Front. Comput. Sci. China 2007, 1(2): 166–179
DOI 10.1007/s11704-007-0017-0

REVIEW ARTICLE

A survey of passive technology for digital image forensics

LUO Weiqi, QU Zhenhua, PAN Feng, HUANG Jiwu (✉)

Guangdong Key Lab of Information Security Technology, Guangzhou 510275, China
School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China

Abstract Over the past years, digital images have been widely used in the Internet and other applications. Whilst image processing techniques are developing at a rapid speed, tampering with digital images without leaving any obvious traces becomes easier and easier. This may give rise to some problems such as image authentication. A new passive technology for image forensics has evolved quickly during the last few years. Unlike the signature-based or watermark-based methods, the new technology does not need any signature generated or watermark embedded in advance. It assumes that different imaging devices or processing would introduce different inherent patterns into the output images. These underlying patterns are consistent in the original untampered images and would be altered after some kind of manipulations. Thus, they can be used as evidence for image source identification and alteration detection. In this paper, we will discuss this new forensics technology and give an overview of the prior literatures. Some concluding remarks are made about the state of the art and the challenges in this novel technology.

Keywords image authentication, passive/blind forensics, watermarking, statistics analysis, pattern recognition

1 Introduction

Tampering with images is not a new issue. In the past, manipulations of the images generated by traditional film cameras required professional knowledge and sophisticated dark-room equipment, which is difficult to perform well for average users.

With the advancement in various digital imaging devices, digital images have become ubiquitous today. However, modifying a digital image without any obvious traces is not a difficult task now with the sophisticated image editing software available, such as Adobe Photoshop, GIMP, etc. In fact, many forgeries have been dispersed [1, 2]. A famous example can be found in the 2004 American presidential elections. A widely circulated picture showing the democratic candidate and a famous Hollywood actress sharing a demonstration podium was, in fact, fake [3]. A popular British newspaper was forced to apologize for publishing photographs showing British soldiers abusing an Iraqi prisoner, which were later proven to be fakes [4]. Apparently, "seeing is no longer believing" [5]. It will get worse as counterfeiting techniques become more and more sophisticated. If the tampered images are abused, it may give rise to some big problems which potentially may have deep moral, ethical and legal implications. Therefore, the authentication of digital images becomes an important issue.

Digital signature and watermarking have been proposed as means to authenticate the contents of digital images. However, signature-based and watermark-based methods require some pre-processing such as signature generation and watermark embedding when creating the images, which would limit their applications in practice. Thus they are active methods.

Recently, a novel method for authenticating the contents of digital images has evolved quickly. The technology assumes that the original image has some inherent patterns, which are introduced by the various imaging devices or processing. These patterns are always consistent in the original image and altered after some tampering operations. We can identify the source of the digital image or determine whether an image is authentic or fake by detecting the patterns. Comparing it with prior active methods, this new technology does not need any extra information such as a watermark or a signature. Therefore, the new technology is passive and completely blind.

The paper is organized as follows. First, we will introduce the principles of passive forensics in Section 2. Then we will present a detailed overview of the prior literatures in this new technology in Section 3. Finally, we will draw the concluding remarks and describe the challenges of passive forensics in Section 4.

Received December 31, 2006; accepted February 27, 2007

E-mail: isshjw@mail.sysu.edu.cn

2 Principle of passive forensics

In this section, we will discuss briefly the watermark-based principles. Then we will describe passive forensics, including image-source identification and alteration detection. After that, we will compare the differences between active and passive technologies for image forensics.

2.1 Watermark-based authentication

There are two main sides in the design of a typical watermarking system [6]. The source side is to generate the watermark signal W and embed W into the original image X to get the watermarked image Y. The other side is to extract the watermark W, and give the confidence measure for the detected image.

Figure 1 shows the generic watermark embedding at the source side. We have the watermarked image $Y = f_1(X, W, K)$, where K denotes the key.

