and splicing etc. Several tampering detection algorithms has been proposed.

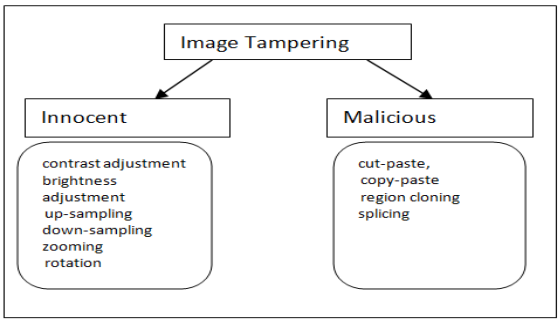

Figure 5: Categories of image tampering

Tampering detection algorithms can also be categorized as Targeted tampering detection algorithms and Universal tampering detection algorithms. Targeted tampering detection techniques focus on detecting a specific type of alteration such as cloning, splicing, re-compression etc. whereas universal tampering detection algorithms seek to spot the existence of common tampering operation that possibly will be an indication of tampering such as filtering, up or down sampling, compression and rotation etc. These technique do not essentially conclude what operation was applied but just that the image has been retouched[15].

Tampering detection can be categorized in three levels: low level, middle level and high level. The low level tampering detection approach uses statistical characteristics of digital image pixels. Middle level uses some basic semantic information such as sharp edges because of splicing operation and inconsistencies in lighting directions and shadows. High level tampering detection uses semantic information to detect tampering[19].

Another type of technique that detects local tampering searches for inconsistencies among the image characteristics, statistics and content across different areas of the image and hence are able to discover and localize tampering. Such techniques are termed as Localized tampering detection techniques and these techniques looks for inconsistencies in sensor noise patterns, CFA demosaicing artifacts and lightning etc[15].

There are two important concepts regarding tampering detection if the image is altered using part of any other image or not. If the image is altered using contents from other image all the techniques that are used for source identification are usually applicable for tampering detection too. As the part taken from other image will have different parameters for different intrinsic fingerprints that can be analyzed by generating histograms for the parameters. When tampering is done using the same image i.e. region duplication then region matching is only viable method to detect the duplicated region which can be done using pattern matching algorithms.

Tampering detection approaches:

Tampering detection on basis of CFA artifacts: the foundation of this approach is that the local tampered area will have different CFA artifacts as compared to the rest of the image. So the CFA artifacts are calculated for entire image by dividing image in small blocks. This approach efficiently localizes the tampered area[14].

Tampering detection based on sensor fingerprints inconsistencies: sensor fingerprint inconsistencies provide another way to detect image forgery. The technique is based on the principle that the tampered region will not have same sensor noise fingerprints if it has been copied from other image. So this approach can be used to detect certain types of forgeries[17].

Tampering detection based on chromatic aberrations: this approach is feasible as it is established that chromatic aberrations are inherent in digital images. When tampering is done in the images these aberration patterns become inconsistent. This inconsistency can be detected in digital images and used as an evidence of image tampering. This approach is also proposed as discrimination technique between synthetic and natural images as computer generated images do not suffer from chromatic aberrations [22].

Tampering detection based on JPEG compression artifacts: this technique is used for tampering detection as well as for source identification. The concept behind this approach is that most cameras use jpeg compression to compress the image before storing it on the storage media. As in all the lossy compression schemes JPEG also uses quantization tables that decide the compression ratio achieved. As different cameras as well editing software uses different quantization tables. The schemes works by first determining the quantization table used in the image at hand and comparing the quantization

values to a database that contains quantization tables for several camera. This comparison results in the possible device identification. Although for a large sample of cameras the quantization tables may not be unique, a few devices may have same quantization table values. For tampering detection the computed quantization values are compared against database entries which contains quantization values for various popular image editing softwares[23].

Tampering detection based on camera response function: this method can be used to classify images into authentic and spliced. Spliced images are those images that has been tampered by pasting parts from a different image into the tampered image. The approach is based on intuition that different cameras have different CRF. CRF is the characteristics that refers to how the radiance arriving on camera sensors after passing through camera lens is transformed into pixel brightness values. The approach is semiautomatic and needs human intervention. A user first observes the image to identify suspicious region i.e. the region that appears to be spliced. The image is divided into three regions: region that appears to be from one device lets say camera1, regions that appears to be forged i.e. regions from camera2 and third region that is interfacing the first two regions. After that regions are compared based on CRF values. If all regions have matching CRF value image is said to be authentic otherwise the image is likely to be a case of spliced image [24].

Other approaches are also available that are targeted forgery detection techniques. J. Fridrich et al. addressed the issue of copy move detection. In copy-move attack some parts of tampered image are copied and pasted into another part of the same image. The aim of copy-move detection is to uncover duplicated regions in an image. The authors described two approaches for the purpose. The image is initially divided into small blocks. The first approach is the exhaustive search approach that selects each region and matches the region with all other regions in the image to detect similarities or matching. Another approach is autocorrelation approach that scans the image finding correlations between regions in the image. The duplicated region will have an obvious peak for correlation values. The algorithms for duplicate region detection looks for two type of region. That region that has exact match with other region in the same image and also looks for robust regions. Robust match are those matches that are not an exact match but good candidate of region duplication. The approach finds pasted regions considering the fact that variations may be caused in duplicated region because of editing and retouch of region done to make tampering less suspectable[25].

