Catalogue of Digital Image Forgery Detection Techniques, an Overview

Archana V. Mire¹, Dr S. B. Dholk², Dr N. J. Mistry¹ and Dr P. D. Porey¹
¹ SVNIT, Surat, Gujarat, India
² VNIT, Nagpur, Maharashtra, India
archam2002@yahoo.co.in, sanjaydhok@gmail.com, njm@ced.svnit.ac.in, pdporey@svnit.ac.in

Abstract — Consistent decrease in cost of digital imaging hardware & increase in high quality user friendly image editing software for novice user has served variety of problems to society. Internet & social networking sites made it possible to host enormous no of images without provenance information or authenticity & made possible to share it with single click. Digital image forensics is a research area trying to resolve the imposed problem of authenticity assuming that different imaging devices or processing would introduce uniform inherent patterns which are consistent in the original clean images and would become inconsistent after image manipulations. These inconsistencies can be used as evidence for image source identification and forgery detection. In this paper we have discussed some state of art forgery detection techniques & an overview of the prior literature.

Index Terms — Resampling, splicing, CFA, JPEG

I. INTRODUCTION

Digital images when used as evidence in legal & scientific organizations may mislead judgment process if belongs to fake authenticity. Image forgery detection is an investigation area identifying authenticity of images before using them as evidence or engaging resources for further investigation. As shown in figure 1, typical digital camera consist of lens, sensors, color filter array (CFA) & Digital signal processor (DSP) unit [1]. Light passes through lens system goes through a set of CFA which allow passing only one color intensity to next layer of sensors. An image sensor is an array of rows and columns of photodiode elements, or pixels. When light strikes the pixel array, each pixel generates an analog signal proportional to the intensity of light, which is then converted to digital signal and processed by the DSP unit.

This stage wise image capturing process inherits consistent patterns in an image which become inconsistent after image forgery. In section2 we have discussed various fingerprints & techniques to retrieve & compare consistency within those fingerprints. In section 3 we have discussed application oriented comparison of these techniques.

II. FORGERY DETECTION TECHNIQUES

Digital images inherit variety of fingerprints such as chromatic aberration, biocoherence, Camera Response Function (CRF), JPEG quantization which can be checked for disturbances on tampering. Similarly tampering process also introduces certain uniformity within image which can be used to detect forgery. Various fingerprints which can be used to detect tampering are discussed below.

© Elsevier, 2013
A. Copy Move Detection

One of the most commonly investigated techniques is copy move detection technique in which some segment of an image is copied & pasted on other segments of the same image to conceal or duplicate objects. If two regions are known, we can compare them by using any standard measure of similarity. Fridrich[2] discussed and analyzed exact match technique which found to be computationally intractable. Further, robust block matching was suggested by them which is used as backbone in many copy move detection techniques. An image is divided into B×B size overlapping blocks. Each block is represented into space-invariant feature and arranged one below the other in lexicographically sorted order. The position of each block is noted into a separate matrix. For each matching block position (i1, i2), (j1, j2), the shift vector $s = (s_1, s_2) = (i1 - i2, j1 - j2)$ is calculated. For each shift vector corresponding frequency counter is maintained and incremented on each occurrence of the same shift vector. Positions of blocks having value above threshold gives copy moved blocks.

J. Fridrich[2] used robust representation in form of quantized DCT coefficients. B.L. Shivakumar[3] discussed several methods of copy move forgery detection in their survey paper. Kakar P. & Sudha N. used MPEG-7 image signature tool to expose post processed copy move forgery [4]. Bravo S. et al. proposed algorithm using colour-dependent feature vectors to reduce the number of comparisons in the search stage and 1-D descriptors [5]. Muhammad N. et al. used different types of wavelet for feature extraction in their different work. Vazquez-Padin D. et al. proposed technique which not only identifies the copy moved block within the image but also identifies which is the original & which is resampled one by using resampling occurred in the area. Computation cost of all these techniques are very high & human interpretation of the results is necessary.

