A SURVEY ON DIGITAL CAMERA IMAGE FORENSIC METHODS

Tran Van Lanh [a], Kai-Sen Chong [b], Sabu Emmanuel [b], Mohan S Kankanhalli [c]
[a] Department of Computer Science, Uppsala University, Sweden
[b] School of Computer Engineering, Nanyang Technological University, Singapore
[c] School of Computing, National University of Singapore, Singapore
latr0465@student.uu.se, {Y030028, asemmanuel}@ntu.edu.sg, mohan@comp.nus.edu.sg

ABSTRACT

There are two main interests in Digital Camera Image Forensics, namely source identification and forgery detection. In this paper, we first briefly provide an introduction to the major processing stages inside a digital camera and then review several methods for source digital camera identification and forgery detection. Existing methods for source identification explore the various processing stages inside a digital camera to derive the clues for distinguishing the source cameras while forgery detection checks for inconsistencies in image quality or for presence of certain characteristics as evidence of tampering.

1. INTRODUCTION

Multimedia Forensics has become important in the last few years. There are two main interests, namely source identification and forgery detection. Source identification focuses on identifying the source digital devices (cameras, mobile phones, camcorders, etc) using the media produced by them, while forgery detection attempts to discover evidence of tampering by assessing the authenticity of the digital media (audio clips, video clips, images, etc). In this paper, we review several techniques in digital camera image forensics, i.e. in source camera identification and in forgery detection. Source camera identification methods explore different processing stages of the digital camera for unique characteristics and exploit the presence of lens radial distortion [1], sensor imperfections [2], [3], color filter array (CFA) interpolation [4], [5], [6], and inherent image features [7], etc. Image forgery includes splicing of images to construct a new concocted image, applying region duplication/swapping to hide/relocate certain objects in the image and applying image editing to remove/add new objects from/into the image. For forgery detection, some of the methods inspect the image for inconsistencies in chromatic aberration [11], lighting [12], and camera response function (CRF) [13] as signs of forgery. Others try to detect certain modes of manipulation using JPEG quantization tables [10], bicoherence [14], and robust matching [15].

In section 2, we give an overview of the structure and processing stages of a typical digital camera. In sections 3 and 4, several methods for source digital camera identification and forgery detection are presented respectively and section 5 concludes the paper.

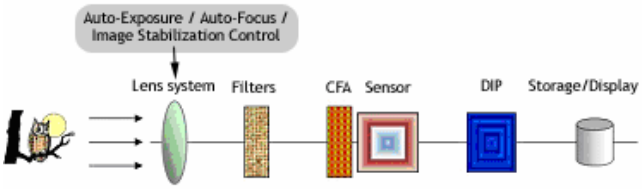

Figure 1. Elements of a typical digital camera

2. INSIDE A DIGITAL CAMERA

The general structure of a digital camera is shown in Figure 1. Digital cameras consist of lens system, filters, color filter array (CFA), image sensor, and digital image processor (DIP) [9]. Color images may suffer from aberrations caused by the lenses, such as chromatic aberration and spherical aberration. Chromatic aberration is the failure to converge different wavelengths at the same position on the sensor, while spherical aberration causes light passing through the periphery of the spherical lens to converge at a point closer to the lens than light passing through the lens center. In the lens systems, these effects can be minimized using special combinations of convex and concave lenses, as well as using aspheric lenses. The lens system also includes the auto-exposure control, auto-focus control and the image stabilization unit. Auto-exposure changes the aperture and the shutter speed along with a carefully calibrated automatic gain controller to capture well-exposed images. Auto-focus runs a miniature motor that focuses the lenses by moving the lenses in and out until the sharpest possible image of the subject is obtained. Image stabilization helps to give sharper pictures by counteracting camera shake.

After passing through the lenses, light goes through a set of filters. An infrared filter is an absorptive or reflective filter allowing only the visible part of the spectrum to pass, while blocking infrared radiation that can decrease the sharpness of the formed image. An anti-aliasing filter reduces aliasing, a phenomenon that happens when the spacing between pixels in the sensor cannot support the finer spatial frequency of the target objects such as decorative patterns.

