ISSN:0975-9646

A Novel Approach for Detecting of Tampering On Images

Sajja.Karthik
M.Tech, Department of CSE,
Vignan's Lara Institute of Technology & Science,
Vadlamudi, Guntur District.

***M.Gargi**
Assistant Professor, Department of CSE,
Vignan's Lara Institute of Technology & Science,
Vadlamudi, Guntur District.

Abstract: **In Our Society Digital Images Are Powerful And Widely Used In Communication Medium. They Have An Important Impact On Our Lives. In The Recent Years, Due To The Advent Of High Performance Commodity Hardware And Improved Human Computer Interfaces. It Has Become Relatively Easy To Create The Fake Images. In The Modern Days, It Is Easy To Use Image Forgeries That Are Undetectable By The Naked Eye. We Make The Assumption That The Image Is Acquired Using A Color Filter Array, And That Tampering Removes The Artifacts Due To The Demosaicking Algorithm. A New Feature Measuring The Presence Of Demosaicking Artifacts At A Local Level, And On A New Statistical Model Allowing Deriving The Tampering Probability Of Each 2x2 Image Block Without Requiring To Know *A Priori* The Position Of The Forged Region. Experimental Results On Different Cameras Quipped With Different Demosaicking Algorithms Demonstrate Both The Validity Of The Theoretical Model And The Effectiveness Of Our Scheme.**

Keywords: Cfa Artifacts, Digital Camera Demosaicking, Forgery Localization, Image Forensics, Tampering Probability Map.

I. INTRODUCTION

IMAGE forensics is a multidisciplinary science aiming at acquiring important information on the history of digital images, including the acquisition chain, the coding process, and the editing operators. The extraction of such data can be exploited for different purposes, one of the most interesting is the verification of the trustworthiness of digital data. Image forensic techniques work on the assumption that digital forgeries, although visually imperceptible, alter the underlying statistics of an image. These statistical properties can be interpreted as *digital fingerprints* characterizing the image life-cycle, during its acquisition and any successive processing. One of the tasks of image forensics is then to verify the presence or the absence of such digital fingerprints, similar to intrinsic watermarks, in order to uncover traces of tampering. As a first basic application of the above principle, the presence/absence of forensic fingerprints can be verified on the whole image (or a given suspected region, as a sort of sub-image), thus providing information about the authenticity of the entire image (or the entire region). However, a more sophisticated result would be a sort of map indicating for each image pixel (or small image block) its trustworthiness: in this case no manual choice of suspected regions would be necessary. Currently, several fingerprints have been studied for acquiring information on an image at a global level, but only few examples of tools that provide a fine-grained localization of forgery within a digital image have been proposed, in particular for double JPEG compression artifacts detection. In many cases a sufficiently large portion of the image (e.g., a block, with) is needed for a reliable statistical analysis of the chosen feature, so even if the image is processed block-wise only a coarse grained localization of tampering is possible. In this paper, we focus our attention on the fine grained forgery localization problem, assuming to have no information on the position of possibly manipulated pixels. Among the numerous fingerprints considered in image forensic literature, we consider the traces left by the *interpolation* process.

Image interpolation is the process of estimating values at new pixel locations by using known values at neighboring locations. During the image life cycle, there are two main phases in which interpolation is applied:

• Acquisition processing, to obtain the 3 color channels (red, green, and blue). The light is filtered by the *Color Filter Array* (CFA) before reaching the sensor (CCD or CMOS), so that for each pixel only one particular color is gathered. Thus, starting from a single layer containing a mosaic of red, green, and blue pixels, the missing pixel values for the three color layers are obtained by applying the interpolation process, also referred to as *demosaicking*.

