IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 1, Feb - March, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Survey On Passive-Blind Image Forensics

Vinita Devi, Vikas Tiwari
SIDDHI VINAYAK COLLEGE OF SCIENCE & HIGHER EDUCATION ALWAR, India

***Abstract*—Digital visual media represent nowadays one of the principal means for communication. And as the use of digital images has become more common throughout society, both the means and the incentive for creating digitally forged images is increasing. So, there is a great need for methods through which digital image alterations can be identified. For this different techniques are available such as digital watermarking by which an image can be authenticated but the drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature and are referred as passive-blind image forensics. In this paper first I provide introduction to the passive-blind image forensics after that passive-blind image forensics is defined in terms of forgery creation and forgery detection. Different forgery detection techniques are being reviewed which are broadly divided in two categories (1) Source device identification and (2) Image forgery detection. 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.**

Keywords: *Digital forensics; digital image forgery; tampering detection; passive-blind image forgery, source device identification*

1. INTRODUCTION

Images and videos have become the main information carriers in the digital era. The expressive potential of visual media and the ease in their acquisition, distribution and storage is such that they are more and more exploited to convey information. But digital images are easy to manipulate because of the availability of the powerful editing software and sophisticated digital cameras. Image processing experts can easily access and modify image content and therefore its meaning without leaving visually detectable traces. Moreover, with the spread of low-cost user friendly editing tools the art of tampering and counterfeiting visual content is no more restricted to experts. As a consequence, the modification of images for malicious purposes is now more common than ever.

At the beginning, the alternation is just enhance the image's performance, but then many people started to alter the image's content, even to gain their ends by these illegal and immorality methods. Based on the above reasons, it's valuable to develop a credible method to detect whether a digital image is tempered, so-called digital image forgery.

2. PASSIVE-BLIND IMAGE FORGERY DETECTION

There are two categories in image forgery: active image forgery and passive-blind image forgery. Active approaches could be further divided mainly into digital watermarks and signatures. The passive (blind) approach is regarded as the new direction. In contrast to active approaches, passive approaches do not need any explicit priori information about the image. Therefore, it does not require watermarks or signatures. There are two main approaches, namely source identification and forgery detection. Source identification focuses on identifying the source digital devices (cameras, mobile phones, camcorders, scanner, etc) to discover evidence of tampering by assessing the authenticity of the digital media by recovering information about their history. In this paper, I review several techniques in discovering different forgery detection methods.

3. IMAGE FORENSICS TOOLS

There are many different tools available for image forgery detection. In [12], Hany Farid describes the set of image forensic tools grouping them into five main categories :1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip postprocessing; 4) physically based techniques that explicitly model and detect anomalies in the three dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera.
Figure 1 is a typical example of image forgery[13].

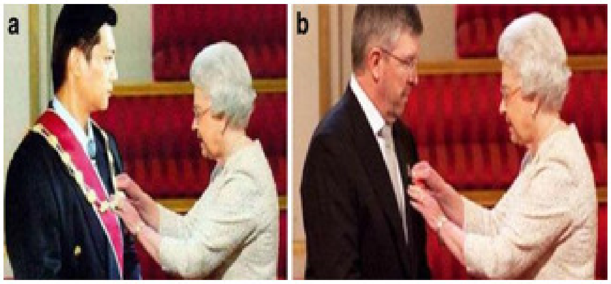

Fig. 1 The doctored image depicting Jeffrey Wong Su En while receiving the award from Queen Elizabeth II, published in Malaysian dailies(a), and the original picture of Ross Brawn receiving the Order of the British Empire from the Queen (b)

4. IMAGE FORENSICS

Image forensics can be divided into three stages: (A)Forgery creation, which includes manipulating an image

(B)Distribution channel which includes knowledge of different forgery creating techniques as well as various forgery detecting algorithms