At the heart of a digital camera is the image sensor. 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 DIP. Most digital cameras use a charge-coupled device (CCD) as the image sensor although CMOS chips are a popular alternative. Sensor pixels are not sensitive to colors; they just record the brightness of light, thus producing a monochromatic output. To produce a color image, a color filter array (CFA) is used in front of the sensor so that each pixel records the light intensity for a single color only. Most digital cameras use the Green-Red-Green-Blue (GRGB) Bayer pattern CFA. The output from the sensor with a Bayer filter is a mosaic of red, green and blue pixels of different intensities. Since each pixel record only one of the three colors, the full color image is accomplished by the DIP using various interpolation (demosaicking) algorithms. Other alternative CFA filters include the Cyan-Yellow-Green-Magenta (CYGM) pattern, the Red-Green-Blue-Emerald (RGBE) pattern, and the Cyan-Magenta-Yellow (CMY) pattern. Besides interpolation, the DIP also performs further processing such as white balancing, noise

reduction, matrix manipulation, image sharpening, aperture correction, and gamma correction to produce a good quality image.

3. SOURCE DIGITAL CAMERA IDENTIFICATION

3.1. Using Lens Aberration

Choi et al [1] propose the lens radial distortion as a fingerprint to identify source camera. Radial distortion causes straight lines to appear as curved lines on the output images and it occurs when the transverse magnification M_T (ratio of the image distance to the object distance) is not a constant but a function of the off-axis image distance r. The authors argue that different manufacturers employ different lens system design to compensate for radial distortion and that the lens focal length affects the degree of radial distortion. Thus, each camera model will express a unique radial distortion pattern that helps to identify it. Two experiments were performed on 3 different camera models obtaining average classification accuracies of 91.53% and 91.39% respectively.

Although this method is not tested for two cameras of the same model, based on the authors' arguments on radial distortion differences, we can expect a low accuracy. Additionally, this method will fail to measure radial distortion if there is no straight line in the image since the distortion is measured using the straight line method. Lastly, the authors assume that the centre of distortion is the centre of image, which may not be the case. If this is taken into account, a higher accuracy may be possible.

3.2. Using Sensor Imperfections

Pixel Defects: Geradts et al [2] examine the defects of CCD pixels and use them to match target images to source digital camera. Pixel defects include point defects, hot point defects, dead pixel, pixel traps, and cluster defects. To find the defect pixels, a couple of images with black background are taken by each of the 12 cameras tested and compared to count the common defect points that appear as white. The result shows that each camera has distinct pattern of defect pixels. However, it is also shown that the number of visible defect pixels for the same camera differs between the images and depends very much on the content of the image. It is also shown that the number of defect pixels visible on images of the same content taken by the same camera at different temperatures is different. Furthermore, for cameras with high-end CCD, the authors cannot find any visible defect pixel, which means that not all cameras necessarily have pixel defects. In addition, most cameras have built-in mechanisms to compensate for the defective pixels. Therefore, the method cannot be directly applied for all digital cameras.

Sensor Pattern Noise: A reliable method for identifying source camera based on sensor pattern noise is proposed by Lukas et al in [3]. The pixel non-uniformity (PNU), where different pixels have different light sensitivities due to imperfections in sensor manufacturing processes, is a major source of pattern noise. This makes PNU a natural feature for uniquely identifying sensors.

The authors study 9 camera models where 2 of them have similar CCD and 2 are exactly the same model. The camera identification is 100% accurate even for cameras of the same model. The result is also good for identifying compressed images. One problem with the conducted experiments is that the authors use the same image set to calculate both the camera reference pattern and the correlations for the images. We have run several experiments with this model for cropped images. It turns out that the model fails to predict the source camera of cropped images. In addition, for the model to work, the size of the images used for computing the camera reference pattern should be the same as the size of the test image.

3.3. Using CFA Interpolation

Traces of Color Interpolation in Color Bands: Bayram et al [4] explore the CFA interpolation process to determine the correlation structure present in each color band which can be used for image classification. The main assumption is that the interpolation algorithm and the design of the CFA filter pattern of each manufacturer (or even each camera model) are somewhat different from others, which will result in distinguishable correlation structures in the captured images. Using the iterative Expectation Maximization (EM) algorithm, 2 sets of features are obtained for classification: the interpolation coefficients from the images and the peak location and magnitudes in the frequency spectrum of the probability maps.

