ISSN: 2321-7782 (Online)

Volume 2, Issue 10, October 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Literature study on Image forgery

Sanawer Alam[1]
Asst. Prof. ,(EIC)
AIET
Lucknow, U.P – India

Deepti Ojha[2]
Student M.Tech,(EIC)
AIET
Lucknow, U.P – India

Abstract: In early 90's era, it was almost impossible to manipulate digital media, but now with the advancement in the technologies it is not a tough task. The growing demand of digital photography has explored new work in the field of image forensic. Reasons to use the digital image are many; like digital camera that produce immediate images, along with the flexibility to the person for deciding to select the appropriate one without waiting for the development of the film. Also digital images can be stored easily. While considering the originality of the digital image, it is quite difficult for the researcher to decide the authenticity of the image. Due to easy manipulation on digital image along with challenges to detect the original one, a new field of image forensic has attracted many researchers. In this paper, we are exploring different techniques to detect the authenticity of an image.

Keywords: Blocking artifacts, Digital forensics, Forgery, JPEG compression.

I. INTRODUCTION

Image forensic is a field in which the authenticity of an image can be verified along with the traces of image tampering can be detected without the knowledge of any pre-embedded or pre-extracted information. Due to the popularity of this field among researchers and numerous published papers in recent years has put considerable need for a complete paper to consolidate the work till now. The present paper puts altogether the existing methods in the field of image forgery. Two major techniques for authentication are Digital watermarking and signature [1]. However, most images captured today actually do not contain any digital watermark or signature. Therefore, it is required to passively check the integrity of digital image.

Basically there are two approaches to check the manipulation in an image:

a) In the first approach, the objective is to detect traces of specific manipulation, for which some common methods are resampling [2], copy paste [3, 4], and color filter array interpolation [5].

b) The second approach is based on the statistics of natural image [6], inconsistencies based on scene lighting direction [7], or camera response normality [8].

Although these approaches are effective in some aspects, still for practical applications new approaches are desirable. In spite of many advantages, there are some limitations of these techniques. The most important one is that they do not guarantee that new techniques may be designed which can be used to hide the traces of image manipulations.

II. IMAGE FORENSIC TOOLS

Tools used for the forgery can be broadly classified into five categories which are as follows:

a) Pixel-based techniques used to detect statistical deviation which has been introduced at the pixel level.

b) Format-based techniques used to analyze the statistical correlations produced during lossy compression.

c) Camera-based techniques used to detect those artifacts which may occur by the sensor, camera lens or on-chip post processing.

d) Physics based techniques used to detect the deviations in the three-dimensional interaction between light, camera and the physical objects.

e) Geometric-based techniques based on the actual measurement and position of the object in the real world and their relative position with respect to camera.

A) Pixel –Based Techniques

It is well known that legally many forensic tools are available such as forensic identification (Deoxyribonucleic acid (DNA) or fingerprint), forensic odontology (teeth), forensic entomology (insects), and forensic geology (soil).

As in the forensic sciences, the main focus is on the all manner of physical evidence. Similarly in the digital domain, the emphasis is on the pixel which is the basic building block of a digital image. In the upcoming sections some pixel based techniques have been discussed, which analyzes directly or indirectly pixel-level correlations that may be introduced during tampering.

1) Cloning (copy and paste): Cloning is the most common method for manipulation in which specific part of the image of a person or some object can be hidden. If the cloning operation is performed carefully then it is difficult to detect it visually. If the cloned image is compared with the original one then it is hardly possible to find out the cloned regions that may be of any shape and location.

Two computationally efficient algorithms have been developed to detect cloned image regions ([9], [10] ; see also [11], [12], and [13]).The authors in [9] has used block discrete cosine transform (DCT), further duplicated regions are detected by lexicographically sorting the DCT block coefficients and grouping similar blocks with the same spatial offset in the image. In a related approach, the authors in [10] apply a principal component analysis (PCA) on small fixed size image blocks to yield a reduced-dimension representation.

To make cloning detection robust with respect to minor changes and lossy compression along with reduction in computational complexity, DCT and PCA representations are employed.

2) Resampling: Sometimes it is required to perform some changes like resizing, rotating, stretching any portion of an image to produce a proper composite image. For example, if we are having an image of two persons with different heights, then to match the relative heights one person have to be resized. In such process, there is a need to introduce specific periodic correlations between neighboring pixels. This is known as resampling.