(C)Forgery detection: At this stage forgery is detected

Figure 2 shows three stages of passive blind image forensics

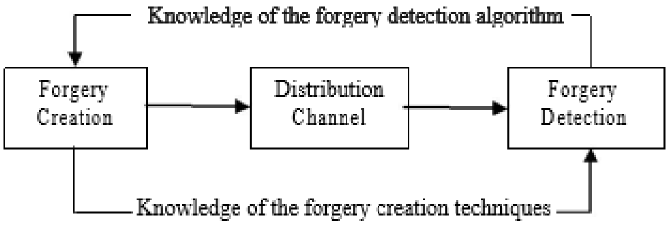
Knowledge of the forgery detection algorithm
Forgery Creation
Distribution Channel
Forgery Detection
Knowledge of the forgery creation techniques

Fig 2 Block Diagram for image forensics

4. (A) PROCESS OF IMAGE FORGERY

In general, the image forgery creation process involves different steps like selection, transformation, composition of the image portions, and retouching of the final image. This process often begins with extracting an object from an image. The forgery creators can then place the transformed image portion generated from the transformed 3D model into another image using different composition techniques. Finally, the composite image is retouched to remove the remaining artifact Process of image for image forgery creation can be explained using figure 3

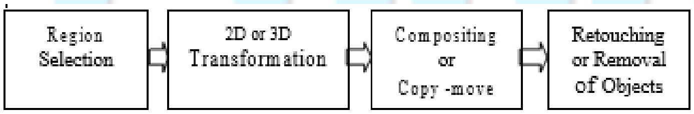

Fig.3 The process of image forgery creation

(B) PROCESS OF DETECTION OF IMAGE FORGERY

When a digital image is forged, we consider that a part of image's statistical characteristics has been changed.

There can be two conditions: (1) Forged area's statistical characteristics are different from the common characteristics of the natural image (2) Forged area's statistical characteristics are only different from the normal area. For detecting the former one, we can only compare the image's statistical characteristics with a natural image, and for the later one, we can calculate the statistical characteristics of every small pieces of the image, and then compare them, so that the forgery can be detected.

Figure 4 illustrates the process of the condition 1 and Figure 5 illustrates the process of the condition 2.

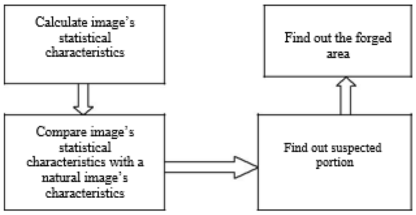
Calculate image's statistical characteristics
Compare image's statistical characteristics with a natural image's characteristics
Find out suspected portion
Find out the forged area

Fig 4 The process of detection of image forgery condition 1

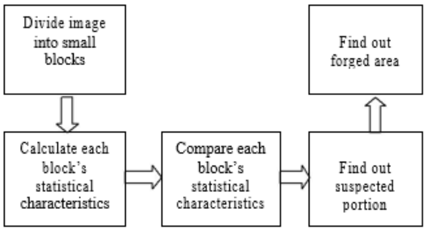
Divide image into small blocks
Calculate each block's statistical characteristics
Compare each block's statistical characteristics
Find out suspected portion
Find out forged area

Fig 5 The process of detection of image forgery condition 2.

5. TECHNIQUES OF PASSIVE FORENSICS

As defined in section II Image forensics has two main problems: (1) Image source device identification (2) Image forgery Detection.

