Sonika *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 7, July- 2015, pg. 63-70 **ISSN: 2321-8363**

A REVIEW ON IMAGE FORGERY USING IMPROVED COLOR FILTER ANALYSIS

Ms. SONIKA (student, M.Tech), Mr. VIKAS MALIK (Assistant Professor in CSE&IT)
Computer science and Engineering (Network Security)
BPS Mahila Vishwavidyalaya, Khanpur Kalan,(Sonepat) Haryana. INDIA
Email address: sonikasingh66@gmail.com, vikassmalik@gmail.com

ABSTRACT: In this we study about the Image Devices used for Forgery of Images by Different Techniques but especially with Color Filter Array. We recognize that digital camera images contain a CFA interpolation relationship between the pixels as a result of using a color filter array with demosaicing algorithms. Typical consumer digital cameras capture the scene by generating a mosaic-like gray-scale image, known as a color filter array (CFA) image. Detection Algorithm of Image forgery is also discussed, for better knowledge figures are also mentioned.

Keywords- CFA interpolation, Demosaicing Artifacts, forgery detection techniques, image forgery.

1. INTRODUCTION

Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive or earn profit by selling the forged item. Copies, studio replicas, and reproductions are not considered forgeries, though they may later become forgeries through knowing and willful misrepresentations.[1] Forging money or currency is more often called counterfeiting. But consumer goods may also be counterfeits if they are not manufactured or produced by the designated manufacture or producer given on the label or flagged by the trademark symbol. When the object forged is a record or document it is often called a false document.

This usage of "forgery" does not derive from metalwork done at a forge, but it has a parallel history. A sense of "to counterfeit" is already in the Anglo-French verb forger, meaning "falsify".

A forgery is essentially concerned with a produced or altered object. Where the prime concern of a forgery is less focused on the object itself – what it is worth or what it "proves" – than on a tacit statement of criticism that is revealed by the reactions the object provokes in others, then the larger process is a hoax. In a hoax, a rumor or a genuine object planted in a concocted situation, may substitute for a forged physical object.

The similar crime of fraud is the crime of deceiving another, including through the use of objects obtained through forgery. Forgery is one of the techniques of fraud, including identity theft. Forgery is one of the threats which is addressed by security engineering.

2. Image Forgery Detection Techniques.[2][3]

2.1 Pixel-based image forgery detection.

Pixel-based techniques emphasize on the pixels of the digital image. These techniques are roughly categorized into four types. We are focusing only two types of techniques splicing and copy-move(cloning) in this paper. This is one of the most common forgery detection techniques. Figure (a) shows categorization of pixel based forgery detection techniques.

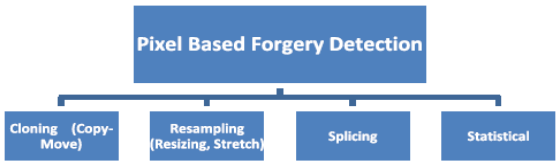


Fig-(a)

2.2 Format-based image forgery detection.

Format based techniques are another type of image forgery detection techniques. These are based on image formats and work mainly in the JPEG format. These techniques can be divided into three types shown in Figure (b). If the image is compressed then it is very difficult to detect forgery but these techniques can detect forgery in the compressed image.

Fig-(b)

2.3 Camera-based image forgery detection.

From the digital camera when we capture an image, the image moves from the camera sensor to the memory and it undergoes a series of processing steps, including filtring, gamma correction ,quantization, colour correlation, white balancing, and JPEG compression. These processing steps from capturing to saving the image in the memory may vary on the basis of camera artifacts and camera model. These techniques work on this principle. These techniques can be divided into four categories as shown in Figure(c).

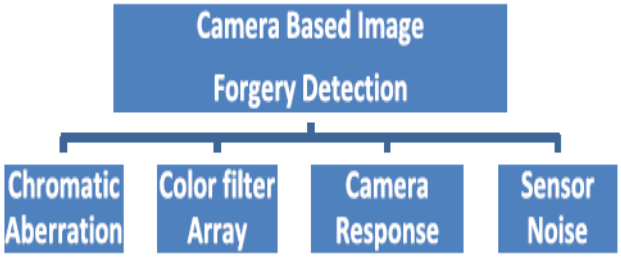


Fig-(c)

2.4 Physical environment-based image forgery detection.

Consider the creation of a forgery showing two movie stars, rumored to be romantically involved, walking down a sunset beach. Such an image might be created by splicing together individual images of each movie star. In so doing, it is often difficult to exactly match the lighting effects under which each person was originally photographed. Differences in lighting across an image can then be used as evidence of tampering. These techniques work on the basis of the lighting environment under which an object or image is captured. Lighting is very important for capturing an image. These techniques are divided into three categories as shown in Figure(d).