Since, these correlations are unlikely to occur naturally, their presence can be used to detect this specific manipulation ([14]; related approaches are described in [15], [16], [17], and [18]).

Let us consider a 1-D signal x (t) having length m to be up sampled by a factor of two, to generate a new signal y (t). Such as for odd samples,

$$y(2i-1)= x(i) \qquad (1)$$

and for even samples,

$$y(2i)= 0.5x(i)+0.5x(i+1). \qquad (2)$$

Where i=1,…, m.

It can be seen that the interpolated pixels can be represented in terms of the resampled samples, as resampled signal contains each sample of original signal.

$$y(2i)=0.5y(2i-1)+0.5y(2i+1). \qquad (3)$$

That is, each even sample of the resampled signal, is the linear combination of its adjacent two neighbors.

By this simple example, we can see that a resampled signal can be easily detected just by observing its neighbors, as they are having a correlation with each other. Similar periodic correlations can be seen for a range of resample signals. By knowing the criteria of resampling correlations one can easily determine the pixels correlations and vice versa.

Unfortunately neither pixel nor resample signal correlations are known generally. The algorithm used to solve such problem is known as expectation/maximization (EM) algorithm, which is a two-step (expectation, maximization) iterative algorithm:

a) The probability of each pixel being correlated with its neighbor is estimated in the expectation step; and

b) The specific form of the correlation between pixels is estimated in the maximization step.

3) Splicing: In a general form of photographic manipulation two or more images are digitally spliced into a single composite. It is visually imperceptible to distinguish the border between the spliced regions when it performed carefully. In [19] and [20], however, the authors show that splicing disrupts higher-order Fourier statistics, which can be subsequently used to detect splicing.

Considering a 1-D signal x(t) and its Fourier transform X(ω). To analyze the frequency composition, the power spectrum

$$P(\omega)=X(\omega)X^*(\omega) \qquad (4)$$

is routinely used. Here (*) denotes complex conjugate. On moving beyond the power spectrum, the bispectrum

$$B(\omega 1, \omega 2) = X(\omega 1)X(\omega 2)X^*(\omega 1+\omega 2) \qquad (5)$$

Measures higher-order correlations between triples of frequencies ω1, ω2, and ω1+ω2. Subtle discontinuities that result from splicing manifest themselves with an increase in the magnitude of the bi-spectrum and in a bias in the bi-spectrum phase, which are used to detect splicing in audio [19] and in images [20].

4) Statistical: The authors in [21], [22], and [23] exploit statistical regularities in natural images to detect various types of image manipulation. The authors in [21] compute first- and higher-order statistics from wavelet decomposition. This decomposition splits the frequency space into multiple scale and orientation subbands. For each wavelet subband, first four statistical moments are calculated, and the correlations between the various subbands are used to determine higher-order statistics. In a complementary approach, the authors in [22] construct a statistical model based on local co-occurrence statistics from image bit-planes. Specifically, in both cases, the statistical model is used to detect everything from basic image manipulations such as resizing and filtering [21] to discriminate photographic from computer-generated images [24] and detecting hidden messages (steganography) [25].

B) Format Based Techniques

In any forensic analysis “preserve the evidence” is the first rule. Lossy image compression like JPEG can be treated as the worst enemy for a forensic analyst. In this regard, lossy compression properties can be exploited for forensic analysis. Here, three forensic techniques have been discussed, that detect tampering in JPEG compressed image.

1) JPEG Quantization: Images are obtained in the JPEG format by most of the cameras. Different manufacturers have different requirement according to which they balance the compression and quality of the image. As described in [26] and [27], this difference can be used to identify the source (camera make/model) of an image.

It has been observed that within each JPEG image, a distinct signature is embedded. The quantization tables can be extracted from the encoded JPEG image or blindly estimated from the image, as described in [28].

According to the quality setting, the quantization tables can vary even within a single camera. Although the tables are different, still there are some similarities across cameras of different models. By the simple observation the researchers can verify the source of an image.

2) Double JPEG: First step for any digital manipulation is that an image must be saved in photo-editing software. Since JPEG is the most popular format for image compression, so both images (original and manipulated) must be in the same format. Assuming that the image was not cropped before second compression, the resultant manipulated image will have double compression with specific artifacts which were not present in the original one. By detecting these artifacts, manipulated image can be identified.

