

Image Forgery Localization via CFA Based Feature Extraction and Poisson Matting

Priyanka Prasad

M-Tech, Department of CSE, SNGCE, Kadayiruppu, Ernakulam, Kerala, India

Abstract: *In this era of digital computing, peoples are used to represent the information that they want to convey in visual forms. Representing in visual forms rather than in pure text form make them more understandable. Digital camera images are used in several important applications in the recent decades. But with widespread availability of image processing and editing software make the integrity of digital camera images at risk. Soverifying the authenticity and integrity of digital images, and detecting the traces of forgery are important. In order to develop techniques for detecting the forgeries and to improve them, a separate science has been formed, called the Image Forensic Science. A lot of methods have been developed to solve the issue This paper describes a novel passive fine grained approach to this problem. we use an in-camera processing method to detect the forgery rather than focusing on the statistical differences between the images textures. 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. The proposed method detects the forgery by estimating a feature value that indicates presence of demosaicing artifacts (interpolation relationship). After detecting the forgery, poisson matting algorithm is used enhance result by cutting the forged region from the image. This method can localize forged region efficiently.*

Keywords: Image Forensic Science, Image Tampering Detection, Blind Methods, Active Methods, CFA interpolation, Demosaicing Artifacts, Poisson Matting

1. Introduction

This paper focuses on the problem of image tamper localization. We use the term tamper in a very broad sense to mean any post-processing operation that has been performed on an image. Many image tamper detection techniques have been proposed in the past years. But some of these techniques focus on detecting a particular type of tampering operation such as resizing, cloning, recompression, splicing. These techniques are Targeted Tamper Detection techniques. Another class of techniques try to detect the presence of generic image manipulation operations that may be indicative of tampering such as filtering, down-sampling, up-sampling, compression, rotation, etc.. These techniques do not necessarily determine what operation has been performed but only that the entire image has been subject to post-processing. We call such techniques Universal Tamper Detection techniques. A third category of techniques for local tamper detection work by detecting inconsistencies in image characteristics, statistics and content across different regions, examples include techniques that detect the presence of inconsistencies in sensor noise pattern, chromatic aberration, lighting. We call such techniques Localized Tamper Detection techniques. In this paper, I develop Color Filter Array (CFA) demosaicing based tamper detection techniques which can be used to detect both local and global tampering operations. The proposed techniques do not target any specific operation but are applicable to a variety of operations such as splicing, retouching, re-compression, resizing, blurring etc. The proposed methods differ from known universal tamper detection techniques in the sense they do not require a complex classifier; instead they use only one feature value to make a decision about the image in question. The basic approach is based on the fact that typically an image tampering operation alters CFA demosaicing artifacts in a measurable way. The absence of CFA artifacts may indicate the presence of global or local

tampering. In this paper, Author proposes a method based on CFA artifacts.

2. Related Works

There are lots of methods has been proposed to detect the tampering. The methods are mainly divided into two classes. They are active methods and passive methods. The active forgery detection techniques can be divided into the data hiding approach (e.g., watermarks) and the digital signature approach. The passive approaches are also known as blind approaches, since they do not have any prior information about the image features.

Cao et al [11] proposes a novel accurate detection framework of demosaicing regularity from different source images. This paper discusses the reverse classification of the demosaiced samples into several categories and then estimating the underlying demosaicing formulas for each category based on partial second-order derivative correlation models, which detect both the intra-channel and the cross-channel demosaicing correlation. A classification scheme called expectation-maximization reverse is used to iteratively resolve the ambiguous demosaicing axes in order to best reveal the implicit grouping adopted by the underlying demosaicing algorithm. The drawback of this technique is that noise variation detection need to be incorporated.

Dirik and Memon [17] proposes a detection method that uses the artifacts produced by the color filter array (CFA) processing in most digital cameras. Here, two CFA features are extracted and techniques are developed based on these features. The techniques are based on computing a single feature and a simple threshold based classifier. The limitation of the technique proposed here is that this technique is sensitive to strong JPEG re-compression and resizing.