When using a 5x5 interpolation kernel, the classification accuracy is 95.71% for two different cameras but it drops to 83.33% when three cameras are compared. A larger set of cameras should have been used to determine its effect on the classification accuracy. No experiment is run for cameras of the same model but we expect the method to fail because cameras of the same model normally share the same CFA filter pattern and interpolation algorithm. In addition, the authors have pointed out that this method does not work well for compressed images.

Quadratic Pixel Correlation Model: Long and Huang [5] obtain a coefficient matrix from a quadratic pixel correlation model where spatially periodic inter-pixel correlation follows a quadratic form. Four cameras together with cartoon pictures are used for the experiments, which obtain 95% accuracy for one camera, 98% for another camera and 100% accuracy each for the remaining two cameras. The authors also test with modified images (compressing, adding Gaussian noise, gamma correction, smoothing). When compressed with quality 80, the accuracy drops to as low as 80%. Accuracy for images with other modifications is even lower.

Since cameras of the same or similar model would use the same demosaicking algorithm, we expect that the model will not correctly differentiate cameras of the same model. Furthermore, as shown by the experiments, the model performs poorly for modified images. Other than that, the model gives a very good performance.

Binary Similarity Measures: Celiktutan et al [6] use a set of binary similarity measures for identifying source cell-phone. The underlying assumption is that proprietary CFA interpolation algorithm leaves correlations across adjacent bit-planes of an image that can be represented by these measures. Binary similarity measures are metrics used to measure the similarity between binary images, i.e. between the bit-planes of an image. 108 binary similarity measures are obtained, and like [7], a set of 10 Image Quality Metrics is used as additional features for classification.

The highest average accuracy for classifying 3 groups of cameras is 98.7%, while the lowest average accuracy is 81.3%. When classifying 9 cameras, only 62.3% of the classification is correct. The results show that this method is dependent on the target cameras and the number of cameras used. Only the Red channel is considered in this paper, thus for a better result, the correlations within Blue and Green channels and across the channels may give a better result.

3.4. Using Image Features

Kharrazi et al [7] identify a set of image features that can be used to uniquely classify a camera model. The 34 proposed features are categorized into 3 groups: Color Features, Image Quality Metrics, and Wavelet Domain Statistics. Features are extracted from images of two cameras, which are then used to train and test the classifier. The result is as high as 98.73% for uncompressed images and 93.42% for JPEG images compressed with a quality factor of 75. The accuracy rate drops to 88% when five cameras are used.

Tsai et al [8] also has a similar study for this method using different camera sets. The reported accuracy rate for cameras with similar or closely related CCD is low (67.48%). Hence, this method does not work well for cameras with similar CCD and is unsuitable for identifying source cameras of the same model. Furthermore, it requires all cameras to take images of the same content and resolution, which is not easy in practice.

4. IMAGE FORGERY DETECTION

4.1. Using JPEG Quantization Tables

Digital cameras generally use JPEG compression to encode images and different manufacturers typically configure their devices with different compression levels and parameters. Farid [10] exploits this difference by extracting the JPEG quantization table from an image and comparing it against a database of known digital cameras for source identification. Likewise, it can be compared against a database of photo-editing software for signs of tampering.

Out of 204 digital cameras used for the experiments, 62 cameras had unique quantization table while the remaining tables fall into equivalence classes ranging from 2 to 28 in size. Using 5 different versions of Adobe Photoshop, an image (presumably uncompressed) is saved at each of the 13 compression levels for each version and it was found that the JPEG quantization tables used were different from those of the 204 cameras. Thus, by detecting the presence of JPEG quantization tables unique to any particular photo-editing software, it can be determined if the image is authentic or was previously tampered with and saved using a photo-editing software. Often, the image output from the camera is already compressed in JPEG format and if edited using editing software, there will exist a double JPEG compression problem, which Popescu et al look at in another paper [21].

4.2. Using Chromatic Aberration

Johnson et al [11] check for the inconsistency of lateral chromatic aberration across an image as a sign of tampering. The authors model lateral chromatic aberration as the expansion or contraction of a color channel with respect to one another, which results in a misalignment of the color channels. Model parameters are sought to bring the color channels back into alignment and a metric based on mutual information is used to quantify the alignment. The error between the local and global model parameters is quantified by computing the average angular error between the displacement vectors at every pixel. If the average angular error exceeds a certain threshold, it is likely that aberration has been inconsistent across the image due to forgery.