3) JPEG Blocking: A JPEG compression is always performed via DCT, which introduces blocking artifacts. These artifacts appear at the border of neighboring blocks in the form of horizontal and vertical edges. So whenever manipulation is performed, these artifacts may be disturbed.

In [29], the authors characterize the blocking artifacts using pixel value differences within and across block boundaries. It has been found that these differences are more prominent at the edges as compare to within the block. So, while cropping and recompressing an image, a new set of blocking artifacts may be introduced, this will not necessarily match with the original boundaries. A histogram of these differences can be computed from all non overlapping image blocks within and across block pixel. Now by proper supervision of these patterns, the researchers can easily discriminate between authentic and inauthentic images.

C) Camera Based Techniques

The artifacts introduced at different stages of image processing, can be analyzed by different image forensic techniques. Since these artifacts may have some irregularities in manipulated image, they can be utilized as an evidence of tampering. Some techniques for detecting different camera artifacts have been discussed here.

1) Chromatic Aberration: In an ideal imaging system, light passes through the lens and is focused to a single point on the sensor. But practically Optical systems (like camera) fail to perfectly focus light of all wavelengths.Specially, in case of chromatic aberration where light of different wavelengths reaches the sensor there is spatial shift in the locations.

In [30], the authors show that this lateral aberration can be approximated as an expansion or contraction of the color channels with respect to one another. As shown in Fig 1(b), the local lateral aberration in the tampered region is inconsistent with the global aberration. The authors of [30] describe how to estimate lateral chromatic aberration in order to detect this type of manipulation. Since the refractive index of glass depends on the wavelength of the light that passes through it, which results in splitting of polychromatic light according to wavelength as it exits the lens and strikes the sensor.

Fig 1(c) shows the splitting of short wavelength light (solid green ray) and long wavelength light (dashed red ray). It is clear that there is misalignment between the color channels due to aberration, from which model parameters are estimated by maximizing the alignment of the color channels.

Finally tampering can be detected by comparing the local chromatic aberration with estimated global aberration.