• Geometric transformations, to obtain a transformed image. When scaling (shrinking and zooming), rotation, translation, shearing, are applied to an image, pixels within the to-be-transformed image are relocated to a new lattice, and new intensity values have to be assigned to such positions by means of interpolation of the known values, also referred to as *resampling* operation. The artifacts left in the image by the interpolation process can be analyzed to reveal image forgery. Ideally, an image coming from a digital camera, in the absence of any successive processing, will show demosaicking artifacts on every group of pixels corresponding to a CFA element. On the contrary, demosaicking inconsistencies between different parts of the image, as well as resampling artifacts in all or part of the analyzed image, will put image integrity in doubt. Our effort is focused on the study of demosaicking artifacts at a local level: by means of a local analysis of such traces we aim at localizing image forgeries whenever the presence of CFA interpolation is not present. Obviously our approach is based on the hypothesis that unmodified images coming from a digital camera are characterized by the presence of CFA demo-saicking artifacts. Starting from such an assumption, we propose a new feature that measures the presence/absence of these artifacts even at the smallest 2x2 block level, thus providing as final output a forgery map indicating with fine localization the probability of the

image to be manipulated. The paper is organized as follows. In Section II, we will provide a brief overview of previous works considering the fingerprints left by the CFA and the interpolation process, highlighting if and how the localization problem is taken into account by the methods proposed so far. In Section III we will present a statistical model for describing the presence of CFA, and starting from it we will propose the new forgery localization algorithm and describe the overall system in Section IV. In Section V, firstly the proposed model will be validated through a set of experiments, and secondly the detection capability of the proposed forgery localization algorithm will be investigated.

II. RELATED WORK

Previous works considering CFA demosaicking as the to be analyzed fingerprint can be divided in two main classes, i) algorithms aiming at estimating the parameters of the color interpolation algorithm, and ii) algorithms aiming at evaluating the presence/absence of demosaicking traces. Whereas the second class focuses on forgery detection (inconsistencies in the CFA interpolation reveal the presence of forged regions), algorithms within the first class are mostly intended to classify different source cameras, though sometimes they can also be used to detect tampering. In [8] propose a method for camera identification by the estimation of the CFA pattern and interpolation kernel; while in [9] the same authors exploit the inconsistencies among the estimated demosaicking parameters as proof of tampering. Cao and Kot in [10] aim at estimating the demosaicking formulas, employing a partial second-order image derivative correlation model, in order to classify different demosaicking algorithms. In [11], Bayram *et al.* detect and classify traces of demosaicking by jointly analyzing features coming from two previous works (see [12] and [13] below), in order to identify the source camera model. In [14], Fan *et al.* propose a neural network framework for recognizing the demosaicking algorithms in raw CFA images, and use it for digital photo authentication. Regarding the detection of demosaicking traces, Popescu and Farid propose an approach for detecting the interpolation artifacts left on digital images by resampling [15] and demosaicking [12] processes. In their approach, the Expectation- Maximization algorithm is applied to estimate the interpolation kernel parameters, and a probability map is achieved that for each pixel provides its probability to be correlated to neighboring pixels. The presence of interpolated pixels results in the periodicity of the map that is clearly visible in the Fourier domain. Such an analysis can be applied to a given image region, however a minimum size is needed for assuring the accuracy of the results: authors tested their algorithms on 256 X256 and 512X512 sized areas. Gallagher in [13] observed that the variance of the second derivative of an interpolated signal is periodic: he thus looked for the periodicity in the second derivative of the overall image by analyzing its Fourier transform. Successively, for detecting traces of demosaicking, Gallagher and Chen proposed in [16] to apply Fourier analysis to the image after high pass filtering, for capturing the presence of periodicity in the variance of interpolated/ acquired coefficients. The procedure has been tested only up to 64X 64 image blocks, whereas a variation yielding a pixel-by-pixel tampering map is based on a 256-point discrete Fourier transform computed on a sliding window, thus lacking resolution. In [17] by Dirik and Memon, the sensor noise power of the analyzed image is taken into account: its change across the image (i.e., its difference value for interpolated and acquired pixels) is considered for demonstrating the presence of demosaicked pixels. In the above paper, a block based CFA detection was also proposed, however the features proposed therein have to be computed on 96X96 blocks, thus permitting only a coarse grained localization of tampering. Demosaicking can also be detected using methods which analyze generic resampling artifacts. In this area, Kirchner in [18], [19] consider an approach similar to [15], by observing that the actual prediction weights of the resampling filter are not necessary for revealing periodic artifacts, thus simplifying the analysis, however experimental results consider only 512X512 images. Mahdian and Saic in [20] consider the derivatives of the interpolated image and apply the method to suspected windows of size at least 64X64, while in [21] they adopt the spectral correlation function, but only considering 512 512 sized images. Finally, in [22] Vazquez-Padin *et al.* demonstrate that the interpolated image is an almost cyclostationary process, with a period depending on the resampling factor. However, the authors use image blocks of size 128X128 pixels for the analysis, which only permits a coarse forgery localization.

