Photomorphic Detection:Image Authentication by Detecting Traces of Demosaicing

Dhamdhere Ashish Vinod, Bari Dhiraj Shivaji, Bankar Deepak Bhanudas, Palade Atul Dattatray

Department of Information Technology
SPCOE College of Engineering Dumbarwadi, Pune-412409
Savitribai Phule Pune University, India
,

Abstract

With increasing technical advances, computer graphics are becoming more photorealistic. Therefore, it is important to develop methods for distinguishing between actual photographs from digital cameras and computer generated images. We describe a novel approach to this problem. Rather than focusing on the statistical differences between the im-age textures, we recognize that images from digital cameras contain traces of resampling as a result of using a color filter array with demosaicing algorithms. We recognize that estimation of the actual demosaicing parameters is not nec-essary; rather, detection of the presence of demosaicing is the key. The in-camera processing (rather than the image content) distinguishes the digital camera photographs from computer graphics. Our results show high reliability on a standard test set of JPEG compressed images from con-sumer digital cameras. Further, we show the application ofthese ideas for accurately localizing forged regions within digital camera image.

1.INTRODUCTION:

1.1 Background And Basic

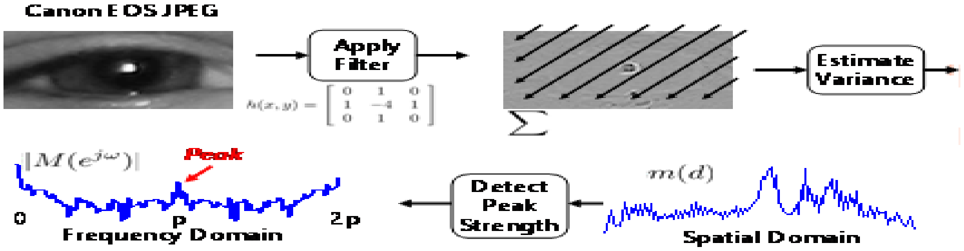
The field of computer graphics is rapidly maturing to the point where human subjects have difficulty distinguishing photorealistic computer generated images (PRCG) from photographic images (PIM).As evidence of the proliferation of computer generated imagery, one need look no further than Hollywood. According to Wikipedia, the first feature-length computer animated flim was Toy Story, in 1995. In 2007, a total of 14 computer animated flims were released, several with stunningly realistic imagery. In addition to computer animated flims, computer graphics are routinely used to create imagery in live action motion pictures that would otherwise be nearly impossible to flims. Partly because of the success of computer animation in popular culture, it is well known by the general public that images can be manipulated and are not necessarily a historical record of an actual event. When viewing movies for entertainment, the audience is usually a willing participant when fooled into believing computer generated images represent a fictional version of reality. However, in other situations, it is extremely important to distinguish between PRCG and PIM. In the mass media, there have been embarrassing instances of manipulated images being presented as if they represent photographically captured events. In legal situations, where photographs are used as evidence. it is crucial to under- stand whether the image is authentic or forged (either computer generated or altered). Furthermore, in the intelligence community, it is of vital importance to establish the origin of an image. Digital image manipulation software is now readily available on personal computers. It is therefore very simple to tamper with any image and make it

available to others. Insuring digital image integrity has therefore become a major issue. Watermarking has become a popular technique for copyright enforcement and image authentication. The aim of this paper is to present an overview of emerging techniques for detecting whether image tampering has taken place. Compared to the techniques and protocols for security usually employed to perform this task, the majority of the proposed methods based on watermarking, place a particular emphasis on the notion of content authentication rather than strict integrity. In this paper, we introduce the notion of image content authentication and the features required to design an effective authentication scheme. We present some algorithms, and introduce frequently used key techniques.Pictures persuade people powerfully. Photos communicate more convincingly than do words alone by evoking an emotional and cognitive arousal that the same information, without the pictures, does not. A picture is a more effective conveyor information than its verbal and written counterparts alone in that the communication of its message occurs in less time, requires less mental effort on the part of the observer,incites less counterargument, and creates more confidence in the conclusions it proffers. People, including jurors, trust photographs. So do courts. Yet it has never been easier for photos to misrepresent the truth than it is now. So great is the risk of a photograph misrepresenting the truth that an international leader in digital imaging was compelled to declare, photographs, as evidence of reality, are dead. If photographs are so untrustworthy, why are they still considered the ultimate proof? Why aphorisms are like photos don't lie and I'll believes it when I see it? so pervasive? The answer has to do with how technology has affected a paradigm shift in the methods used to take pictures. To comprehend how the fidelity of the photograph has been forfeited, it is first necessary to understand the previous picture paradigm and juxtapose it with the modern domain of digital images.