5.1. IMAGE SOURCE DEVICE IDENTIFICATION

Figure 6 shows the typical image acquisition pipeline [13]. The Light enters the imaging device through a system of optical lenses, which conveys it towards the imaging sensor. The imaging sensor is the heart of every digital camera, and it is composed of an array of photo detectors, each corresponding to a pixel of the final image, which transform the incoming light intensity into a proportional voltage. Most cameras use CCD (Charged Coupled Device) sensors, but CMOS (Complementary Metal Oxide Semiconductor) imagers can also be found. To render color, before reaching the sensor the light is filtered by the Color Filter Array (CFA), a specific color mosaic that permits to each pixel to gather only one parti cular light wavelength (i.e. color).The CFA pattern arrangement depends on the manufacturer, although Bayer's filter mosaic is often preferred. As a result, the sensor output is a mosaic of e.g. red, green and blue pixels arranged on a single layer. To obtain the canonical 3-channels representation, the signal needs to be interpolated. Demosaicing algorithms are applied to this. Before the eventual storage, additional processing is performed, such as white balance, gamma correction, and image enhancement. Finally, the image is recorded in the memory device. Also in this case the format can vary, but a common choice is JPEG. The described image acquisition pipeline is common for most of the commercially available devices; nonetheless, each step is performed according to specific manufacturer choices, and hence might depend on the camera brand and model.

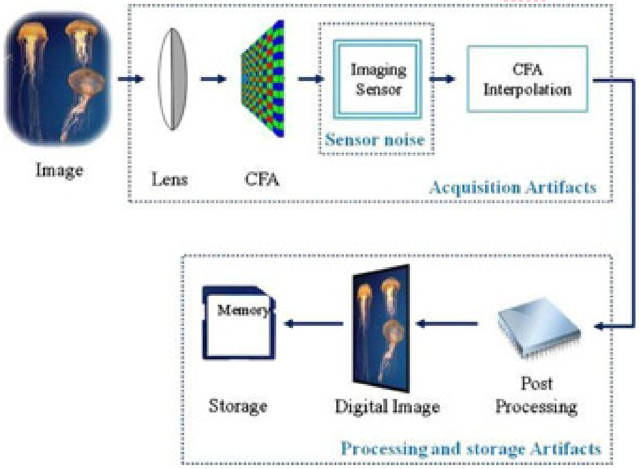

Fig 6 Standard digital image pipeline

This variation can be used to determine the type of camera from which a specific image was obtained. Indeed, each stage in the pipeline can introduce imperfections in the final image or characteristic traits: lens distortion, chromatic aberration, pixel defects or CCD sensor imperfections, statistical dependencies related to proprietary CFA interpolation algorithms and other a intrinsic image regularities which leave tell-tale footprints. These artifacts are statistically stable and can be considered as a signature of the camera type or even of the individual device.

5.1.1 IDENTIFICATION USING LENS ABERRATION

Due to each lens and image geometries and to the design of the camera, lenses produce distortions (aberrations) in the captured images. Radial distortion for example deforms the image so that straight lines in object space appear as curved lines. Choi et al. [1] propose to analyze this kind of lens aberration as a fingerprint to identify the 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 say that different manufacturers use different lens system design to compensate for radial distortion and that the lens focal length affects the degree of radial distortion. In this way, 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.

5.1.2 IDENTIFICATION USING SENSOR IMPERFECTION

Imaging sensors introduce various defects and create noise in the pixel values.

SENSOR NOISE

The sensor noise is defined as any noise component that survives frame averaging, which is an-other important characteristic of imaging sensors. The pattern noise [3] include two main components: the fixed pattern noise (FPN) and the photo-response non-uniformity noise (PRNU)

FPN is mainly caused by the dark current on a CCD chip. The dark current is due to thermal activity in the photocathode and the dynodes. And it is present whether the shutter is open or closed. However, the magnitudes of the dark current on a CCD are always nonuniformity as different pixels may have different generation rates of dark current. The millions of nonuniformity pixels are arranged regularly on each CCD, and therefore can create the unique pattern for each sensor**.**

The sensor noise is the result of three main components, i.e. pixel defects, fixed pattern noise (FPN), and Photo Response Non Uniformity (PRNU).

PIXEL DEFECTS

Pixel defects include point defects, hot point defects, dead pixels, pixel traps, and cluster defects, which reasonably vary across different sensors, independent on the specific camera model. Geradts et al [2] examine the defects of CCD pixels and use them to match target images to source digital camera.