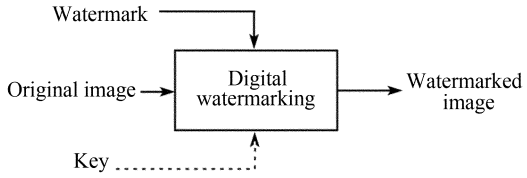

Fig. 1 Generic watermark insertion

Figure 2 shows the watermark extraction at the receiver side. The recovered watermark can be denoted as $\hat{W} = f_2(Y, K)$, where Y is the image to be authenticated. We then use the $\hat{W}$ to identify whether the test image has been tampered with, and then we locate the tampered region.

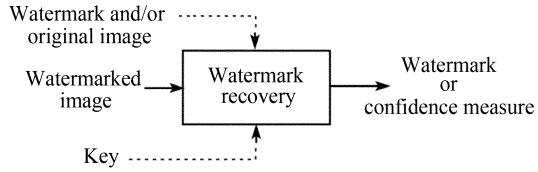

Fig. 2 Watermark extraction

As mentioned above, the basic idea of the watermark-based technology for image authentication is to add a watermark to the original image at the source side, and to recover the watermark fully or partly at the receiving side to identify whether the image has been altered. Therefore any manipulations before the watermark was embedded cannot be detected using this method. The signature-based method has a similar scheme and characteristics, and both of them are active methods.

2.2 Passive authentication

Passive technology assumes that the patterns of original images are distinguishable due to the different imaging devices and image processing inside them. The original patterns (which sometimes are constrained by the statistical characteristics in nature scenes, physical conditions in a scene, etc.) would be altered after tampering. According to the two assumptions, we can divide prior literatures related to passive forensics into the following two main issues[1)]:

2.2.1 Identification of image source

A digital image may come from various imaging devices, e.g., different cameras, scanners, computer graphics technology, etc. The issue concerns source identification. In this case, the process inside the devices is always known. However, different imaging devices have different characteristics due to the use of different physics apparatus, different image processing, and different parameters applied inside the imaging devices, etc. Thus it would lead to different patterns of the output images. We can use these patterns as inherent "fingerprints" of the imaging devices to identify the source of the image.

Figure 3 shows the generic image-source identification scheme. Assume that image X is to be detected. It may come from some candidate imaging devices. The identification process is as follows. Firstly, the features from X and the patterns from the imaging devices are extracted mainly using the knowledge of image acquisition model. Then the similarities between these patterns and the characteristic features are measured. Lastly, a confidence measure for each imaging device to identify the source of the image X is given.

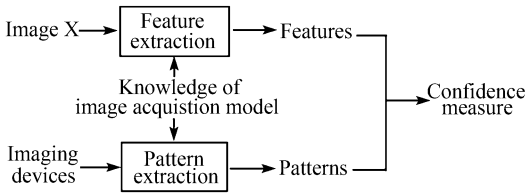

Fig. 3 Generic image source identification

2.2.2 Detection of image alteration

A digital image may be altered by some image processing after being captured by a given imaging device. The issue concerns the problem whether it is possible to determine whether or not an image has been altered by a certain operation. As we know, original images always contain some consistent characteristics, such as consistent noise distribution, light condition, and so on. However, the characteristics would be changed after some image post-processing operations. Then some features of the altered images would become more or less inconsistent. Finding the differences before and after the operations is the key of the technology. It

1) The method of classification is adopted from Ref. [7]. Actually, the two categories are overlapping, some methods may be employed in both cases.

is noted that some of the operations involve malicious tampering, while some do not change the contents of the image, e.g., color and contrast adjustment, etc. However, some operations may be confusing. Take double JPEG compression, for example. Double JPEG-compressed images often result from forgeries when a part of the original image is replaced by another part from the same (region-duplication) or another (splicing) image and then resaved. On the other hand, a user may resave a high-quality JPEG image to a lower-quality one to save storage space. Therefore, detection of image alteration does not necessarily prove malicious tampering in some situations. But it can make us doubt about the contents of the image and help us with further analysis.