Mahdian and Saic proposed in [20], forgery detection techniques, where the image noise in consistencies are considered for the detection of traces of tampering. A segmentation method that detects changes in noise level is proposed here. A commonly used tool to conceal the traces of tampering is the addition of locally random noise to the altered image regions. The noise degradation is the main reason for the failure of many active or passive image forgery detection methods. Usually, the amount of noise is uniform across the entire authentic image. Adding locally random noise may create inconsistencies in the image's noise. Therefore, the tampering can be found by the detection of various noise levels in an image may signify. The technique proposed in this paper is capable of dividing an investigated image into various partitions with homogenous noise levels. The local noise estimation is based on tiling the high pass wavelet coefficients at the highest resolution with non-overlapping blocks. The noise standard deviation of each block is estimated using the widely used median-based method. The standard deviation of noise is used as the homogeneity condition to segment the investigated image into several homogenous sub-regions. This method can be used as a supplementary along with other blind forgery detection tasks, but the limitation is that the method fails whenever the degradation of noise is very small.

Gallagher and Chen [21] introduce a concept based on the demosaicing features. Rather than focusing on the statistical differences between the image textures, the feature of images from digital cameras are recognized to contain traces of resampling as a result of using a color filter array with demosaicing algorithms. Here the estimation of the actual demosaicing parameters is not necessarily considered; rather, detection of the presence of demosaicing is taken into consideration. The in camera processing (rather than the image content) distinguishes the digital camera photographs from computer graphics. The presence of demosaicing is a checklist being used in this detection algorithm. The drawback is that if a malicious computer animator wishing to add an element of realism to her computer graphic images could simply insert a software module to simulate the effect of color filter array sampling and then apply demosaicing. Here this algorithm might fail, and therefore this type of algorithm is not an effective way to deal with such attacks.

Z. Lin, J. He, X. Tang [24] proposed a method for Fast, automatic and fine-grained tampering detection in JPEG image via DCT coefficient analysis. The method is based on the DQ effect. The DQ effect is the exhibition of periodic peaks and valleys in the histograms of the discrete cosine transform (DCT) coefficients in forged JPEG images. The main advantage of this method is that it can produce fine-grained output of the forgery region at the scale of 8×8 image blocks. The other four advantages of our algorithm, namely automatic tampered region determination, resistant to different kinds of forgery techniques in the tampered region, ability to work without full decompression and fast detection speed, make our algorithm very attractive. Main drawback of this approach is that the estimation of quantization from only the underlying DCT coefficients is both computationally nontrivial, and prone to some estimation error, which leads to vulnerabilities in the forensic analysis. They tried to use the inconsistency to locate the

tampered region. However, the average detection rate both in image level and region level are below 65%; and their method are sensitive to the estimation of the period.

In [9], Hany Farid proposes a technique to detect whether the part of an image was initially compressed at a lower quality than the rest of the image, which is applicable to images of high and low quality as well as resolution. This concept mainly depends upon the following basis. When creating a digital forgery, for example, when compositing one person's head onto another person's body. If these images were originally of different JPEG compression quality, then the digital composite may contain a trace of the original compression qualities, where the above approach comes into existence. The drawback of this method is that the complexity of the analysis is very high. Another limitation is that it is only effective when the tampered region is of lower quality than the image into which it was inserted. The main advantage of this approach is that it is effective on low-quality images and can detect relatively small regions that have been altered. And the approach does not require that the image be cropped in order to detect blocking inconsistencies. In addition, this approach can detect local tampering unlike the global approach which can only detect an overall crop and re-compression.

In [1] Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva proposed a method namely improved DCT coefficient analysis for forgery localization in JPEG images. This method discriminates between original and forged regions in JPEG images, under the assumption that the former are doubly compressed while the latter are singly compressed. Main benefit of this approach is the significant improvement of the accuracy of the probability map estimation and consequently of the algorithm performance and unlike previous method it provide a probability map. Main drawback is that it is fine grained with a scale of only 8×8 blocks. This method work only in the presence of aligned double JPEG compression,

In [5], Alin C. Popescu and Hany Farid assumed that image tampering would involve resampling. They proposed approaches to detect periodicity of correlations introduced by resampling. Here authors describe a technique for detecting traces of digital tampering in the complete absence of any form of digital watermark or signature. This approach works on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may, nevertheless, alter the underlying statistics of an image. In order to create a convincing match, it is often necessary to re-size, rotate, or stretch portions of the images. This process requires re-sampling the original image onto a new sampling lattice. Although this re-sampling is often imperceptible, it introduces specific correlations into the image, which when detected can be used as evidence of digital tampering. This technique is able to detect a broad range of re-sampling rates, and is reasonably robust to simple counter attacks. But, this technique is not able to uniquely identify the specific re-sampling amount, as different re-samplings will manifest themselves with similar periodic patterns. They have only described how linear or cubic interpolation can be detected. However, they did not give enough real examples for tampered region localization.