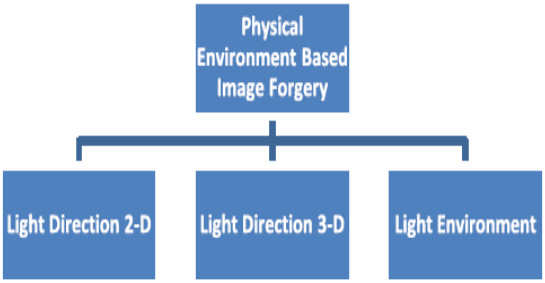


Fig-(d)

2.5 Geometry-based image forgery detection.

Grooves made in gun barrels impart a spin onto the projectile for increased accuracy and range. These grooves introduce somewhat distinct markings to the bullet fired, and can therefore be used to link a bullet with a specific handgun. In the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. Geometry-based techniques make measurement of objects in the world and their position relative to the camera. Geometry-based image forgery techniques are divided into two categories shown in Figure(e).

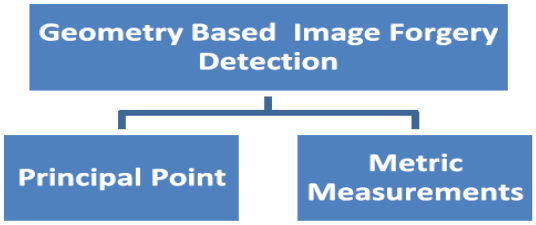
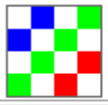
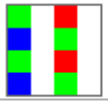


Fig-(e)

3. COLOR FILTER ARRAY (CFA)

[4][5]Color filters are needed because the typical photo sensors detect light intensity with little or no wavelength specificity, and therefore cannot separate color information. Since sensors are made of semiconductors they obey solid-state physics.

The color filters filter the light by wavelength range, such that the separate filtered intensities include information about the color of light. For example, the Bayer filter (shown on next page) gives information about the intensity of light in red, green, and blue (RGB) wavelength regions. The raw image data captured by the image sensor is then converted to a full-color image (with intensities of all three primary colors represented at each pixel) by a demosaicing algorithm which is tailored for each type of color filter. The spectral transmittance of the CFA elements along with the demosaicing algorithm jointly determines the color rendition. The sensor's pass band quantum efficiency and span of the CFA's spectral responses are typically wider than the visible spectrum, thus all visible colors can be distinguished. [6]The responses of the filters do not generally correspond to the CIE color matching functions, so a color translation is required to convert the tristimulus values into a common, absolute color space.

Image	Name	Description	Pattern size (pixels)
	Bayer filter	Very common RGB filter. With one blue, one red, and two green.	2×2
	RGBE filter	Bayer-like with one of the green filters modified to "emerald"; used in a few Sony cameras.	2×2
	CYYM filter	One cyan, two yellow, and one magenta; used in a few cameras of Kodak.	2×2
	CYGM filter	One cyan, one yellow, one green, and one magenta; used in a few cameras.	2×2
	RGBW Bayer	Traditional RGBW similar to Bayer and RGBE patterns.	2×2
	RGBW #1	Three example RGBW filters from Kodak, with 50% white. (*See Bayer filter#Alternatives*)	4×4
	RGBW #2		
	RGBW #3		2×4

3.1.Analysis of CFAs.

As all the multiplex components coexist in the same frequency space, it is inevitable that aliasing occurs, which leads to demosaicking artifacts in the demosaicked images, such as blur, false color, and zippering. [12]With the frequency structure and the statistics of multiplex components, we can predict the performance of a CFA by analyzing at what frequencies and to what degree the frequency aliasing occurs.

It is easy to see that the spectra around nonzero chromas will suffer more aliasing, and the amount of aliasing depends on the distance between the multiplex components and their relative positions.

For example, the frequency structure SBayerof the Bayer CFA shows that luma and chromas overlap around frequencies (1/2, 0), (0, 1/2) and (1/2, 1/2). The chromas−(R−B)/4 at (1/2, 0), and (R−B)/4 at (0, 1/2) will suffer more aliasing because the lumais high in these two directions. This is the major shortcoming of the Bayer CFA. The frequency structure Sdiag shows that the two chromas of the Diagonal Stripe CFA are modulated at frequencies (1/3,−1/3) and (−1/3, 1/3), respectively. [7][8]This CFA is good in the sense that the chromas are not on the horizontal or vertical axes. However, it is still unsatisfactory because there is small distance between the chromas and the luma.

3.2 Detection of Image Forgery by CFA Based Features.

Almost all digital cameras contain an image sensor with a color filter array, for example, the Bayer filter array shown in Figure 3.2(a). A filter is positioned over each photo site, sensing either the red, green, or blue component of the incident light. The image from the image sensor contains only a single signal value at each pixel position. This pixel value further corresponds to only a single color component (red, green, or blue in the case of the Bayer filter array) [9]. The Color Filter Array can be use for image forgery detection. On the Basis of these CFA artifacts, there are two proposed methods. First based on CFA pattern number estimation and the secondly based on CFA based noise analysis.