The authors propose to determine pixel noise by taking images with black or green background with 12 different cameras and then comparing the defect points which appeared as white. Their experiments show that each camera has distinct patterns of defect pixels also across the same model; nonetheless, the impact of defect pixels closely depends on the content of the image. 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.

5.1.3 IDENTIFICATION USING IMAGE FEATURES

Kharrazi et al [4] identify a set of image features that can be used to uniquely characterize a camera model. Authors assume that the image can be affected by color processing and transformations done by the camera prior to the storage. The authors study statistical properties of the image organized into two groups: (1) color-related measurements, such as average pixel value, RGB pairs correlation, neighbor distribution center of mass, energy ratio and wavelet domains statistics, and (2) image quality features. Supported by a SVM(Support Vector Machine) classifier, this approach shows an effective result on low compressed images taken by different camera models. However, this technique can only be applied on images containing similar content.

5.1.4 IDENTIFICATION USING JPEG HEADERS

Digital cameras generally use JPEG compression to encode images and different manufacturers configure their devices with different compression levels and parameters. The specific quantization tables and Huffman codes which are needed to decode a JPEG file are embedded into the JPEG header.

The JPEG quantization table and Huffman codes along with other data extracted from the JPEG header can be used as a distinct camera signature which can be used for authentication. Farid et al [6] proposes that a camera signature can be extracted from a JPEG image consisting of information about quantization tables, Huffman codes, thumbnails, and EXIF format. They divide these parameters in three categories:

1) Image parameters 2) Thumbnail parameters 3) EXIF Metadata parameters.

IMAGE PARAMETERS

The first three components of their camera signature are the image dimensions, quantization table, and Huffman code. The image dimensions are used to distinguish between cameras with different sensor resolution. The image dimensions are specified as the minimum dimension follow[redacted] by the maximum dimension. The set of three 8 8 quantization tables are specified as a one dimensional array of 192 values: each channel's table is specified in column-order, and the three tables are specified in the order of luminance (Y), chrominance (Cb) and chrominance (Cr).

The Huffman code is specified as six sets of 15 values corresponding to the number of codes of length 1, 2 …. 15: each of three channels requires two codes, one for the DC co-efficients and one for the AC coefficients.

THUMBNAIL PARAMETERS

A thumbnail version of the full resolution image is often embedded in the JPEG header. The next three components of their camera signature are extracted from this thumbnail image. A thumbnail is created by cropping, filtering and down-sampling the full-resolution image. The thumbnail is then typically compressed and stored in the header as a JPEG image.

EXIF METADATA

The final component of authors' camera signature is extracted from an image's EXIF metadata. There are five main image file directories (IFDs) into which the metadata is organized:

(1) Primary; (2) EXIF; (3) Interoperability; (4) Thumbnail; and (5) GPS.

Thus authors extract 8 values from the metadata: 5 entry counts from the standard IFDs, 1 for the number of additional IFDs, 1 for the number of entries in these additional IFDs, and 1 for the number of parser error, that occurs when some camera manufacturers customize their metadata in ways that do not conform to the EXIF standard.

Thus authors extract 284 header values from the full resolution image, a similar 284 header values from the thumbnail image, and another 8 from the EXIF metadata, for a total of 576 values. These 576 values form the signature by which images will be authenticated.

They show that this signature is highly distinct across 1.3 million images spanning 773 different cameras and cell-phones. Specifically, 62% of images have a signature that is unique to a single camera, 80% of images have a signature that is shared by three or fewer cameras, and 99% of images have a signature that is unique to a single manufacturer.