Jia et al [14] proposed a method to remove a particular region of interest. In this paper, the problem of natural image matting is formulated as one of solving Poisson equations with the matte gradient field. The approach, called Poisson matting, has the following advantages. First, the matte is directly reconstructed from a continuous matte gradient field by solving Poisson equations using boundary information from a user supplied trimap. Second, by interactively manipulating the matte gradient field using a number of filtering tools, the user can further improve Poisson matting results locally the desired output is obtained. The modified local result is seamlessly integrated into the final result. The limitation is that when the foreground and background colors are very similar, the matting equation becomes ill-conditioned, in which case the underlying structure of the matte cannot be easily distinguished from noise, background or foreground. The second difficulty arises when the matte gradient estimated in global Poisson matting largely biases the true values, so that small regions need to be processed for local refinements in local Poisson matting, which increases user interaction. Last, when the matte gradients are highly interweaved with the gradients of the foreground and background within a very small region. Effective user interaction is an issue in this difficult situation.

3. Proposed Algorithm

In order to overcome the demerits of existing passive forgery detection, a passive method based on demosaicing artifacts has been developed. The proposed algorithm has four major stages. They are feature extraction, forgery detection, probability map generation and poission matting (shown in fig 1).The first stage feature extraction calculates a new feature value that indicates the presence of CFA artifacts. The second stage forgery detection checks the feature value extracted to detect the forgery. If forgery is detected in the second stage, third stage produces a map in which the probability of each block to be forged is noted. The last stage removes the forged area with the aid of the probability map.

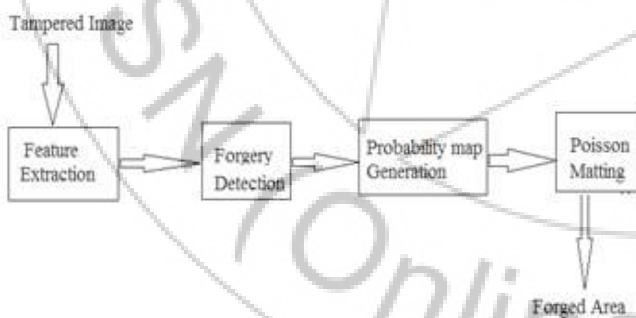


Figure 1: Work Flow of Proposed Algorithm

3.1 Feature Extraction

Feature extraction is the first step. Here we are using an in camera processing method to calculate the feature value. We are using the demosaicing (CFA interpolation) process. Usually when taking images using digital cameras, it does not capture all three RGB components of a pixel, it only captures one of the three according to the filter array used. Commonly used filter array is Bayer's filter (shown in fig 2).

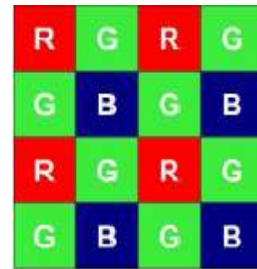


Figure 2: Bayer's Filter

After capturing the image, it looks like mosaic floor. To create the actual image, camera does demosaicing. In demosaicing, cameras find the remaining components of each pixel by interpolating near-neighbour values. The green channel is considered during the feature extraction because in bayer's filter the numbers of green pixels are upsampled by a factor of 2. So green channel is used for feature extraction to make the results accurate.



Figure 3: Green Channel

In Fig 3. *A* represents the acquired green pixels and *I* represents the interpolated green pixels. Here we are using a bayer filter of order 2x2 (fig 4) that means for each 2x2 block we are calculating the feature value rather than calculating one feature value for entire image .



Figure 4: 2x2 bayer filter

Let us suppose $s(x,y)$ is the image. The prediction error is calculated as:

$$e(x,y) = s(x,y) - \sum_{u,v \neq 0} k_{u,v} s(x+u,y+v) \quad \text{-----}(1)$$

Where $K_{u,v}$ the interpolation kernel.