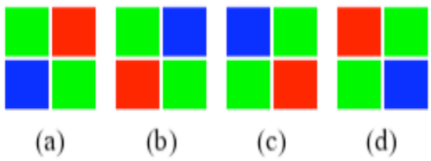


Fig-3.2(a) Different Bayer CFA patterns

4. CONCLUSION

In this era of digital computing, the interest and necessity of representing information in visual forms has become very important. Due to considerable improvement in computing and network technologies, and the availability of better bandwidths, the past few years have seen a considerable rise in the accessibility, sophistication, and transmission of digital images using imaging technologies like digital cameras, scanners, photo-editing, and software-packages. However, this technology is also being used for manipulating digital images and creating forgeries that are difficult to distinguish from authentic photographs. Thus the problem of

establishing image authenticity has become more complex with easy availability of digital images and free downloadable image editing softwares leading to diminishing trust in digital photographs.

REFERENCES

[1]. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358, Priyanka Prasad, "Image Forgery Localization via CFA Based Feature Extraction and Poisson Matting".

[2].http://www1.inf.tu.dresden.de/~rb21/publications/KB2009_CFA-Synthesis_SPIE.pdf, Matthias Kirchner and Rainer Böhme, "Synthesis of Color Filter Array Pattern in Digital Images".

[3].http://www.ee.nthu.edu.tw/~cwlin/pub/mmsp08forensics.pdf, Chih-Chung Hsu, Tzu-Yi Hung, Chia-Wen Lin and Chiou-Ting Hsu, "Video Forgery Detection Using Correlation of Noise Residue".

[4].http://www.eie.polyu.edu.hk/~enyhchan/JTIP.Lossless_Compression_for_CFAimage.pdf, King-Hong Chung and Yuk-Hee Chan, "A Lossless Compression Scheme for Bayer Color Filter Array Images".

[5]. Quen Mary University of London RR-08-04 May 2008 Department of Computer Science ISSN 1470-5559, Yan Li, PengweiHao, and Zhouchen Lin, "Color Filter Arrays: Representation and Analysis".

[6]. World Academy of Science, Engineering and Technology 71 2012, SomayehSadeghi, Hamid A. Jalab and SajjadDadkhah, "Efficient Copy-Move Forgery Detection for Digital Images".

[7].IEEE Trans Image Process. 2006 Nov;15(11):3261-78, Lian NX, Chang L, Zagorodnov V and Tan YP, "Reversing demosaicking and compression in color filter array image processing: performance analysis and modeling".

[8]. EuroCon 2013 1-4 July 2013 Zagreb, Croatia, Muhammad Hussain, Ghulam Muhammad, Sahar Q. Saleh, Anwar M. Mirza and George Bebis, "Image Forgery Detection Using Multi-Resolution Weber Local Descriptors".

[9]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12, December 2013, GeetanjaliSahu and UshaKiran, "Survey of Different Techniques for Image Tamper Detection on Digital Images".

[10]. Sajja.Karthik et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8110-8113, Sajja.Karthik and M.Gargi, "A Novel Approach for Detecting of Tampering On Images".

[11].http://isis.poly.edu/~forensics/pubs/dirik_icip09.pdf, Ahmet Emir Dirik and NasirMemon, "IMAGE TAMPER DETECTION BASED ON DEMOSAICING ARTIFACTS".

[12]. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 539-543, PradyumnaDeshpande and PrashastiKanikar, " Pixel Based Digital Image Forgery Detection Techniques".

[13]. 978-1-4244-5309-2/10/$26.00 ©2010 IEEE, PatcharaSutthiwan, Yun-Qing Shi, Jing Dong, Tieniu Tan and Tian-Tsong Ng, "New Developments in Color Image Tampering Detection".

[14]. International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Special Issue No. 01, September 2014 ISSN (online): 2348 – 7550, YogeshKatre and Prof. Gajendra Singh Chandel, "IMAGE FORGERY DETECTION USING ANALYSIS OF CFA ARTIFACTS".

[15]. A. Leonardis, H. Bischof, and A. Pinz (Eds.): ECCV 2006, Part III, LNCS 3953, pp. 423–435, 2006. Springer-Verlag Berlin Heidelberg 2006, Junfeng He, Zhouchen Lin, LifengWang and Xiaoou Tang, "Detecting Doctored JPEG Images Via DCT Coefficient Analysis".

[16]. IETE JOURNAL OF EDUCATION VOL 55 NO 1 JAN_JUN 2014, MohdDilshad Ansari, S. P. Ghrera&VipinTyagi, "Pixel-Based Image Forgery Detection: A Review".