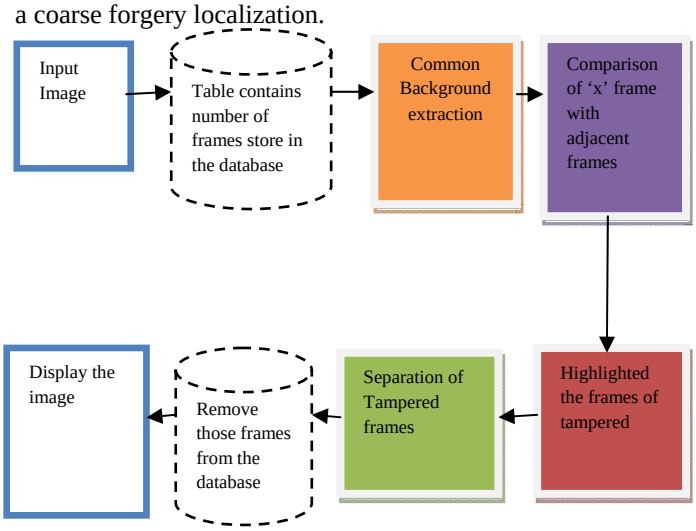


Figure. 1. The flow of the proposed algorithm

IV. PROPOSED ALGORITHM

In order to extend the previous analysis to the bidimensional case, without loss of generality we will consider as specific CFA the most frequently used Bayer's filter mosaic, a 2 2 array having red and green filters for one row and green and blue filters for the other (see Fig. 1(a)). Furthermore, we will consider only the green channel; since the green channel is upsampled by a factor 2, for a generic square block we have the same number of samples (and the same estimation reliability) for both classes of pixels (either acquired or interpolated). By focusing on the green channel, the even/odd positions (i.e.,

acquired/interpolated samples) of the one-dimensional case turn into the quincunx lattice for the acquired green values and the complementary quincunx lattice for the interpolated green values (see Fig. 1(b)). Similar to the one-dimensional case, we assume that in the presence of CFA interpolation the variance of the prediction error on lattice is higher than the variance of the prediction error on lattice, and in both cases it is content dependent. On the contrary, when no demosaicking has been applied, the variance of the prediction error assumes similar values on the two lattices. Hence, in order to detect the presence/absence of demosaicking artifacts, it is possible to evaluate the imbalance between the variance of the prediction error in the two different lattices.

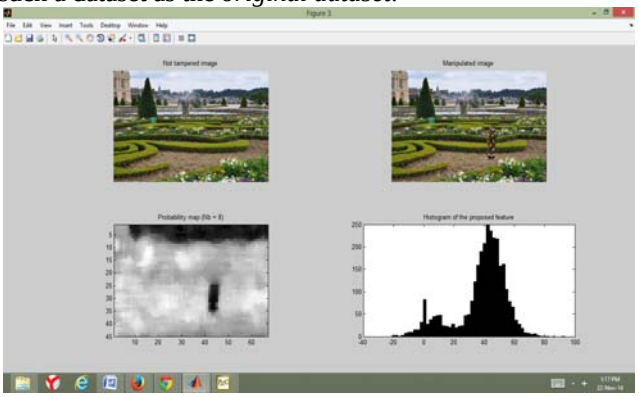
Overall System

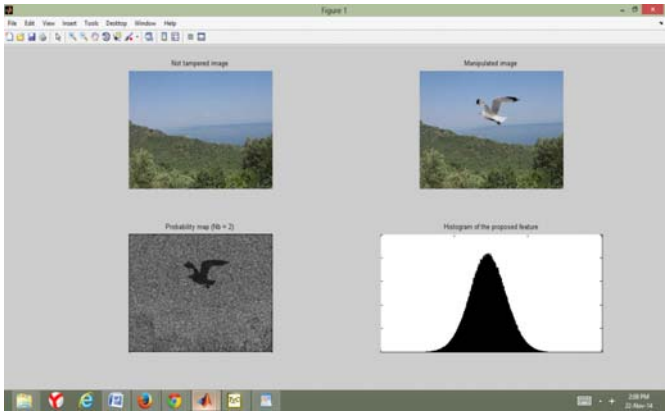
In Fig. we show the overall system that, given a suspected image, produces the corresponding forgery map: each pixel in the forgery map indicates for each image block its probability to contain CFA artifacts, so that low values in the output map correspond to likely forged areas.

