Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 6, Issue, 03, pp.5955-5958, March, 2014

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

PHOTO MORPHING DETECTION

Galphade, M. N., Suresh Khule, *Sumit Sharma and Rohit Khose

Department of Computer Engineering, Pune University, India

ARTICLE INFO

Article History:
Received 10th December, 2013
Received in revised form
19th January, 2014
Accepted 14th February, 2014
Published online 31st March, 2014

Key words:
Demosaicing,
Color Filter Array,
High pass Filter,
Morphing.

ABSTRACT

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 main aim of this project is to provide software which will help to detect the manipulation in the photo. Most digital cameras employ an image sensor with a color filter array such as shown on the left. The process of Demosaicing interpolates the raw image to produce at each pixel an estimate for each color channel. With proper analysis, traces of Demosaicing are exhibited in the peak of an analysis signal. The presence of Demosaicing indicates the image is from a digital camera rather than generated by a computer.

INTRODUCTION

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 of 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.

Traditional, Analog Photography

Traditional photography is an analog science. Light enters through a camera‘s lens and the image the camera views is faithfully recorded onto a negative. This negative is then printed into a recognizable image. Although the images represented in the photograph have typically been faithful to the image seen by the camera, photographic trickery and distortion have long existed. Several variables affect how a photo turns out, all of which can either subtly or drastically change the story a photo tells. A low-angle shot, for instance, can make a human subject seem much taller than she is in reality. Spotting, cropping, color balancing, brightness and contrast adjustment, burning, and dodging, and adjusting exposure time are also very common ways to manipulate the story told by a photograph. For decades, books, newspapers, and magazines have used photographs to tell fantastic and impossible stories, from self-propelled, flying men to proof of the existence of jack elopes. And yet, analog photographs maintain their integrity because alterations and manipulations to an analog print have always been very easy to detect. In fact, by looking for four different types of clues density, shadows splice lines, and image continuity it becomes simple to finger a fraudulent analog photograph. Moreover, making alterations to analog photographs is a complicated and costly ordeal.

When the Federal Rules of Evidence were enacted in 1975, the fidelity of photographs was presumed, which did not present a problem because the ease with which modifications and manipulations could be identified made it a very manageable matter for courts to protect themselves from fraudulent photographs. Since then, however, digital technology has permeated society, making it more costly for courts to be cavalier about what images are considered authentic. In fact, today it may be more accurate to say that a picture is worth a thousand lies.

Corresponding author: Sumit Sharma
Department of Computer Engineering, Pune University

Modern, Digital Photography

Digital photography is the new norm for image capture. Digital cameras, in contrast to their analog complements, do not store information in a continuous medium. Instead, information is recorded in discrete bits of information called binary code, which is a string of ones and zeroes that makes up the storage language of hard drives, compact discs, computers, and all other digital devices. By using a series of numbers, instead of the continuous crests and troughs characteristic of analog information, digital image manipulation is much easier, cheaper, and infinitely more difficult to detect than an analog alteration. The main aim of the project is to provide software which will help to detect the manipulation in the photo. Most digital cameras employ an image sensor with a color filter array such as shown on the left. The process of demosaicing interpolates the raw image to produce at each pixel an estimate for each color channel. With proper analysis, traces of demosaicing are exhibited in the peak of an analysis signal as shown on the right. The presence of demosaicing indicates the image is from a digital camera rather than generated by a computer.

As shown in above fig. The first one is original one and the second one is edited using photo editing software. But we are not able to recognize the Image easily .So this is our Problem statement which gives us a challenge to Distinguish between photographic images and photorealistic computer generated images.

Related Work

Many approaches are there to identify whether the image is manipulated or not. Image can be authenticated by Digital watermarking [3]. Various watermark techniques, have been proposed in recent years, which can be used not only for authentication, but also for being an evidence for the tamper detection. Wang et al. and Lin et al. Both embedded watermarks consisting of the authentication data and the recovery data into t is forged inside other image. Two methods have been suggested for achieving the authenticity of digital images: having a digital camera sign the image using a digital signature, or embedding a secret code in the image. The first method uses an encrypted digital \signature" which is generated in the capturing devices. A digital signature is based on the method of Public Key Encryption. A private key is used to encrypt a hashed version of the image. This encrypted message is called the signature of the image, and it provides a way to ensure that this signature cannot be forged. This signature then travels with the image. The authentication process of this image needs an associated public key to decrypt the signature. The image received for authentication is hashed and compared to the codes of the signature. If they match, then the received image is authenticated. Above methods have clear drawbacks. In their propositions, authenticity will not be preserved unless every pixel of the images is unchanged. There are several possible approaches for authenticating the source of a digital image.

An Active Approach for Manipulation Detection

Image can be authenticated by Digital watermarking. Various watermark techniques, have been proposed in recent years, which can be used not only for authentication, but also for being an evidence for the tamper detection. Wang et al. and Lin et al. Both embedded watermarks consisting of the authentication data and the recovery data into image blocks for image tamper detection and recovery in the future. The drawback of watermark techniques is that one must embed a watermark into the image first. Also a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. Many other techniques that work in the absence of any digital watermark or signature have been proposed.