6. CONCLUSION AND FUTURE SCOPE

This paper reviewed the main contribution done in the area of passive digital image forensics for multimedia security. The text covers main approaches used for digital image authentication and tampering detection which are based on intrinsic fingerprints. A wide range of tools and techniques are now available to look into digital images to verify their authenticity and integrity.

Although the challenge still remain for techniques that are robustness of the existing techniques and confidence in the accuracy of the results achieved by these techniques. Lack of standardization of tools and benchmarks is the main hurdle in the world wide adaption of DIF techniques.

DIF techniques provides a number techniques to investigate digital multimedia for originality and authentication of content. Further DIF is a tool to perform steganalysis of the multimedia to find hidden information. Therefore DIF techniques can also be used to securely hide secret messages into the contents of a digital multimedia object.

7. REFERENCES

[1] Alessandro Piva,. "An Overview on Image Forensics", ISRN Signal Processing Article ID 496701, 22 pages, Volume 2013

[2] Judith A. Redi, Wiem Taktak, and Jean-Luc Dugelay, "Digital image forensics: A booklet for beginners", Multimedia Tools and Applications, 51(1):133–162, 2010.

[3] H. T. Sencar, and N. Memon, "Overview of State-of-the-art in Digital Image Forensics", Part of Indian Statistical Institute Platinum Jubilee Monograph series titled Statistical Science and Interdisciplinary Research,' World Scientific Press, 2008.

[4] Sintayehu Dehnie, Husrev T. Sencar, and Nasir Memon, "Digital image forensics for identifying computer generated and digital camera images", In IEEE International Conference on Image Processing, pages 2313– 2316, 2006.

[5] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion", In Optics Express, vol. 14, pp. 11551–11565, 2006.

[6] A. E. Dirik, H. T. Senear, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust", In IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 539–552, 2008.

[7] Ismail Avcibas, Sevinc Bayram, Nasir Memon, Mahalingam Ramkumar, and Bulent Sankur, "A classifier design for detecting image manipulations", In IEEE International Conference on Image Processing, pages 2645–2648, 2004.

[8] W Luo, Z Qu, F Pan, J Huang, "A survey of passive technology for digital image forensics", Frontiers of Computer Science in China 1 (2), 166-179, 2007.

[9] Tian-Tsong Ng, Shih-Fu Chang, Ching-Yung Lin, and Qibin Sun, "Multimedia Security Technologies for Digital Rights", chapter Passive-Blind Image Forensics, pages 383–412. Elsevier, 2006.

[10] Irene Amerini, Roberto Caldelli,, Alberto Del Bimbo and Giuseppe Serra, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery", IEEE Transactions on Information Forensics and Security, VOL. 6, NO. 3, September 2011.

[11] Chih-Ming Kung, Shu-Tsung Chao; Yen-Chen Tu, Yu-Hua Yan and Chih-Hsien Kung, "A Robust Watermarking and Image Authentication Scheme used for Digital Content Application", JOURNAL OF MULTIMEDIA, VOL. 4, NO. 3, JUNE 2009.

[12] Seyed Mohammad Mousavi, **"**Image Authentication Scheme using Digital Signature and Digital Watermarking", IJCEM International Journal of Computational Engineering & Management, Vol. 16 Issue 3, May 2013.

[13] J Sravanthi, Dr. MHM Krishna Prasad, "Robust and secure Digital Signature for Image Authentication over

Wireless Channels", International Journal of Computer Trends and Technology- July to Aug Issue 2011.

[14] Sevinc Bayram, Husrev T. Sencar, Nasir Memon and Ismail Avcibas, "Source Camera Identification based on CFA Interpolation", in International Conference on Image Processing IEEE Genova, Italy, 2005.

[15] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in Proceedings of the International Conference on Image Processing (ICIP '09), pp. 1497–1500, IEEE, Cairo, Egypt, November 2009.

[16] Jan Lukas, Jessica Fridrich and Miroslav Goljan, "Determining digital image origin using sensor imperfections", In Proceeding. SPIE 5685, Image and Video Communications and Processing 2005.

[17] J. Fridrich, "Digital image forensic using sensor noise," in IEEE Signal Processing Magazine, vol. 26, no. 2, pages. 26–37, 2009.

[18] Ashwin Swaminathan, Min Wu, and K. J. Ray Liu, "Nonintrusive Component Forensics of Visual Sensors Using Output Images", in IEEE Transactions on Information Forensics and Security 2.1, pages 91–106, March 2007.

[19] Wei Wang, Jing Dong, Tieniu Tan, "A Survey of Passive Image Tampering Detection", Digital Watermarking Lecture Notes in Computer Science, Volume 5703, pp 308-322 ,2009.

[20] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, "Methods for Identification of Images Acquired with Digital Cameras", Proc. of SPIE, Enabling Technologies for Law Enforcement and Security, vol. 4232, February 2001.

[21] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration", Proceedingsof the SPIE 2006.

[22] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration", In ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.

[23] H. Farid, "Digital Image Ballistics from JPEG Quantization",Technical Report, TR2006-583, Dartmouth College, Computer Science, 2006.

[24] Y.-F. Hsu and S.-F. Chang, "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics consistency", In ICME, Toronto, Canada, July 2006.

[25] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", Proc. of DFRWS 2003.

[26] J. Fridrich, "Image Watermarking for Tamper Detection," Proc. of IEEE International Conference on Image Processing (ICIP), vol. 2, pp. 404–408, Chicago, IL, Oct. 1998.

[27] M.Sreerama Murty, D.Veeraiah, A.Srinivas Rao ,"Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis", Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, June 2011.