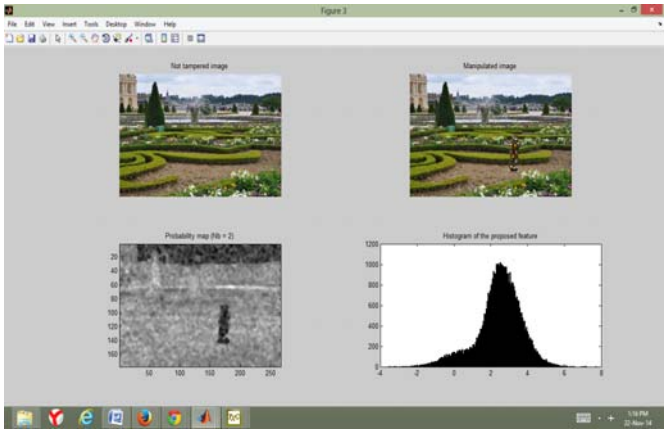
As a first step, the green channel is extracted from the image, and the prediction error is computed. Because in-camera processing algorithms are usually unknown, a fixed predictor is used: the choice of the adopted predictor will be discussed and validated in Section V. The weighted local variance is then estimated and the feature is obtained for each block. The GMMparameters are globally estimated exploiting the EM algorithm and used for the generation of the forgery map. When the forgery map is generated using the likelihood ratios in (17), whereas for we use the cumulated likelihood map in (18). Optionally, the intermediate log-likelihood map can be filtered using either a mean filter or a median filter.

V. EXPERIMENTAL RESULTS

The results presented in this section have been obtained on a dataset consisting of 400 original color images, in TIFF uncompressed format, coming from 4 different cameras (100 images for each camera): Canon EOS 450D, Nikon D50, Nikon D90, Nikon D7000. All cameras are equipped with a Bayer CFA, thus respecting our requirement that authentic images come from a camera leaving demosaicking traces, but the in-camera demosaicking algorithms of such devices are unknown. Each image was cropped to 512x512 pixels, maintaining the original Bayer pattern, which is assumed to be known3. We will refer to such a dataset as the *original dataset*.







VI. CONCLUSION

In this work, a forensic algorithm to localize forged regions in a digital image without any *a priori* knowledge about the location of the possibly tampered areas has been presented. Considering the CFA demosaicking artifacts as a digital fingerprint, we proposed a new feature measuring the presence of demosaicking artifacts even at the smallest 2 2 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. The validity of the proposed system has been demonstrated by computing the ROC curve of a forgery detector based on thresholding the probability map, considering different scenarios and different algorithm parameters, and comparing the performance with the approaches in [17] and [16]. The results show that by a proper parameter configuration CFA artifacts are usually reliably localized even at 8 8 block resolution.

Results are also confirmed by tests carried out on realistic forgeries. The fine-grained localization of tampered regions using CFA artifacts is the main contribution of this work, since in previous approaches either the area to be investigated has to be manually selected, or automatic block processing obtains poor detection performance when forced to reveal CFA artifacts at a fine-grained scale. The results show that the proposed algorithm can be a valid tool for detecting and localizing forgeries in images acquired by a digital camera. However, it should be remarked that the detection performance is strongly affected by JPEG compression, limiting the applicability to scenarios in

which the image under test is either uncompressed or compressed with high quality factors. Moreover, the present method may not be directly applicable to cameras using a super CCD [25].

REFERENCES

[1] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and finegrained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition 2009 – Elsevier*, pp. 2492–2501, 2009.