2. RELATED WORK

There are several possible approaches for authenticating the source of a digital image. With active watermarking , an image is altered to carry an authentication message by the image capture device. At a later time, the message can be extracted to verify the source of the image. Unfortunately, this method requires coordination between the insertion and extraction of the watermark. In contrast to the active approach, statistical methods are also used to characterize the difference between PRCG and PIM. For example, in , a set of wavelet features are extracted from the images to form a statistical model of PRCG and PIM, and classification is performed with standard ma-chine learning techniques. It is shown that geo-metric and physical features are also effective for classifying between PRCG and PIM. In essence, both of these approaches are effective because of the lack of perfection of the state-of-the-art computer graphics. For example, in , it is noted that PRCG contain unusually sharp edges and occlusion boundaries. A reasonable explanation for this is that the imperfections such as dirt, smudges, and nicks that are pervasive in real scenes are difficult to simulate. It is far easier to construct a computer graphic of a gleamingly new office than the image of that office after a decade of wear. In any case, as the field of computer graphics matures with more realistic modeling of scene detail and more realistic lighting models, it seems reasonable to assume that the statistical differences between real scenes and computer generated scenes will diminish. Meanwhile, researchers have recently shown that when an image is resampled through interpolation, statistical traces of resampling are embedded in the image signal it-self. The signature is recovered by applying a Laplacian operator to the image. The Laplacian is shown to have a higher variance at positions corresponding to pixel locations in the original uninterpolated image, and this pattern is recovered with Fourier analysis. Similarly, the EM algorithm along with Fourier analysis are used to recover the correlations between neighboring pixels that are introduced through interpolation. In addition, because a forgery is generally created by resampling an object and inserting it into a target image, this approach has been shown to be useful for detecting candidate forged image regions and is robust to JPEG compression. Other researchers have focused on matching images to specific digital camera models using cameramodel specific properties of demosaicing. This work is based mostly on simulated demosaicing without the nonlinearities associated with post-processing. Our contributions are the following: we describe a novel approach for distinguishing between photorealistic computer graphic images and photographic images captured with a digital camera based on the idea that photographic images will contain traces of demosaicing. We recognizethat finding the actual demosaicing parameters is not necessary for distinguishing between photorealistic computer graphics and photographic images. We achieve the highest reported accuracy on a standard test set for distinguishing between photographic images and photorealistic computer graphics by detecting traces of demosaicing. We demonstrate robustness by working only with images captured and processed with consumer-grade digital cameras, including the associated JPEG compression. Further, we extend our algorithm to examine images locally, accurately detectingforged regions in otherwise natural images.

3.BLOCK DIAGRAM:



4.ALGORITHM:

There six main modules in this software namely:

a) Browsing the image:- This is the very first module of the system. After successful login first we have to take the image from the user which we want to test. F or this we have to enter the complete path of the image or there is a browser to brows the image from computer system. After browsing the image click on load button to display the image.
b) Applying high pass filter
c) Calculating positional variance.
d) Applying DFT.
e) Peak value analysis.
f) Detecting forged image regions:-The algorithm shown in Section 4 can be applied locally to detect regions of an image that have possibly been tampered with. The main work is: demosaicing produces periodic correlations in the image signal. When a image is manipulated, an image piece from another source (it can be from another image or a computer graphic) is pasted over a portion of the image. In gene ral, this image piece is resample to match the geometry of the image. The application of the high pass filter is the same as previously described. Estimating the variance becomes a local operation : Where o(x; y) = |h(x, y) * i(x, y)|, the absolute value of the output of applying the filter h(x, y) to the image i(x, y). The parameter n is the size of the local neighborhood; by default we use n = 32. At each position (x, y), a local (256 point) one-dimensional DFT is computed along each row, and the local peak ratio s(x, y) is computed as described. The above equation estimates the variance for detecting forged image regions.
g) Displaying the output.

4. IMAGE SENSORS AND DEMOSAICING

Nearly all digital cameras contain an image sensor with a color filter array, for example, the Bayer filter array. A filter is positioned over each photosite, sensitizing it to either the red, green, or blue component of the incident light. While other color filter array patterns and filters are sometimes used, the Bayer is the most common. The raw 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). Typically, a demosaicing algorithm also called color filter array interpolation, is applied to the raw image to estimate the pixel value for each color component. The inter-polation can either be linear or adaptive. With a na¨ive interpolation, each color channel is interpolated independently using only samples from the same color, for example, with bilinear or bicubic interpolation. In
more complicated linear algorithms, interpolation is performed by considering the local pixel values of multiple color channels. For example, all of the missing green val-ues can first be found. Then missing red pixel values are found by interpolating a red minus green differential. In even more complex nonlinear algorithms, the interpolation kernel is adaptive depending on the characteristics of the pixel values of the local neighborhood. Generally speaking, demosaicing algorithms have several features in common. Missing color values are determined from a weighted linear combination of neighboring pixels, and the sum of the weights is one. In general that interpolation of this variety leaves a signature that can be reliably detected. Detailed analysis of the signal traces left by interpolation are found so we present an example to provide intuitive understanding of our algorithm for detecting the presence of demosaicing.