In order to make the method content independent, we calculate the local weighted variance of the prediction error as:

$$\sigma_e^2(x,y) = \frac{1}{c} \left[\left(\sum_{i,j=-K}^K \alpha_{ij} e^2(x+i,y+j) \right) - (\mu_e)^2 \right] \quad \text{-----}(2)$$

Where α_{ij} are suitable weights, $\mu_e = \sum_{i,j=-K}^K \alpha_{ij} e(x+i,y+i)$ is a local weighted mean of the prediction error and $c = 1 - \sum_{i,j=-K}^K \alpha_{ij}^2$ is a scale factor that makes the estimator unbiased, i.e., $E[\sigma_e^2(x,y)] = \text{var}[e(x,y)]$ for each pixel class.

The feature value L for block is given as:

$$L(k, l) = \log \left[\frac{GM_A(k, l)}{GM_I(k, l)} \right]$$

where $GM_A(k, l)GM_I(k, l)$ is the geometric mean of the variance of prediction errors at interpolated pixel positions and whereas $GM_A(k, l)$ is similarly defined for the acquired pixels.

A. Forgery Detection

Forgery is detected by checking the value of proposed feature. For an untampered image, the histogram of feature is a gaussian distribution, but in tampered image histogram is a mixture of gaussians (fig 5.)

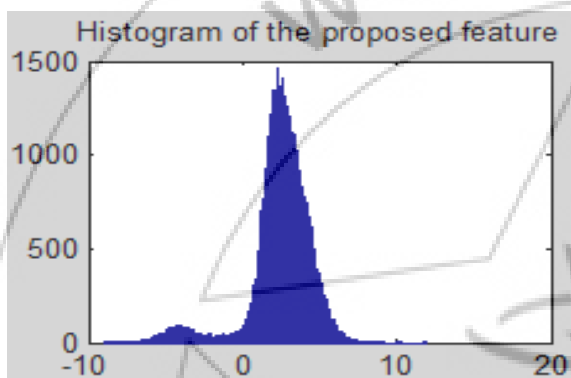


Figure 5: Histogram of feature(tampered image)

Usually in case of forgery the local variance of the prediction error of acquired pixels is higher than that of interpolated pixels. Otherwise, if image is forged, the value of feature L is positive.

B. Probability Map Generation

Third step is the probability map generation. The map indicates the probability of each 2x2 block of the image to be forged. By Assuming the priori probability to be forged and not forged is 1/2, we get posterior probability of being an original block by exploiting Baye's theorem.

C. Poisson Matting

Matting refers to the process of extracting foreground object from an image. Matting is an important task in image and video editing. Matting tasks usually produces a "matte" that can be used to separate foreground from the background in a given image. Matte can also used to combine a given foreground on a different background to produce new plausible image. An image is a composite of foreground and background. Hence each pixels intensity is a linear combination of a foreground and background that can be written as:

$$I_i = \alpha_i * F_i + (1-\alpha_i) * B_i \quad \text{-----(4)}$$

In matting equation all quantities on the right of the equation are unknown. Thus for a color image we have 7 unknowns and 3 equations. Hence this problem is severely under-constrained. So a rough segmentation of foreground and background is required to extract a good matte. This segmentation can be in form of trimap or scribbles.

In my work, i use poisson matting to extract the forged area from the tampered image by providing a trimap. Here the trimap indicates the definitely forged and definitely not forged part. At stage of poisson matting, user should provide the trimap to extract the forged part if any. Trimap can be generated by using the probability map which shows the probability of each block to be forged.

Poisson matting algorithm takes trimap and tampered image as input. By solving the poisson equations we can remove the forged part. Global poisson matting is used

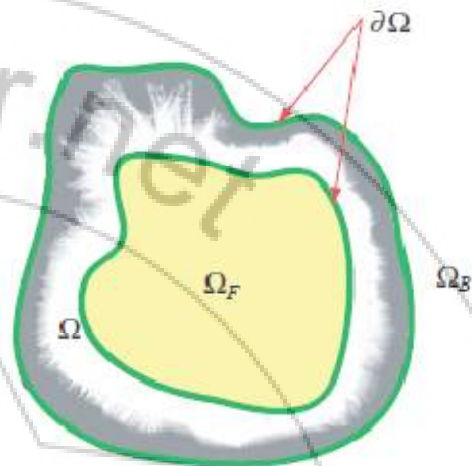


Figure 6: Boundary Condition For Poisson Matting

As shown in Fig7, Ω_F , Ω_B and Ω are defined as "definitely forged", "definitely not forged" and "unknown" regions respectively. For each pixel $p = (x, y)$ in the image, I_p is its intensity, F_p and B_p are the foreground and background intensity respectively. Let N_p be the set of its 4 neighbours. $\partial\Omega = \{p \in \Omega_F \cup \Omega_B \mid N_p \cap \Omega \neq \emptyset\}$ is the exterior boundary of Ω . To recover the matte in the unknown region Ω given an approximate $(F - B)$ and image gradient ∇I , we minimize the following variational problem:

$$\alpha^* = \arg \min_{\alpha} \int \int_{p \in \Omega} \left\| \nabla \alpha_p - \frac{1}{F_p - B_p} \nabla I_p \right\|^2 dp \quad \text{---(5)}$$