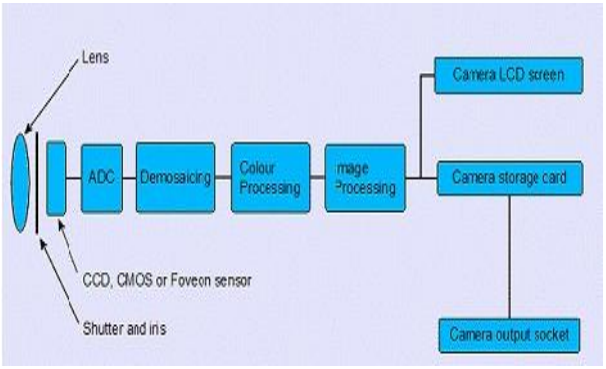
Passive Approach for Manipulation Detection

In contrast to approaches such as active digital watermarking and Steganography, passive techniques for image manipulation detection are carried out in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools for passive or blind approach for manipulation detection can be roughly categorized as pixel-based techniques, format-based techniques, camera-based techniques geometric based techniques.

Image Formation

In the digital cameras , the image formation is not due to the chemical reaction that take place, rather it is a bit more complex then this. In the digital camera, a CCD array of sensors is used for the image formation. CCD stands for charge-coupled device. It is an image sensor, and like other sensors it senses the values and converts them into an electric signal. In case of CCD it senses the image and convert it into electric signal e.t.c. This CCD is actually in the shape of array

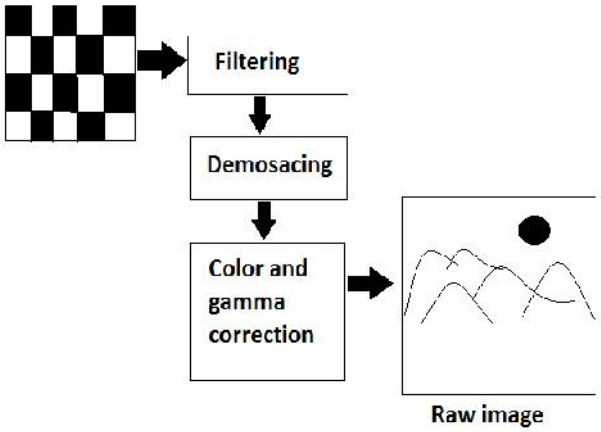
or a rectangular grid. It is like a matrix with each cell inthe matrix contains a censor that senses the intensity of photon. In Image formation firstly light passes from scene to be capture to the lens. after that there is analog to Digital converter which converts analog signals to the digital levels .after that Demosaicing process takes place in which every pixel has given an appropriate RGB value, missing values are obtained by using neighboring pixel values, after that there is color processing in which colors are processed according to their RGB values, finally image processing takes place and image is stored in storage of camera. There are two parts to the image formation process The geometry of image formation, which determines where in the image plane the projection of a point in the scene will be located. The physics of light, which determines the brightness of a point in the image plane as a function of illumination and surface properties.



Like analog cameras, in the case of digital too , when light falls on the object, the light reflects back after striking the object and allowed to enter inside the camera. Each sensor of the CCD array itself is an analog sensor. When photons of light strike on the chip, it is held as a small electrical charge in each photo sensor. The response of each sensor is directly equal to the amount of light or (photon) energy striked on the surface of the sensor. Since we have already define an image as a two dimensional signal and due to the two dimensional formation of the CCD array, a complete image can be achieved from this CCD array. It has limited number of sensors, and it means a limited detail can be captured by it. Also each sensor can have only one value against the each photon particle that strike on it. So the number of photons striking (current) are counted and stored. In order to measure accurately these, external CMOS sensors are also attached with CCD array.

Demos icing

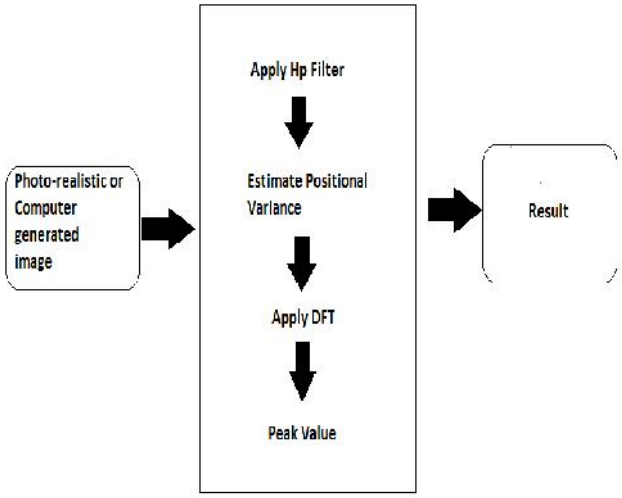
Demos icing algorithm is a digital image process which is use to reconstruct a full color image from the incomplete color sample output taken from the image. This color is taken with the help of CFA i.e. (color filter array) which takes or sense the color information while taking animage. Here, the Demos icing is comes while taking a real image through camera. This traces of Demos icing we are detecting in the whole process. This demos icing is the reconstructors which do the work of completing the incomplete portion of the image. While taking an image through a camera there is a loss of resolution, blurness and have no proper visibility. Here, the work of demos icing began it make all the incomplete work



to the top. By adding quality, color, resolution, remove blurness and more. This work is of demos icing with the help of CFA. This can also be called as CFA interpolation or color reconstructors i.e. it is builder. In general, demos icing algorithm have several feature in common missing color value are determined from neighboring pixel and then made it complete.