5.2 IMAGE FOGERY DETECTION

5.2.1 REGION-DUPLICATION/SPLICED IMAGES DETECTION

One of the common image tampering is object removal, where the regions of unwanted objects in an image are replaced by other parts of the same image. This type of operation is called copy-move or region-duplication. Since there is similar information, e.g., texture, noise, and color inside the same image, it is hard to identify these forgeries via visual inspection. Furthermore, some postprocessing such as adding noise, blurring, lossy compression, may be performed on tampered images, which would make the task of detecting forgery significantly harder. Therefore the robustness against various post-processing operations is the main problem of the detection algorithm.

In [7], Fridrich, et al., analyzed the DCT coefficients for each block. They propose detection of copy-move forgery by block matching. The method divides an image into small blocks, extract the features for each block, and then identify possible duplicated regions by comparing their similarities They performs two matches:

1) Exact match 2) Robust match

Exact match uses an exact match for detection of forgery. Whereas robust match is based on an approximate match.

5.2.2 FORGERY DETECTION USING STATISTICAL INTRINSIC FINGERPRINTS

Mathew C. Stamm and K.J. Ray Liu in [8] define techniques based on fingerprints. The authors observe that most of the image processing operations can be viewed as pixel mappings which leave statistical traces; as such, every tampered image carries some kind of "fingerprint" describing the image processing history. Given a mapping (processing algorithm) m , each pixel w in the tampered image J is related to its corresponding pixel x in the original image I by the relationship w = m (x). Therefore, the original image histogram H_I and the histogram H_J corresponding to J are related by:

$$H_J(l) \quad \overset{255}{H_I(l)} \qquad (1)$$

$t\ 0,m(t)$ [redacted]

The authors define the intrinsic fingerprint of the tampering m as $f_m(l)\ H_J(l)\ H_I(l)$, which describes the changes in the image histogram after the application of m .The fingerprint is modeled processing-dependent and analyzed to identify tampered and original image.

Contrast enhancement, for example, is observed to produce an increase in high frequency components of the original histogram. They show that if power law transformation is applied to an image for contrast enhancement it will show an increase in image's high frequency component.

5.2.3 FORGERY DETECTION USING DOUBLE *JPEG*

For any digital manipulation minimum requirement is that an image must be loaded into a photo-editing software program some manipulations will be done and resaved. Since most images are stored in the JPEG format, it is likely that both the original and manipulated images are stored in this format. In this case, the manipulated image is compressed twice. Due to the lossy nature of the JPEG image format, this double compression introduces specific artifacts not present in singly compressed images (it is assumed that the image was not also cropped prior to the second compression).

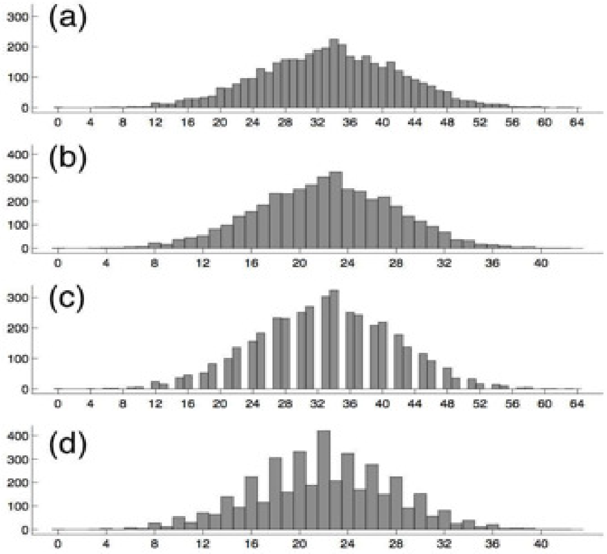

Fig 7 Shown along the top row are histograms of single-quantized signals with (a) Step 2 and (b) Step 3. Shown in the bottom row are histograms of double-quantized signals with (c) Step 3 followed by Step 2, and (d) Step 2 followed by Step 3. Note the periodic artifacts in the histograms of double-quantized signals.