The associated Poisson equation with the same boundary condition is:

$$\Delta \alpha = \text{div} \left(\frac{\nabla I}{F - B} \right) \quad \text{-----(6)}$$

Where $\Delta = (\partial^2/\partial x^2 + \partial^2/\partial y^2)$ and div are Laplacian and Divergence operators respectively.

Global Poisson matting is an iterative optimization process:

- (F - B) initialization** Absolute values of F and B are not necessary, since $(F - B)$ provides enough information to determine the matte. Initially, for each pixel p in Ω , F_p and B_p are approximated by corresponding the nearest forged pixel in Ω_F and not forged pixel in Ω_B . Then, the constructed $(F - B)$ image is smoothed by a Gaussian filter to suppress significant changes due to noise and inaccurate estimation of F and B .

2. α reconstruction α is reconstructed by solving Poisson equation(6) using the current $(F - B)$ and ∇I .

3. F, B refinement Let $\Omega^+_F = \{p \in \Omega | \alpha p > 0.95, I_p \approx F_p\}$. The condition $\alpha p > 0.95$ and $I_p \approx F_p$ guarantee that the pixels in Ω^+_F are mostly forged. Similarly, let $\Omega^+_B = \{p \in \Omega | \alpha p < 0.05, I_p \approx B_p\}$. Here, F_p, B_p and I_p represent the color vectors at pixel p . We update F_p and B_p according to the color of the nearest pixels in Ω^+_F and in Ω^+_B , respectively. A Gaussian filter is also applied to smooth $(F - B)$.

We iterate the above steps 2 and 3 until change in the matting results is sufficiently small or both Ω^+_F and Ω^+_B are empty in step 3. Typically, only a few iterations are needed. In each iteration, the selection of Ω^+_F and Ω^+_B has little error, which guarantees that more accurate colors in these two regions are further propagated into less accurate neighboring pixels. Global Poisson matting works well in scenes with a smooth foreground and background.

4. Results

All cameras are equipped with bayer filter, so the method work on all camera captured images. To make the result fine grained we use a bayer filter of order 2x2. The method work well on copy-move and splicing forged images.

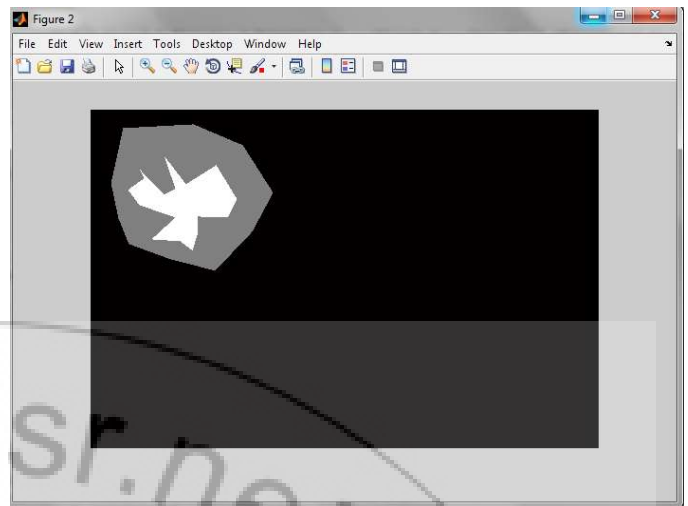


Figure 8: Trimap

Figure 8 shows the trimap. For generating this trimap user should set definitely forged and not forged region in image. In this, black coloured area represents the definitely not forged area, white coloured area represents the definitely forged area and grey coloured area represents the unknown regions where the poisson matting should apply.