System Architecture

System architecture for Photo Morphing Detection is shown below. First a high pass filter is applied, then the variance of each diagonal is estimated. Fourier analysis is



used to find periodicities in the variance signal, indicating the presence of demosaicing. Combining the neighboring pixel values, an interpolated pixel value is generated. The variance gets affected by the weight of the neighboring pixels which produce an interpolated pixel value. This forms the pattern of variances which can be detected and serves as the basic idea for detecting demosaicing. For demonstrating our approach we consider channels of only specific color while use of any channel is permitted during actual system implementation. Figure 3 shows the basic flow of our approach. First high pass operator h(x, y) is operated on the image i(x,y) and low frequency information is removed from it. When demosaicing occurred, embedded periodicity is also enhanced. Operator selection is done:

$$h(x,y) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

The variance of the output of operator can be found from a distribution with variance σ^2. If we again make the simplifying assumption that the channel is interpolated with linear interpolation:

$$\sigma_0^2 = 4\left(\frac{1}{4}\right)^2 \sigma^2 + 4\left(\frac{1}{2}\right)^2 \sigma^2 + (1-4)^2\sigma^2$$

$$= \frac{41}{4}\sigma^2$$

$$\sigma_i^2 = 0\sigma^2$$

σ_0^2 is the variance of the output of application of $h(x,y)$ at positions corresponding to original photosites in the image sensor, and thus nine pixel values from the original sensor contribute to the filter output and four with a coefficient $\frac{1}{4}$, four with a coefficient $\frac{1}{2}$, and position (x, y) itself has coefficient -3. σ_i^2 Corresponds to locations where the green value is interpolated by considering the green channel is interpolated with linear interpolation. In case, if missing green values were actually estimated with linear interpolation and all other image processing operations in the camera are ignored, then application of the filter h(x, y) yields a value of zero at each pixel location with an interpolated green value. The choice of h(x, y) was made to maintain a large value for $\frac{\sigma_0^2}{\sigma_i^2}$ and testing using a small number of training images. A large ratio of $\frac{\sigma_0^2}{\sigma_i^2}$ aids in the detection of the periodic pattern of variances characteristic of demosaicing.

Our test images are different from the demosaicing operated images. Test images are finished images from real consumer cameras. Demosaicing is performed on nonlinear filter and the image processing path contains various activities such as noise suppression, image enhancement etc. After that, estimate of the variances is calculated using the method called Maximum Likelihood Estimation (MLE). The statistical variance of the pixel values along each diagonal is found to compute the MLE estimation of variance. This projects the image down to a single-dimension signal, $m(d)$, where $m(d)$ represents the estimate of the variance corresponding to the d^{th} diagonal:

$$m(d) = \frac{\sum_{x+y=d} |h(x,y) * i(x,y)|}{N_d}$$

Where, N_d is the number of pixels along the d^{th} diagonal and is used for normalization. To find the periodicity in $m(d)$, the DFT is computed to find $|M(e^{j\omega})|$. A relatively high peak at frequency $\omega = \pi$ indicates that the image is not morphed and it is the characteristic of demosaicing. The peak magnitude at $\omega = \pi$ is calculated as:

$$s = \frac{|M(e^{jw})|_{\omega=\pi}}{k}$$

Where $\omega = \pi$high peak value at frequency ω and k is is the median value of the spectrum, by omitting the DC value. Normalizing by k was found to be vital to differentiate between true image and images containing signals with large energy across the frequency spectrum thus we can distinguish between photographic image and computer generated photorealistic image.

Conclusions and Future Work

Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. There is such a strong demand for image manipulation techniques and applications that they are becoming more and more sophisticated and are accessible to a greater number of people. It is new photo-morphing detection framework proposed for image content authentication such that the original image can be restore is robust to JPEG compression and is signed with cryptographic signature algorithm. According to our experiment result, we claim that our system survive JPEG compression with quality factor. Future work includes refining our method to be applicable to more images format and to increase the robustness of the system to tolerate lower JPEG compression quality factor.

REFERENCES

Andrew C. Gallagher, Tsuhan Chen, "Image Authentication by Detecting Traces Of Demosaicing" IEEE 2013.

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

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

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

Popescu, A. and H. Farid. Exposing digital forgeries by detecting traces of resampling. *IEEE Trans. on Signal Process-ing*, 2005

****