The presence of these artifacts can, therefore, be used as evidence of some manipulation. Alin C. Popescu and Hany Farid [9] define technique to detect double JPEG compression. Note that double JPEG compression does not necessarily prove malicious tampering. Authors consider the example of a generic discrete 1-D signal x[t]. Quantization is a point-wise operation that is described by a one-parameter family of functions:

$q_a(u)\ u$ [redacted] w[redacted]re a is the quantization step (a strictly

positive integer), and u denotes a value in the range of x[t]. Dequantization brings the quantized values back to their

original range: $q_a^{\ 1}(u)$ [redacted] u .Note that the function $q_a(u)$

is not invertible, and that de-quantization is not the inverse function of quantization. Double quantization is a point-wise operation described by a two-parameter family of functions:

$q_{ab}(u)\ u$ [redacted] b [redacted] where *a* and *b* are the quantization

steps. Double quantization can be represented as a sequence of three steps:1) quantization with step *b*, followed by 2) dequantization with step *b*, followed by 3) quantization with step *a*. They also consider a set of coefficients normally distributed in the range [0,127]. To illustrate the nature of the double quantization artifacts, they consider four different quantizations of these coefficients. Shown in the top row of Figure 1 are the histograms of the coefficients quantized with steps 2 and 3. Shown in the bottom row are the histograms of the coefficients double-quantized with steps 3 followed by 2 and 2 followed by 3. When the step size decreases [Figure 7(c)], some bins in the histogram are empty, because the first quantization places the samples of the original signal into 42 bins, while the second quantization redistributes them into 64 bins. When the step size increases [Figure 7(d)], some bins contain more samples than their neighboring bins, because the even bins receive samples from four original histogram bins while the odd bins receive samples from only two. In both cases of double quantization, note the periodicity of the artifacts introduced into the histograms. This type of detection is in format based category as described in section 3.

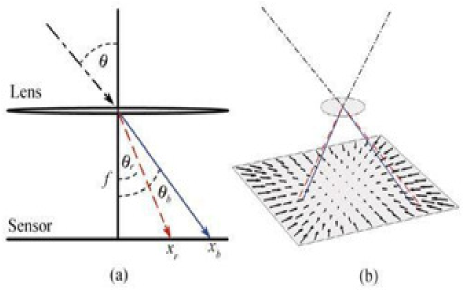

Fig 8 Chromatic aberration, (a) 1-D, (b) 2-D. Figure courtesy of Prof. Hany Farid.

5.2.4 FORGERY DETECTION USING CHROMATIC ABERRATION

In an ideal imaging system, light passes through the lens and is focused to a single point on the sensor. Optical systems, however, deviate from such ideal models in that they fail to perfectly focus light of all wavelengths. Specifically, lateral chromatic aberration manifests itself as a spatial shift in the locations where light of different wavelengths reaches the sensor. There are two kinds of chromatic aberration: longitudinal and lateral. The lateral aberration is introduced by the different wavelengths of light having the different refractive indices of optical lens.

Fig. 8 shows the splitting of short (solid blue) and long wavelength (dash red) light in 1-D and 2-D situation. Johnson and Farid in [10] used a first-order approximation to model the lateral aberration as follow.

$x_r \quad (x_g \quad x_0) \quad x_0$ and $y_r \quad (y_g \quad y_0) \quad y_0$ (2)

where the parameter is a scale value for the color channels with respect to one another. The coordinate (x_0 , y_0) is the center point of the image due to the complexities of the multi-lens system. The model parameters can be obtained by brutal force searching to maximize the mutual information of two color channels. A displacement vector for each pixel in the image can be obtained using the estimated model parameters. When tampering an image, the relation between global estimation and local estimation fails to be consistent, thus the tampered region can be located.