From experiments, the average angular error is 14.8° with around 98.0% of the errors below 60°. For forensic purposes, the image is tested in blocks and if the block's local estimate differs from the global estimate by more than 60°, it is considered to be inconsistent with the global estimate and indicates signs of tampering. One apparent weakness is that it is difficult to estimate chromatic aberration from a block with little or no spatial frequency content, such as a largely uniform patch of sky. Therefore, if the manipulated regions of the image consist of content with little spatial frequency (e.g. concealment of features in the sky), it is unlikely to be detected by the algorithm.

4.3. Using Lighting

Johnson et al [12] propose a technique of detecting inconsistencies in the direction of the illuminating light source for each object or person in an image using a 2-D model, which builds upon the work by Nillius et al [16]. Three different situations – infinite, local and multiple light sources – are tested to determine the error in the estimated light source direction relative to the actual direction. The errors are typically below 2° except for the infinite light source case where the estimated light direction of an object with non-constant reflectance yielded an error of 10.9°. When tested on sample images, the algorithm is successful in detecting contradicting light source directions. While this technique should work well for outdoor scenes where the Sun is often the only light source, indoor scenes with multiple light sources would make analysis complicated due to multiple occluding boundaries.

4.4. Using Camera Response Function (CRF)

Hsu et al [13], [22] propose a method of detecting image splicing using geometry invariants and camera response function (CRF). This idea is similar to the work by Lin et al [17] that detects for splicing by observing for abnormality in the camera response functions (CRF). The suspected splicing boundary is first manually identified. The geometry invariants from the pixels within each region on either side of this boundary are computed and used to estimate the CRF. The CRFs from each region are then checked for consistency with each other using cross-fitting techniques. If the data from one region fits well to the CRF from another region, this image is likely to be authentic, and spliced if otherwise. Finally, the cross-fitting errors from each region are represented using a 6-dimensional vector and fed into a RBF SVM classifier to classify into authentic or spliced.

Only images in RAW or BMP format are tested and each spliced image is created in Adobe Photoshop using authentic images from 2 cameras with no post-processing to focus on the effects of splicing. The classification accuracy in 6 runs is 87.55% with the spliced image detection rate as high as 90.74%. However, the false acceptance rate (FAR) is also at least 15.58%. Even though the accuracy is reasonably high, only uncompressed images have been tested. Whether this technique would work well for JPEG compressed images remains unknown. Furthermore, spliced images created from original images taken by the same camera, or even the same model, are unlikely to be detected as forgery.

4.5. Using Bicoherence and Higher Order Statistics

Based on Farid's [19] earlier success in applying bicoherence features for human-speech splicing detection, Ng et al [14], [18] investigate the prospect of using bicoherence features to detect for the presence of abrupt discontinuities in an image, or the absence of optical low-pass property, as a sign of splicing. Besides using the original features that describe the mean of magnitude and phase entropy, the authors propose 2 new methods to augment the performance: (1) estimating the bicoherence features of the authentic counterpart, and (2) incorporating image features that capture the characteristics of different object interfaces.

Using SVM classification, the mean accuracy obtained is 71.48%. Although the initial results are promising, the accuracy of 71.48% is not very high and more effective features must be derived to model the sensitivity of bicoherence due to splicing.

4.6. Using Robust Matching

Fridrich et al [15] focus on the detection of a particular type of forgery, the copy-move attack, where a part of an image is cloned or duplicated elsewhere in the same image, usually to conceal an important feature. Popescu et al [20] have a similar approach.

For uncompressed images, matching is carried out between blocks of size *B*x*B* to detect for exact replicas. To extend this idea to images saved in lossy JPEG format, instead of directly matching the pixel representation of each *B*x*B* block, the authors use a robust representation consisting of quantized DCT coefficients.

Experiments on sample altered images have produced good results with the copied-and pasted areas successfully matched and identified. However, the authors also acknowledge that the algorithm might have falsely identified matching segments in flat, uniform areas, such as the sky. Thus, human interpretation is necessary to interpret the output of the algorithm.

5. CONCLUSION

Having examined several camera identification and forgery detection methods, we now can derive some interesting observations. It is observed that the identification methods based on intrinsic features of camera hardware, such as the lens and CCD sensor, give more reliable and better results than those methods based on other camera software parts (e.g. CFA interpolation algorithms). It also seems that only the methods modeling the imperfections of camera hardware can distinguish cameras of the same model. From our observations, there are two promising approaches towards a more stable, accurate method for identifying source cameras. The first one is to utilize the sensor noise pattern in some way that can overcome the problem of cropped images. The second approach is to combine several kinds of lens distortions such as chromatic aberration, spherical aberration, radial distortion, etc.