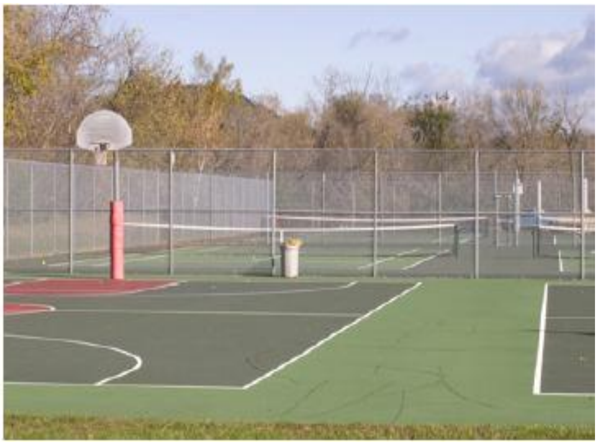

Fig 1(a): Original image

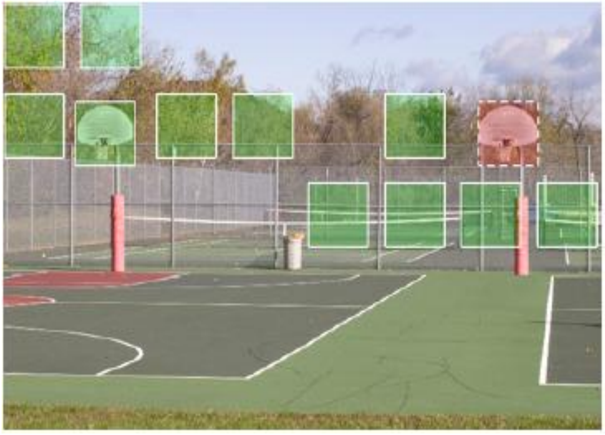

Fig 1(b): Manipulated image

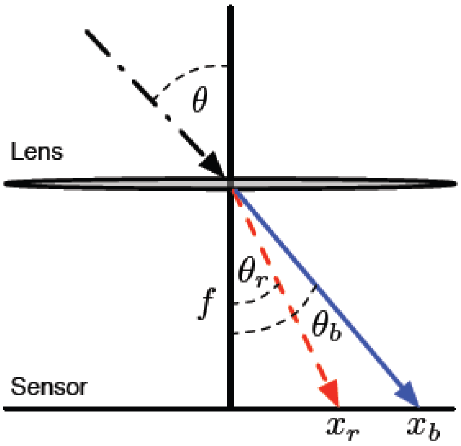

Fig 1(c): Chromatic Aberration

2) Camera Response: Since digital camera sensors are almost linear in nature, there should be a linear relationship between the amount of light measured by each sensor element and the corresponding final pixel value [31]. But during the enhancement of final image, a point wise nonlinearity is introduced. The authors in [32] describe how to estimate this mapping, termed as response function, from a single image. Further tampering can be detected by calculating the differences in the response function.

3) Sensor Noise: During processing, a digital image undergoes through various steps, like quantization, white balancing, demosaicking, color correction, gamma correction, filtering and, usually, JPEG compression. These steps introduce a unique signature into the image, which can be used to estimate the authentication of an image.

D) Physics Based Techniques

Let us consider the creation of a tampered image having two celebrities, rumored to be romantically involved, walking down in a rainy day. To create such type of image, splicing of individual images can be done. In this process, matching of lighting effects (under which each person was originally photographed) of both images cannot be done perfectly. Such differences across an image in lighting can be used as evidence of tampering.

E) Geometric-Based Techniques

1) Metric Measurements: Consider an image of a license plate as shown in Fig 2(a) which is largely illegible. After transformation, as shown in Fig 2(c), license plate number is clearly visible. For such process, several tools are available in projective geometry which can perform rectification of planar surfaces along with real-world measurements under certain conditions. Some of them are discussed here. In the first method, polygons of known shapes (e.g., street sign, license plate, lettering on a billboard) are used for transformation.

Second approach requires knowledge of boundary conditions on a plane for example, a pair of known angles on the plane.

In the third approach two or more coplanar circles are used (e.g., car wheels).

Note that in each case, there is requirement of only single image. Thus by using these techniques world-to-image transformation can be estimated, thereby allowing metric measurements to authenticate the image.

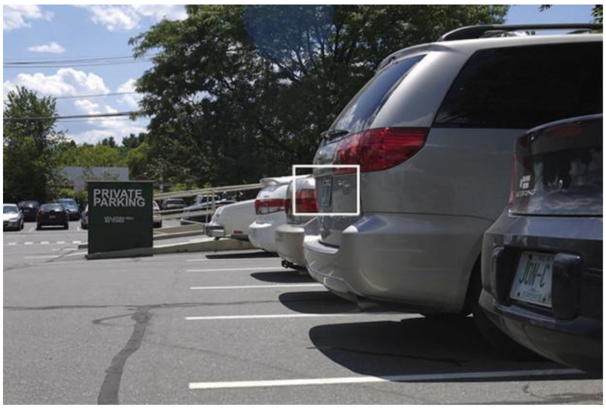

Fig 2(a): Original image

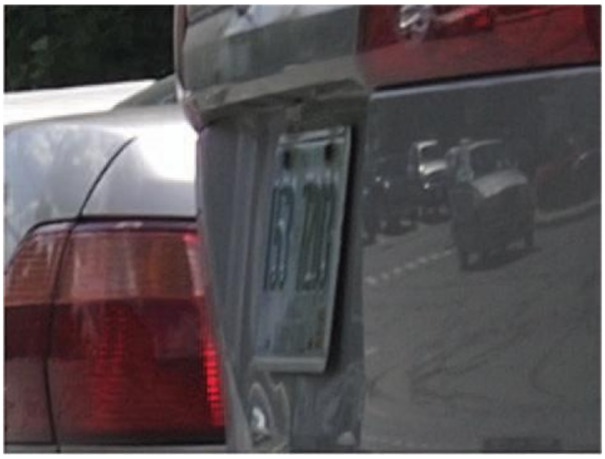

Fig 2(b): Closer view of license plate

.