5. DETECTING TRACES OF DEMOSAICING

An interpolated pixel value is produced with a weighted linear combination of neighboring pixel values. The weights directly affect the variance of the distribution from which the interpolated pixel value is drawn. This pattern of variances can be detected and is the basis for de-tecting demosaicing. In our implementation, we consider only the green channel of the image to demonstrate our ap-proach. The other color channels (or differences between color channels) can be analyzed in a similar manner.

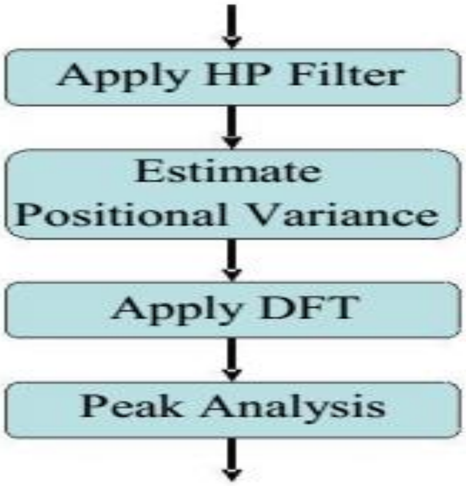


Figure :- Flow diagram for detecting demosaicing. First a highpass filter is applied, then the variance of each diagonal is estimated. Fourier analysis is used to find periodicities in the variance signal, indicating the presense of demosaicing.

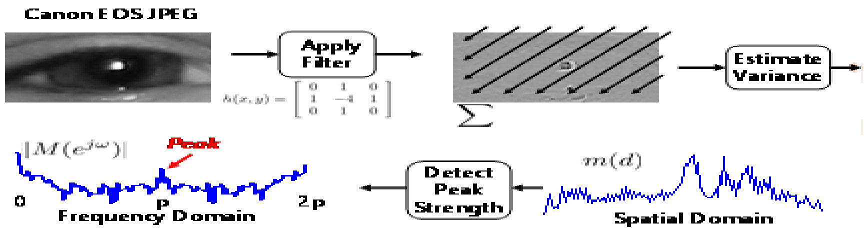
6.APPLICATION:

a. Law Enforcement Officers.
b. Forensic Department.
c. All Areas Where Editing an Image is strictly restricted.

7.ADVANTAGES:

a) Support multiple Image Formats i.e. JPEG,GIF,BMP.
b) Original Image is not Required For Image Authentication.
c) Forged Regions Can be Found out.

Block-diagram



REFERENCES

[1] J. Adams and J. Hamilton. Design of practical filter array interpolation algorithms for digital cameras. *Proc. SPIE*, 1997.

[2] S. Bayram, H. T. Sencar, and N. Memon. Source camera identification based on cfa interpolation. In *Proc. ICIP*, 2005.

[3] D. Cok. Signal processing method and apparatus for producing interpolated chrominance values in a sampled color
image signal. *U.S. Patent 4,642,678*, 1986.

[4] A. Gallagher. A small tampered image database. http://amp.ece.cmu.edu/people/Andy/authentication.html.

[5] A. Gallagher. Detection of linear and cubic interpolation in JPEG compressed images. In *Proc. CRV*, 2005.

[6] A. Gallagher. Method for detecting image interpolation. *U.S. Patent 6,904,180*, 2005.

[7] J. Lukas, J. Fridrick, and M. Goljan. Determining digital image origin using sensor imperfections. *Proc. SPIE*, 2005.

[8] S. Lyu and H. Farid. How realistic is photorealistic? *IEEE Transactions on Signal Processing*, 2005.

[9] T.-T. Ng, S.-F. Chang, J. Hsu, and M. Pepeljugoski. Columbia photographic images and photorealistic computer graphics dataset. Technical report, Columbia University, 2005.

[10] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui. Physics-motivated features for distinguishing photographic images and computer graphics. In *Proc. ACM MM*, 2005.

[11] A. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. *IEEE Trans. on Signal Processing*, 2005.

[12] A. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *Trans. on Signal Processing*, 2005.

[13] V. Potdar, S. Han, and E. Chang. A survey of digital image watermarking techniques. *Proc. Industrial Informatics*, 2005.

[14] A. Swaminathan, M. Wu, and K. J. R. Liu. Non-intrusive forensic analysis of visual sensors using output images. In *Proc. ICASSP*, 2006.

[15] C.-Y. Tsai and K.-T. Song. A new edge-adaptive demosaicing algorithm for color filter arrays. *Image Vision Comput.*,
2007.

[16] Wikipedia. list of computer-animated films. Downloaded March 2008. http://en.wikipedia.org/wiki/Listof
computeranimated
films.