5.2.5 FORGERY DETECTION USING COLOR FILTER ARRAY

A digital color image consists of three channels containing samples from different bands of the color spectrum, e.g., red, green, and blue. Most digital cameras, however, are equipped with a single CCD or CMOS sensor and capture color images using a color filter array (CFA). Most CFAs uses three color filters (red, green, and blue) placed atop each sensor element. Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image. The estimation of the missing color samples is referred to as CFA interpolation or demosaicking. The simplest demosaicking methods are kernel-based ones that act on each channel independently (e.g., bilinear or bicubic interpolation).Regardless of the specific implementation, CFA interpolation introduces specific statistical correlations between a subset of pixels in each color channel. Since the color filters in a CFA are typically arranged in a periodic pattern, these correlations are periodic. At the same time, it is unlikely that the original recorded pixels will exhibit the same periodic correlations. As such these correlations can be used as a type of digital signature. If the specific form of the periodic correlations is known, then it would be easy to determine which pixels are correlated with their neighbors. On the other hand, if it is known which pixels are correlated with their neighbors, the specific form of the correlations can easily be determined. But in practice, of course, neither is known. In [11] the authors describe how to simultaneously determine both the form of the correlations and which pixels are and are not CFA-interpolated. The authors used the expectation/maximization (EM) algorithm. The EM algorithm is a two-step iterative algorithm: 1) in the expectation step the probability of each pixel being correlated with its neighbors is estimated; and 2) in the maximization step the specific form of the correlations among pixels is estimated. By modeling the CFA correlations with a simple linear model, the expectation step reduces to a Bayesian estimator and the maximization step reduces to weighted least squares estimation. In an authentic image, it is expected that a periodic pattern of pixels will be highly correlated with their neighbors and deviations from this pattern are the evidence of localized or global tampering.

6. CONCLUSION

After examining so many source identification and forgery detection methods now we are able to derive some conclusion.

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)or on methods relying on scene content (e.g. lighting and image statistics). This difference is possibly due to the relative difficulty in applying the same hidden characteristics consistently to all the spliced components.

From the 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, 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,

Passive-blind image forensics is still a research area at its infancy. There are fundamental issues related to the parameter estimation of physical model, the design issues of practical system and the system security issues which remain to be addressed. For an effective solution to these issues, expertise from various domains such as computer vision, signal processing, computer graphics, machine learning, imaging sensors, and even mechanical systems are needed.

7.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] Geradts Z, Bijhold J, Kieft M, Kurosawa K, Kuroki K, Saitoh N (2001) “Methods for identification of Images Acquired with Digital Cameras” Proc. SPIE: Enabling Technologies for Law Enforcement and Security 4232:505–512

[3] Lukas J, Fridrich J, Goljan M. “Digital camera identification from sensor pattern noise”, IEEE Transactions on Information Forensics and Security, June 2006, 1(2): 205–214

[4] M. Kharrazi, H.T. Sencar, and N. Memon, “Blind source camera identification”,*ICIP*,2004.

[5] H. Farid, “Digital Image Ballistics from JPEG Quantization”,
Technical Report, TR2006-583, Dartmouth College, Computer Science2006.

[6] Eric Kee, Micah K. Johnson and Hany Farid “Digital Image Authentication from JPEG Headers”, IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, September 2011

[7] Fridrich J, Soukal D, Lukas J. “Detection of copy-move forgery in digital images” In Proc. of DFRWS, Cleveland, OH, USA, 5-8 Aug. 2003

[8]Matthew C. Stamm *and K. J. Ray Liu* “Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints”, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 3, September 2010

[9] A. C. Popescu and H. Farid, “Statistical tools for digital forensics,” in Proc. 6th Int. Workshop on Information Hiding,
Toronto, Canada, 2004, pp. 128–147

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

[11] A. C. Popescu and H. Farid, “Exposing digital forgeries in color filter array interpolated images,” *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3948–3959, 2005.

[12] Hany Farid “Image Forgery Detection [A survey]”, IEEE Signal
Processing Magazine, March 2009

[13] Judith A. Redi & Wiem Taktak & Jean-Luc Dugelay “Digital image forensics: a booklet for beginners”, Multimed Tools Appl (2011) 51:133–162