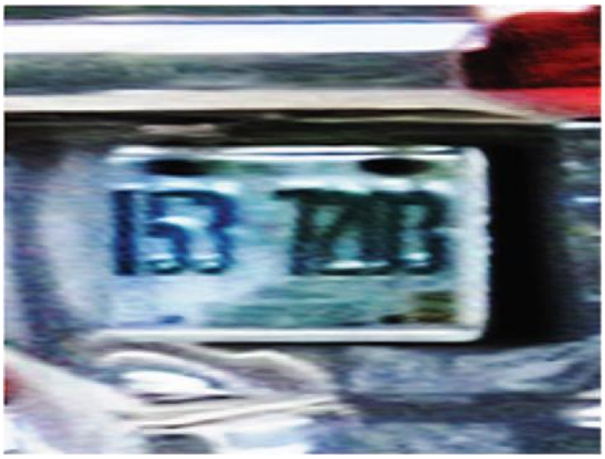

Fig 2(c): A visible license no. after planar rectification

***2) Principal Point*:** The projection of the camera center onto the image plane is known as the principal point, which is near the center of the image if it is authentic. If the tampering is performed with respect to any person or object, the principal point is deviated. This deviation can be used as an evidence of tampering. In [33], the authors described how to estimate a camera's principal point by the help of the image of a pair of eyes (i.e., two circles) or other planar geometric shapes. It is clear from fig 3, that if there is a translation in the image, there is a shift in the principal point. This deviation can be used as an evidence of tampering.

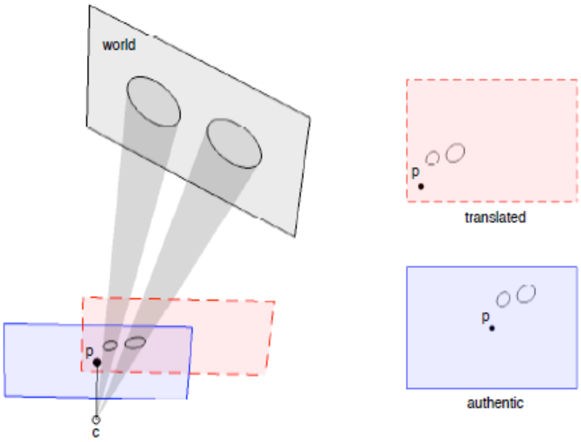

Fig.3 Left: Projection of two eyes (circles) from a world plane (black solid line) onto an image plane (original-blue solid line, translated-red dashed line) with c (camera center) and p (principal point).
Right: Deviation in principal point in the translated image with respect to authentic image.

III. Performance Measures

To evaluate the robustness and efficiency of the forgery techniques, there are two parameters namely, Precision and Recall rates, which will determine the number of correctly detected tampered parts in an image.

A) Precision Rate

It is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false positive. Those regions of the image which are really not tampered but detected as tampered by the algorithm are called false positive.

Mathematically,

$$\text{Precision Rate} = \frac{\text{Correctly detected part} \quad {*}100}{\text{Correctly detected parts} + \text{False Positives}} \qquad (6)$$

B) Recall Rate

It is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false negative. Those regions of the image which are really tampered, but not detected by the algorithm, are called false negative.

Mathematically,

$$\text{Recall Rate} = \frac{\text{Correctly detected parts} \quad *100}{\text{Correctly detected parts + False Negative}} \qquad (7)$$

IV. Conclusion

Manipulation of digital media was almost impossible hardly 20 years ago, which is quite common now a day. Moreover, future's technology will definitely allow tampering digital media in an unimaginable way. Although, very efficient techniques are available to detect tampering, even then the number of tampering is also increasing. Undoubtedly, processing information can be finding out by using these techniques for a manipulated image, but the fact is that an expert can do undetectable manipulations in the image. All these demand for a new technique in the forensic as well as in the anti forensic field. As discussed before, many of these techniques are based on extracting earlier processing history; there is a possibility to generate an undetectable forgery compression. So the future work should be focused on the development of new techniques which can detect such type of tampering. As with the virus/antivirus and spam/antispam game there is competitive fight between forger and forensic analyst. However, forensic analyst will continue to make it more time-consuming and harder (but never impossible) to create a forgery that cannot be detected.