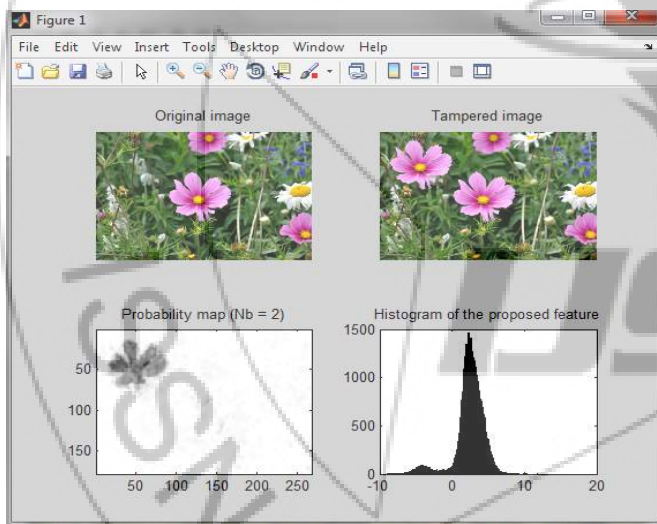


Figure 7: Forgery Detection

In fig 7, bright areas of map indicate high probability of presence of demosaicing artifacts, whereas dark areas indicate low probability of presence of demosaicing artifacts. Here the histogram is a mixture of gaussians, so the image is forged.

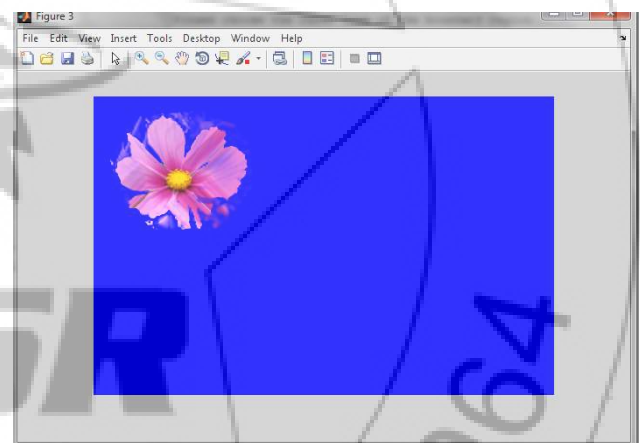


Figure 9: Forged Area

Fig 9 shows forged area. This is the output of poisson matting.

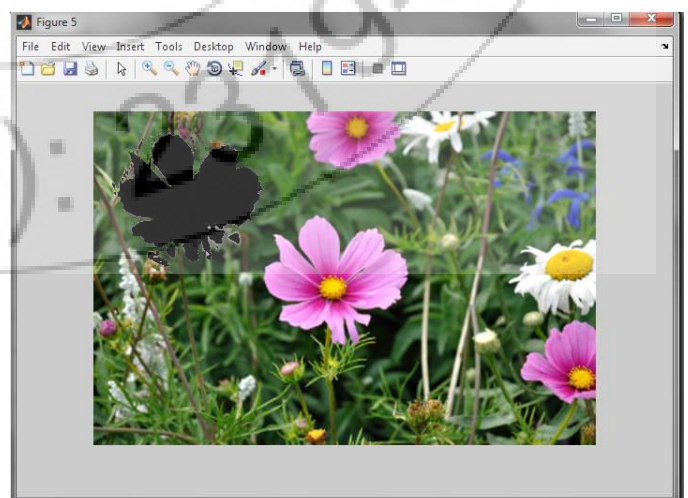


Figure 10: Image after Removing Forged Part

5. Conclusion

Sophisticated tools and software's have made forgery detection are challenging one. Image forensic is still a growing area in this era. There are techniques exhibiting improved detection accuracy, but having high computational complexity. Most of the techniques existing not effective by one or more factors that include limited accuracy rate, low reliability and high complexity in addition to their sensitivity to various transformations and non-responsiveness to noise. Most of the passive forgery detection methods are mainly applied to the image and can be extended to audio and video.. Considering the CFA demosaicing artifacts as a digital fingerprint, we proposed a new feature measuring the presence of demosaicing artifacts even at the smallest 2x2 block level; by interpreting the local absence of CFA artifacts as an evidence of tampering, the proposed scheme provides as output a forgery map indicating the probability of each block to be trustworthy. Further poisson matting is used to cut the forged area from the inputted image.

6. Future Scope

By using other segmentation methods available instead of poisson matting to cut down the forged part more correctly and to make results much better.