B. Resampling Detection

Whenever two images are spliced together at least one image needs to be cropped, resized, or rescaled. Creation of more promising forgery depends on the smoothness of these resampling techniques. Various interpolation techniques such as bilinear interpolation, bicubic interpolation are keys for such resampling operations. Though these techniques improve the quality of forgery it also introduces correlations between neighboring pixels which can be traced to identify forgery.

Figure 2 shows bilinear interpolation in which kernel window (b) is moved on spike image (c) created from original image (a). Effective value is calculated at the centre of each kernel window which gives resampled image (d). On resultant image if we apply reverse kernel (e) we can see resultant periodicity in form alternate row & columns of zeros. Resampling detectors exploit these periodic artifacts, which can be found in the derivatives of a resampled signal.

![Fig. 1. Image capturing process](image-url)

![Fig. 2 Bilinear Interpolation](image-url)
Propescu & Farid [8] gave expectation maximization (EM) algorithm, iterative two-stage procedure estimating simultaneously both, the set a specific pixel most likely belongs to, and the unknown weights $\alpha$. First, the E-step uses the Bayes theorem to calculate the probability for each pixel belonging to set $M_1$.

$$\text{prob} (y_{i,j} \in M_1 | y_{i,j}) = \frac{\text{prob} (y_{i,j} \in M_1) \prod_{k=1}^{2} \text{prob} (y_{i,j} \in M_k)}{\sum_{k=1}^{2} \text{prob} (y_{i,j} \in M_k)}$$

In the E-step $\alpha$ is chosen randomly & in the M-step, vector $\alpha$ is updated using a weighted least squares estimator. The decision whether an image was resampled or not is made on the basis of regularity of spectral representation of probability map. B. Mahadian & Saic [9] discussed various approaches checking periodicity in resampled images. Also they proposed a method based on a derivative operator and radon transform detecting nearest neighbour, linear & cubic interpolation. In [10] Weimin Wei et al. proposed a DFT based method able to detect digitally zoomed images even after JPEG compression. Block transfer in JPEG inserts periodicity in image which may conflict with periodicity introduced by resampling & may result as identifying non resampled image as resampled image. Matthias Kirchner and Thomas Gloe [11] used these JPEG blocking artifacts to improve resampling detection. L. Nataraj et al. [12] added Gaussian noise to resized JPEG images to suppress periodicity introduced due to JPEG compression while maintaining periodicity introduced due to resampling & found that controlled noise addition works better than median filtering & weighted averaging. Feng et al. [13] examined the normalized energy density present in the second derivative of the image in the frequency domain and derived a 19-dimensional feature vector to train a SVM classifier.

C. Image splicing Detection

Image splicing means compositing new image from two different source images. Since portion of image is from two different sources they posses different properties inconsistent within block of images. These inconsistencies within an image can be used to identify splicing within an image. Most digital cameras employ a sensor to catch single intensity in conjunction with a CFA and then interpolate the missing color samples to obtain a three channel color image. First pattern of figure 3 shows arrangement of RGB filter above 3×3 sensor diode allowing single intensity to diode. As a result only one pixel color component get stored at each pixel location. Remaining color component at each pixel location are obtained by interpolating neighboring color components as shown in next three columns of figure 3 (Capital case indicate actual color intensity, lower case indicate interpolated sample).

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
<td>g</td>
<td>b</td>
</tr>
<tr>
<td>G</td>
<td>B</td>
<td>G</td>
<td>r</td>
<td>G</td>
<td>b</td>
</tr>
<tr>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
<td>g</td>
<td>b</td>
</tr>
</tbody>
</table>