On the other hand, methods for forgery detection have lower accuracy rates compared to camera identification methods. Out of the methods that check for inconsistencies across an image as a sign of tampering, it seems that the methods relying on hardware-dependent characteristics (e.g. aberration and CRF) are potentially more reliable than methods relying on scene content (e.g. lighting and image statistics). This is possibly due to the relative difficulty in applying the same hidden characteristics consistently to all the spliced components. With the exception of the method exploiting CRF inconsistency, the other discussed methods would generally be resilient against composite images created from images captured with multiple cameras or even cameras of the same model. There are also methods examining CFA interpolation for its consistency across an image [23] or for absence of induced correlation [24].

6. REFERENCES

[1] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration*", Proceedings of the SPIE 2006*.

[2] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, "Methods for Identification of Images Acquired with Digital Cameras", *Proc. of SPIE, Enabling Technologies for Law Enforcement and Security, vol. 4232,* February 2001.

[3] J. Lukas, J. Fridrich, and M. Goljan, "Digital Camera Identification from Sensor Pattern Noise", *IEEE Transactions on Information Forensics and Security*, June 2006.

[4] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Source Camera Identification Based on CFA Interpolation", *ICIP 2005*.

[5] Y. Long and Y. Huang, "Image Based Source Camera Identification using Demosaicking", *IEEE MMSP 2006*.

[6] O. Celiktutan, I. Avcibas, B. Sankur, and N. Memon, "Source cell -phone identification", *Proc. ADCOM*, 2005.

[7] M. Kharrazi, H.T. Sencar, and N. Memon, "Blind source camera identification", *ICIP*, 2004.

[8] M.-J. Tsai and G.-H. Wu, "USING Image Features to Identify Camera Sources", *ICASSP 2006*.

[9] J. Adams, K. Parulski, and K. Spaulding, "Color processing in digital cameras", *IEEE Micro, vol. 18, no. 6, pp. 20–31*, 1998.

[10] H. Farid, "Digital Image Ballistics from JPEG Quantization", Technical Report, TR2006-583, Dartmouth College, Computer Science, 2006.

[11] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration", In *ACM Multimedia and Security Workshop*, Geneva, Switzerland, 2006.

[12] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", In *ACM Multimedia and Security Workshop*, New York, NY, 2005

[13] Y.-F. Hsu and S.-F. Chang, "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency", In *ICME*, Toronto, Canada, July 2006.

[14] T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind Detection of Photomontage Using Higher Order Statistics", In *IEEE International Symposium on Circuits and Systems (ISCAS)*, Vancouver, Canada, May 2004.

[15] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", *Proc. of DFRWS 2003*.

[16] P. Nillius and J.-O. Eklundh, "Automatic estimation of the projected light source direction", *Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001.

[17] Z. Lin, R. Wang, X. Tang, and H.-Y. Shum, "Detecting doctored images using camera response normality and consistency," in *CVPR*, 2005, pp. 1087–1092.

[18] T.-T. Ng and S.-F. Chang, "Blind Detection of Digital Photomontage using Higher Order Statistics", *ADVENT Technical Report #201-2004-1 Columbia University*, June 2004.

[19] H. Farid, "Detecting Digital Forgeries Using Bispectral Analysis", *Technical Report*, AIM-1657, MIT AI Memo, 1999.

[20] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[21] A.C. Popescu and H. Farid, "Statistical tools for digital forensics", *International Workshop on Information Hiding*, 2004.

[22] T.-T. Ng, S.-F. Chang, C.-Y. Lin, and Q. Sun, "Passive-blind Image Forensics", In Multimedia Security Technologies for Digital Rights, W. Zeng, H. Yu, and C. –Y. Lin (eds.), Elsvier, 2006.

[23] A. Swaminathan, M. Wu, and K. J. R. Liu, "Component forensics of digital cameras: A non-intrusive approach", *Proc. Of Conference on Information Sciences and Systems, pp. 1194-1199*, Princeton, NJ, March 2006.

[24] A.C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images", *IEEE Trans. On Signal Processing, vol. 53, no. 10, part 2, pp. 3948-3959*, October 2005.