References

- [1] A. D. Rosa T. Bianchi, , and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in Proc. of ICASSP 2011, Prague, Czech Republic, May 2011, pp. 2444–2447.
- [2] Babak Mahdian, Stanislav Saic, 'Cyclostationary Analysis applied to Image Forensics', 2009 IEEE, pp: 279-284.
- [3] Chiou-Ting Hsu Yi-Lei Chen, , ' Detecting Recompression of JPEG Images via Periodicity Analysis of Compression Artifacts for Tampering Detection', IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011.
- [4] Farid, H ,Johnson, M.K.,.: Exposing digital forgeries by detecting inconsistencies in lighting. ACM Multimedia and Security Workshop, pp. 1–10 (2005)
- [5] Farid, H ,Popescu, A.C.,: Exposing digital forgeries by detecting traces of resampling.IEEE Transactions on Signal Processing 53(2), 758–767 (2005)
- [6] Farid, H ,Popescu, A.C.,.: Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing 53(10), 3948–3959 (2005)
- [7] Ferrara, Piva,Rosa,, 'Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts', 2012 IEEE.
- [8] Guangjie Liu, Junwen Wang, Shiguo Lian, Yuewei Dai, ' Detect image splicing with artificial blurred boundary', Elsevier 2013, pp: 2647-2659.
- [9] Hany Farid, 'Exposing Digital Forgeries from JPEG Ghosts', IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 1, MARCH 2009, Pp: 154-160.
- [10] H. Farid, and M. K. Johnson, "Exposing Digital Forgeries Through Chromatic Aberration," ACM 1595934936/06/0009. MM & Sec'06, September 26–27, 2006, Geneva, Switzerland.
- [11] Hong Cao, 'Accurate Detection of Demosaicing Regularity for Digital Image Forensics',IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4,NO. 4, DECEMBER 2009, pp. 899-910.
- [12] Irene Amerini,Lamberto Ballan, Roberto Caldelli, Alberto DelBimbo, Giuseppe Serra ,Luca Del Tongo, 'Copy Move Forgery Detection And Localization By Means Of RobustClustering With JLinkage'.
- [13] Johnson, M.K., Farid, H.: Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security 2(3), 450–461(2007)
- [14] Jiaya Jia, Jian Sun, Tang, Shum, 'Poisson Matting', unpublished.
- [15] Kaiming He, Christoph Rhemann, Carsten Rother, Xiao Tang, Jian Sun, 'A Global Sampling method for Alpha Matting', 2049-2056.
- [16] Luka, J.,Goljan, M, Fridrich, J.,.: Detecting digital image forgeries using sensor pattern noise. In: Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 6072, pp. 362–372 (February 2006)
- [17] Nasir Memon, Ahmet Emir Dirik, 'Image Tamper Detection based on demosaicing artifacts', IEEE Transactions 2010.
- [18] Radim Nedbal, Babak Mahdian, and Stanislav Saic, 'Blind Verification of Digital ImageOriginality: A Statistical Approach', IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 9, SEPTEMBER 2013, pp: 1531-1540.
- [19] Sheetal Kusal and Prof.Jyoti Rao, "Robust Image Alignment Using SVM Clustering forTampering Detection", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 5, 2013, pp. 147 - 154, ISSN Print: 0976 – 6367, ISSN Online:0976 – 6375.
- [20] Stanislav Saic, Babak Mahdian, 'Using Noise Inconsistencies For Blind Image Forensics',Elsevier, Image and Vision Computing 27 (2009) 1497–1503.
- [21] Tshuan Chen Andrew C. Gallagher, , ' Image Authentication by Detecting Traces ofDemosaicing', unpublished.
- [22] WeiLu, WeiSun Zhongwei He, , JiwuHuang, 'digital Image Splicing Detection Based onMarkov Features in DCT and DWT', Elsevier 2012, 4292-4299.
- [23] Yuenan Li, ' Image copy-move forgery detection based on polar cosine transform andapproximate nearest neighbor searching', Elsevier 2013, 59-67.
- [24] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," Pattern Recognition 2009 - Elsevier, pp. 2492–2501, 2009.

Author Profile



Priyanka Prasad received the B-Tech degree in computer science and engineering from Sree Narayana Gurukulam College of Engineering, Mahatma Gandhi University, Kottayam, Kerala, India in 2012. Now pursuing M-Tech in computer science and engineering from Sree Narayana Gurukulam College Of Engineering, Mahatma Gandhi University, Kottayam, Kerala, India.