Camera Based Indicators for Image Forgery Detection

Ido Yerushalmy & Dr. Hagit Hel-Or
University of Haifa, Israel

The Problem:

Digital images can be easily forged using simple software. This reduces the reliability of digital images – leading to the necessity of image authentication.

The Goal:

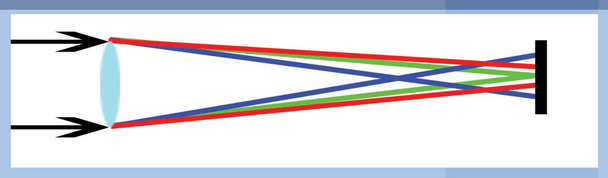
Detect forgery using no additional data except for the tested image.

Previous Solutions:

Watermarking: additional information is encoded into the image.

Statistics: Use only the image itself. Extract feature vectors to distinguish forged from real images.

Lateral Chromatic Aberration (LCA): red, green and blue wavelengths are not focused by the lens at the same point in the image plane.



Purple Blooming Aberration (PBA): the camera's CCD sensor interacts with the lens and produces additional aberrations including the PBA, which appears as a blue-purple halo near the edges of objects in the image.

LCA Based Solution:

In the study presented in [7], the extraction-contraction characteristic of the LCA is assumed. A brute force algorithm is used to determine the scaling origin and scaling factor between the color channels.

Image regions inconsistent with the globally estimated parameters are suspected as forgery.

Paper Contributions:

1- Use only the tested image itself. No added data such as in watermarking.

2- Forgery signs are inherent, making the method robust.

3- Not limited only to LCA.

4- In copy-move forgeries, can distinguish between the original patch and its copies.

Solution Proposed In This Paper:

One of the most important characteristics of the PBA is that the purple-blue halo is directional (it appears on the distal side of bright objects) relative to the image center . We exploit this characteristic to locate the image center.

PBA detection:

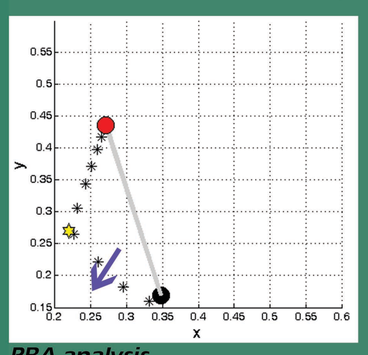
Detection of PBA is based on the assumption that in digital images the transition area between two colored regions should contain a mixture of both colors with a possible change in luminosity. This becomes visibly clear in the *xyY* color space. In the case of PBA this assumption is violated, since a blue-purple hue is added to the edge.

Center location calculation based on PBA:

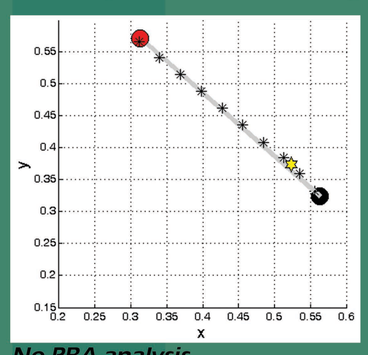
Let (x_i,y_i) be the spatial coordinates of the i-th detected PBA point and let (x_0,y_0) be the image center to be determined. The point (x_i,y_i) is associated with a line normal to the edge and passing through the point. The process finds the point (x_0,y_0) which minimizes the squared distance to all the lines (normalized by the PBA strength, S_i , and the reliability factor, R_i) :

$$\sum \frac{(a_j x_0+b_j y_0+c_j)^2}{(1-S_j R_j)^2} + P_j(x_0,y_0)$$

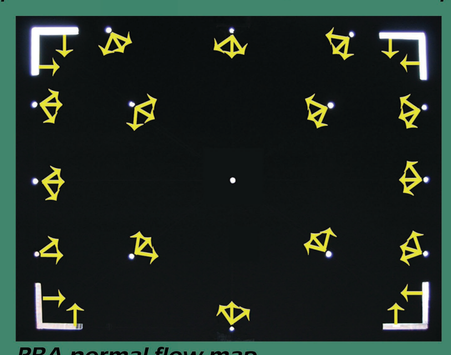
(P_i is a penalty factor given to center locations that are inconsistent with the PBA direction)