References

1. Shuiming Ye, Qibin Sun, and Ee-Chien Chang "Detecting digital image forgeries by measuring inconsistencies of blocking artifacts", ICME 2007.
2. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling",IEEE Transactions on Signal Processing, vol. 53,no. 2, pp.758-767, 2005.
3. F. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", Digital Forensic Research Workshop, Cleveland, USA,Aug. 2003.
4. T. Ng, S.F. Chang, and Q. Sun, "Blind Detection of Photomontage using Higher Order Statistics", IEEE International Symposium on Circuits and Systems, Canada, May 2004.
5. A.C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images",IEEE Transactions on Signal Processing, vol. 53,no. 10, pp. 3948-3959, 2005.
6. S. Lyu and H. Farid, "How Realistic is Photorealistic?". IEEE Transaction on Signal Processing, vol. 53, no. 2, pp.845-850, Feb. 2005.
7. M.K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", ACM Multimedia and Security Workshop, New York, NY, 2005.
8. Z. Lin, R. Wang, X. Tang, and H.-Y. Shum,"Detecting Doctored Images Using Camera Response Normality and Consistency", IEEE Conference on Computer Vision and Pattern Recognition, pp.1087-1092, 2005.
9. J. Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003.
10. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep.TR2004-515, 2004.
11. G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in IEEE Int.Conf. Multimedia and Expo, Beijing, China, 2007, pp. 1750–1753.
12. W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital images," in Proc. Int. Conf. on Pattern Recognition, Washington, D.C., 2006, pp. 746–749.
13. B. Mahdian and S. Saic, "Detection of copy move forgery using a method based on blur movement invariants," Forensic Sci. Int., vol. 171, pp. 180–189, 2007.
14. A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.
15. A.C. Gallagher, "Detection of linear and cubic interpolation in jpeg compressed images," in Proc. 2nd Canadian Conf. Computer and Robot Vision., Victoria, British Columbia, Canada, vol. 171, 2005, pp. 65–72.
16. M. Kirchner, "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue," in ACM Multimedia and Security Workshop, 2008, pp. 11–20.

17. B. Mahdian and S. Saic, “Blind authentication using periodic properties of interpolation,” IEEE Trans. Inform. Forensics Security, vol. 3, no. 3, pp. 529–538, 2008.

18. S. Prasad and K. R. Ramakrishnan, “On resampling detection and its application to image tampering,” in Proc. IEEE Int. Conf. Multimedia and Exposition, Toronto, Canada, 2006, pp. 1325–1328.

19. H. Farid, “Detecting digital forgeries using bispectral analysis,” AI Lab, Massachusetts Institute of Technology, Tech. Rep. AIM-1657, 1999.

20. T.-T. Ng and S.-F. Chang, “A model for image splicing,” in Proc. IEEE Int.Conf. Image Processing, Singapore, 2004, vol. 2, pp. 1169–1172.

21. H. Farid and S. Lyu, “Higher-order wavelet statistics and their application to digital forensics,” in Proc. IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), Madison, WI, 2003.

22. S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation detection with binary similarity measures,” in Proc. European Signal Processing Conf., Turkey, 2005.

23. S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” IEEE Trans. Inform. Forensics Security, vol. 1, no. 1, pp. 111–119, 2006.

24. H. Farid, “Digital image ballistics from JPEG quantization,” Dept. Comput.Sci., Dartmouth College, Tech. Rep. TR2006-583, 2006.

25. H. Farid, “Digital ballistics from jpeg quantization: A followup study,” Dept. Comp. Sci., Dartmouth College, Tech. Rep. TR2008-638, 2008.

26. Z. Fan and R. L. de Queiroz, “Identification of bitmap compression history: JPEG detection and quantizer estimation,” IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, 2003.

27. W. Luo, Z. Qu, J. Huang, and G. Qiu, “A novel method for detecting cropped and recompressed image block,” in Proc. IEEE Conf. Acoustics, Speech and Signal Processing, Honolulu, HI, 2007, pp. 217–220.

28. M. K. Johnson and H. Farid, “Exposing digital forgeries through chromatic aberration,” in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland,2006, pp. 48–55.

29. Hany Farid, “Image Forgery Detection [A survey]”, IEEE SIGNAL PROCESSING MAGAZINE, MARCH 2009 ,pp.16-25.

30. Z. Lin, R. Wang, X. Tang, and H-V Shum, “Detecting doctored images using camera response normality and consistency,” in Proc. Computer Vision and Pattern Recognition, San Diego, CA, 2005.

31. M. K. Johnson and H. Farid, “Detecting photographic composites of people”’, in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.