Fig.3 CFA Interpolation

This interpolation introduces specific correlations within image which are likely to be destroyed on tampering. A. Popescu & H Farid [14] used expectation maximization algorithm to generate probability map of CFA interpolation. Ferrara P. et al [15] discussed various CFA interpolation techniques & proposed a feature measuring the presence of demosaicking artifacts even at the smallest 2 ×2 block level. They also generated probability map of consistent CFA artifacts. Li L. et al calculated posterior probability map of CFA interpolation with compression related guassian model to detect correlation patterns [16].
Chromatic aberration results from the failure of an optical system to perfectly focus light of different wavelengths. This shift results in various imperfections in the image. Aberration is calculated from image based on snail’s law. When image gets tampered aberration gets disturbed which can be used to detect splicing present in image. Johnson et al. [17] estimated global aberration from image assuming manipulated image block is of very small size & will not affect global estimation. Any block that deviates significantly from the global estimate is suspected as being manipulated. Chennamma, H. R & Rangrajan [18] assumed that because of aberration straight lines in 3D will appear as distorted broken line in the 2D image plane and used these lines to calculate aberration. The camera’s Charge Coupled Device (CCD) sensors interact with the lens and produce additional aberrations including the Purple Fringing Aberration (PFA) which appears in the form of a blue-purple halo near the edges of objects in the image. Yerushalmy, I. & Hel-Or [19] used this PFA which can be found along edges, especially where high contrast exists to identify the forgery. There is point wise non linearity in each sensor sensing the light intensity which arises due to imperfections in the silicon wafer used to manufacture the imaging sensor. This pixel to pixel variation of output signal is called as the Photo Response Non Uniformity (PRNU). Chierchia et al. [20] estimated Global PRNU & blocks deviating from this PRNU assumed to be spliced block within image.

Before recording image output on memory cards, cameras perform various linear, nonlinear, point-wise or spatial operations on the incoming light rays. All of which when combined yield visually pleasant images to human eyes. Camera Response Function (CRF) is the most salient point-wise operation which maps scene irradiance to image brightness nonlinearly. T.T. Ng et al [21] used CRF to detect splicing within images. If image is captured from a scene consisting of moving object then boundary of objects gets blurred this is called motion blur. Magnitude & direction of blur depends on direction & movement of object in motion. Pravin kakar et al [22] discussed previous research work for estimating motion blur. Also they proposed a technique using inconsistency within magnitude & direction of motion blur to identify the forgery within image. They used a variant of the widely recognized cepstral method in order to estimate motion blur. Instead of employing the cepstrum directly they used the spectral characteristics of the image gradients making it more robust to noise. For the case of uniform motion blur, blurring process is modeled as the convolution of a sharp image with a blurring kernel. Fang & Wang [23] proposed edge based method checking consistency of color distribution in the neighborhood of edge pixels. For a given image they classified edges into different categories and extracted shadow-shading-specular invariant edges as the candidate of splicing boundaries. They used inconsistency of color distribution among different edge pixel neighborhood to localize the splicing boundary. Li H. & Zeng [24] showed that the edge width will increase after the artificial blur operation which can be utilized to detect forged area. More discussion on camera based properties can be found in bibliographic survey by B. Mahadian & Saic [25].

D. Geometry based detection

Since light is an inseparable factor of an image there are several techniques dealing with fake or manipulated images based on light source direction, light intensity, reflection or shadow geometry. When image is forged it is often difficult to keep the appearance of the image’s correct perspective. This methodology is derived from basic rules of three-dimensional geometry, planar reflection, and linear perspective projection. Micah K. Johnson and Hany Farid [26] proposed three techniques for estimating the transformation of a plane imaged under perspective projection. Using this transformation, a planar surface can be rectified to be frontoparallel, providing a useful forensic tool. Wei Zhang et al [27] described a technique for detecting image composites by analyzing two-view geometrical constrains. A very important advantage of this approach is that it is hard to conceal the traces of inconsistencies in projective geometry. Difficulties for automation create one of the main drawbacks of this approach. Projection of camera centre onto image plane is called as principal point. In authentic images the principal point is near the centre of the image. When a person or object is translated in the image principal point is moved proportionally. Differences in the estimated principal point across the image can therefore be used as evidence of tampering. Johnson et al. [28] estimated camera’s principal point from the eye of person present in the image & showed how translation in the image plane is equivalent to a shift of the principal point. Hu. J et al [29] used information in the scene such as is parallels, orthogonality or the known angles, circles and their centers to calculate principal point as objects of these shapes are common in our daily life. If light is coming from point source, direction of shadow must be the same for all objects in an image. Criminisi I [30], W. Zhang et al [27] used shadow geometry to identify forgery. Liu Q Cao [31] proposed a framework for detecting tampered digital images based on photometric consistency of illumination in shadows. They formulated color characteristics of shadows measured by the shadow matte value.
Reflections are observed in a scene when light leaving some object bounces off a specular surface and subsequently enters the aperture of the observing imaging device. For smooth planar reflectors the angle between the incoming direction and the surface normal is the same as that between the normal and the outgoing direction & they should define a common reflection vanishing point and are coplanar. For a given planar reflecting surface, the set of lines connecting points on objects to the corresponding points on their reflections will all appear as if they were rays in the three dimensional scene that are perpendicular to the surface and therefore mutually parallel. O’Brien, J.F. & Farid[32] suggested model for identifying principal point, centre of projections, vanishing points from reflections.