PBA analysis



No PBA analysis



PBA normal flow map

Algorithm:

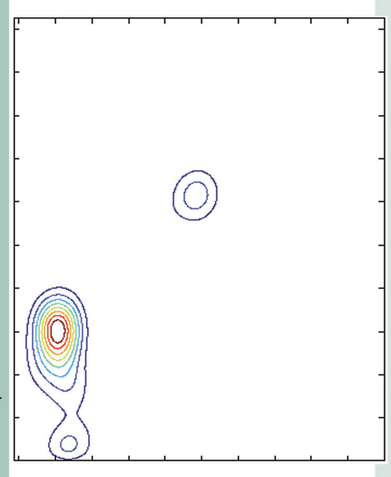
1- Identify edges with PBA and assign a reliability measure according to aberration strength, edge contrast and distance from the geometric center of the image.

2- Determine PBA direction in each region.

3- From the collection of PBA directions calculate the center of the image.

4- Find regions inconsistent with the geometric center and mark them as suspected to be forged.

An intensity map describing the level of inconsistency with the geometric center. High levels indicate a forged region.



Results:

An analysis of the algorithm's error rate over a set of 45 JPEG compressed images, using various cameras, shows a significant improvement compared to [7], mainly due to its generic nature.

Insertion detection:

Top image- original

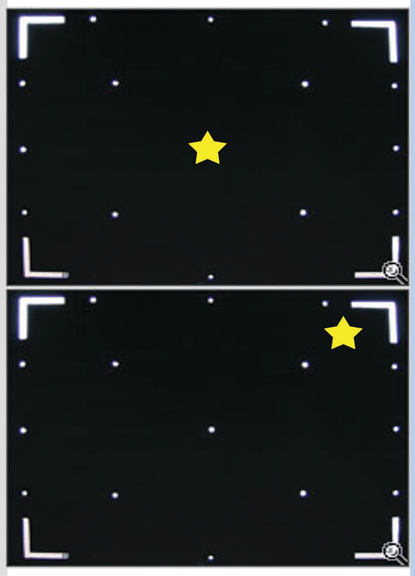
Crop detection:

Top image- original

Image center detected at a distance from the image's geometrical center, accompanied by a consistent "normal flow" map, may indicate that the image has been cropped.

A comparative example

Top- our result, Bottom- result of [7]



References:
[1] A.C. Popescu and H. Farid, Exposing Digital Forgeries in Color Filter Array Interpolated Images, IEEE Transactions on Signal Processing, vol. 53(10), pp. 3948–3959, 2005.
[2] DpReview website, http://www.dpreview.com/reviews/canondigitalixus330/page11.asp.
[3] J. Fridrich, D. Soukal, and J. Lukáš, Detection of Copy-Move Forgery in Digital Images, Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003.
[4] J. Lukas and M. Goljan, Detecting Digital Image Forgeries Using Sensor Pattern Noise, Proc. of SPIE Electronic Imaging, Photonics West, January 2006.
[5] Kingslake Rudolf, Optics in Photography, SPIE Optical Engineering Press,1992.
[6] M. Kutter, J. D. Frederic and F. Bossen, Digital watermarking of color images using amplitude modulation, J. Electronic Imaging 7(02), 326-332, Eds, April 1998.
[7] M.K. Johnson and H. Farid, Exposing Digital Forgeries Through Chromatic Aberration, ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.
Databases, Jan 1998.
[8] S. Lyu and H. Farid, How Realistic is Photorealistic?, IEEE Trans. Signal Processing, 53(2):845–850, Feb 2005.