[2] T. Bianchi, A. D. Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in *Proc. ICASSP 2011*, Prague, Czech Republic, May 2011, pp. 2444–2447.

[3] T. Bianchi andA. Piva, "Analysis of non-aligned double JPEG artifacts for the localization of image forgeries," in *Proc. WIFS 2011*, Foz do Iguaçu, Brazil, Nov./Dec. 2011.

[4] W. Wang, J. Dong, and T. Tan, "Exploring DCT coefficient quantization effect for image tampering localization," in *Proc. WIFS 2011*, Foz do Iguaçu, Brazil, Nov./Dec. 2011.

[5] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.

[6] H. Farid, "Image forgery detection – A survey," *IEEE Signal Process. Mag.*, vol. 2, no. 26, pp. 16–25, Mar. 2009.

[7] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," *Multimedia Tools Applicat.*, vol. 51, no. 1, pp. 133–162, 2011.

[8] A. Swaminathan, M. Wu, and K. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Trans. Inf. Foresics Security*, vol. 2, no. 1, pp. 91–106, Mar. 2007.

[9]A.Swaminathan,M.Wu,andK.J.R.Liu,"Digitalimageforensicsvia intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[10] H. Cao and A. Kot, "Accurate detection of demosaicing regularity for digital image forensics," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 899–910, Dec. 2009.

[11] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models based on demosaicing artifacts," Digital Investigation, vol. 5, pp. 46–59, 2008.

[12] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp. 3948–3959, Oct. 2005.

[13] A. C. Gallagher, "Detection of linear and cubic interpolation in JPEG compressed images," in Proc. Canadian Conf. Computer and Robot Vision, 2005, vol. 0, pp. 65–72. [14] N. Fan, C. Jin, and Y. Huang, "A pixel-based digital photo authenti- cation framework via demosaicking inter-pixel correlation," in Proc. 11th ACM Multimedia and Security Workshop (MM&Sec '09), 2009, pp. 125–129.

[15] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Trans. Signal Process., vol. 53, no. 2, pt. 2, pp. 758–767, Feb. 2005.

[16]A.C.GallagherandT.Chen,"Imageauthenticationbydetectingtraces of demosaicing," in Proc. IEEE Computer Vision and Pattern Recognition Workshops (CVPRW 2008), 2008, pp. 1–8.

[17] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in Proc. 16th IEEE Int. Conf. on Image Processing (ICIP '09), 2009, pp. 1497–1500.

[18] M. Kirchner, "Fast and reliable resampling detection by spectral analysis of fixed linear prediction residue," in Proc. 10th ACM Multimedia and Security Workshop (MM&Sec '08), 2008, pp. 11–20.

[19] M. Kirchner and T. Gloe, "On resampling detection in re-compressed images," in Proc. First IEEE Int. Workshop on Information Forensics and Security, 2009, Dec. 2009, pp. 21–25.

[20]B.MahdianandS.Saic,"Blindauthenticationusingperiodicpropertiesofinterpolation,"IEEETrans.Inf.ForensicsSecurity,vol.3,no.3,pp. 529–538, Sep. 2008.

[21]B.MahdianandS.Saic,"Acyclostationarityanalysisappliedtoimageforensics,"inProc.2009 IEEEWorkshoponApplicationsofComputer Vision, Snowbird, UT, 2009, pp. 389–399. [22]D.VazquezPadin,C.Mosquera,andF.Perez-Gonzalez,"Two-dimensionalstatisticaltestforthepresenceofalmostcyclostationarityonim- ages,"inProc.17thIEEEInt.Conf.onImageProcessing(ICIP2010), Sep. 2010, pp. 1745–1748. [23] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm," J. Royal Statist. Society: Series B, vol. 39, pp. 1–38, 1977.

[24] S. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, pp. 674–693, Jul. 1989.

[25]T.Yamada,K.Ikeda,Y.G.Kim,H.Wakoh,T.Toma,T.Sakamoto,K.Ogawa,E.Okamoto,K.Masukane,K.Oda,andM.Inuiya,"AprogressivescanCCDimagesensorforDSCapplications,"IEEEJ.Solid-State Circuits, vol. 35, no. 12, pp. 2044–2054, Dec. 2011.