E. JPEG Format based detection

JPEG format based detection techniques use the anomalies created in the image by 8×8 block processing operation of JPEG compression which become more prominent in boundary of block & easily visible in expanded images. If two images are used to create a forgery, it is likely that both have different levels of compression. Visibility of inconsistency increases with difference in image quality. If tampering involved only changing an area’s brightness and shadow levels JPEG technique may fail. In general JPEG Algorithm checks for differences in blocking artifacts along boundary of 8×8 block. For each 8×8 block difference \( R(i,j) = |A− B − C + D| \) is calculated. Where A,B,C,D are adjacent corner pixels present in different four adjacent 8×8 blocks. Difference of \( R(i,j) \) at each 8×8 block position at vertical direction & horizontal direction are compared with threshold to give difference in quality of jpeg images combined together. JPEG tampered image may inherit the characteristics of quantization tables from different sources and thus may result in inconsistencies. Histogram of DCT coefficients concentrate only on multiples of quantization steps and the power spectrum of DCT coefficients can be analyzed for quantization table estimation to detect block inconsistency. Markov model, probability mass function (PMF)[33] can be used for quantization table estimation from image which can be compared with quantization table from JPEG header. Binachi T. & Piva[34] discussed research work using JPEG compression artifacts for forgery detection. They proposed a forensic algorithm to discriminate between original and forged regions in JPEG images under the hypothesis that the tampered image presents a double JPEG compression, either aligned (A-DJPG) or nonaligned (NADJPG). Their approach doesn’t require manual selection of suspected region & automatically computes a likelihood map indicating the probability for each 8×8 discrete cosine transform block of being doubly compressed. Chen Y.-L. et al [35] discussed a method for detection of recompression of JPEG Images via Periodicity Analysis of Compression artifacts.

III. CONCLUSION

From the above discussion it is clear that one need to apply specific type of forgery detection technique to detect specific type of forgery. Weighted results of all possible forgery detection techniques should be combined to take any decision. Also with all of the techniques presented, close human interpretation is needed and there appears to be no single straight path in terms of a detection scheme. Various methods available in the image processing toolkit will need to be applied to this area with results closely scrutinized. Performance of different forgery detection techniques in various domains are explained in table 1.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Merits</th>
<th>Demerits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robust Copy-Move Forgery</td>
<td>Automation possible. Good for minor variations due to additve noise and lossy compression.</td>
<td>Computationally expensive &amp; can detect only duplicated region.</td>
</tr>
<tr>
<td>Resampling detection</td>
<td>Able to detect large classes of forgery since resampling is default while forgery.</td>
<td>May not work in compressed images as correlation created due to compression may affect resampling detection process.</td>
</tr>
<tr>
<td>Splicing Detection</td>
<td>Works for both synthetic and real images.</td>
<td>Won’t work for large size forgery as fingerprint is calculated from the image itself.</td>
</tr>
<tr>
<td>Geometrical inconsistency</td>
<td>Works equally for JPEG compressed images.</td>
<td>Dependent on existence of objects enabling estimation of light. Results need to verify with other method.</td>
</tr>
<tr>
<td>Format Based</td>
<td>Frequently used format</td>
<td>Results deteriorate for re-compressed forged images.</td>
</tr>
</tbody>
</table>
REFERENCES