Figure 4 shows the generic image alteration detection scheme. The test image X may be an original image, or may be altered by a certain operation. Similarly as shown in Fig.3, we first extract the features from X and obtain the original/altered patterns mainly using the knowledge of the image manipulation model, or sometimes combining with the statistical characteristic in nature scenes, and the image acquisition model, etc. Then we compare the distance between the features and the patterns to decide whether or not image X has been altered.

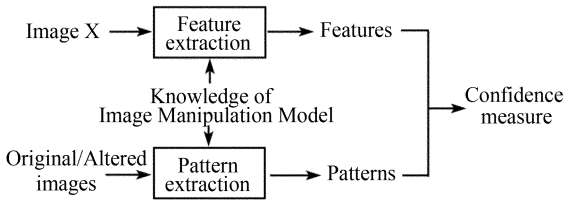

Fig. 4 Generic image alteration detection

In brief, comparing with signature-based and watermark-based methods, passive technology need not use any extra embedded information in advance. We can identify the source or detect the alteration of the image just by using the patterns of the digital images themselves. From another viewpoint, the images have some inherent “watermarks” (patterns). The “watermarks” are introduced not by our intrusive operations, but by the various imaging devices or constrained by some statistical characteristics in the nature scenes. The “watermarks” would be altered after some post-processing. These different “watermarks” can be used as evidence for image forensics.

In most cases, passive forensics can be converted to a problem of pattern recognition. The solution to the problem is finding the different patterns according to the knowledge from various imaging devices or the manipulations or the nature scene constraints, etc. The selected patterns with distinguishing ability are crucial for this new technology. In the following section, we will give a detailed overview of some prior typical works in this new area, and show which exact inherent patterns can be applied to digital image forensics.

3 Techniques of passive forensics

As mentioned above, image-source identification and image-alternation detection are the two main issues in passive forensics technology. In this section, we will discuss these two issues.

3.1 Identification of image source

Digital images can be captured by various imaging devices such as digital cameras, scanners, and so on. These imaging devices are available to our average users. In many applications, we must deal with problems about the source of the digital images. In a court case involving child pornography, for example, if a suspect camera has been found, is it possible to determine whether the images have been captured by the same camera? In other cases, images can also be generated entirely by computer. As computer graphics technology progresses, it becomes difficult to distinguish by sight the photographic images from the computer-generated images. Recently, some digital forgeries mixing the real scene and computer-generated virtual scene together have been reported. Is it possible to identify and distinguish these two kinds of images?

3.1.1 Identification of digital camera

High-resolution and low-cost digital cameras have been rapidly replacing the typical film cameras. Now, most images in our daily life are acquired by various brands of digital cameras, such as Canon, Nikon, Sony, Olympus, etc. One of the main problems related to source identification is the classification of the different camera models or individuals for a given image.

The most straightforward solution for camera identi fication is to check the EXIF (Exchangeable Image File, most digital cameras now use the EXIF format [8]) header of the output image (Raw, Tiff or JPEG format file, and most digital cameras export images in the JPEG format). Some settings of an image are stored in the headers, and the settings are constrained by a given camera, such as the manufacturer, the model of the camera, image size, exposure time, and the quantization matrix used in JPEG compression [9], etc. If the given image settings are out of the range of the given camera, it can be concluded that the image did not come from the camera or it was not the original one at least. However, we cannot distinguish among the cameras of the same or similar model whose images contain the same header information. Furthermore, the header information can be easily replaced or made consistent by JPEG recompression or other operations. Can we find other features that cannot be easily removed by average users? In the following, we describe briefly the operations inside a typical digital camera first, and then analyze which knowledge can be used as reliable evidence for camera identification.

Figure 5 shows the operations inside a typical digital camera. The light coming from the scene passes through the

camera lens, and then through an anti-aliasing filter. The photons reach a color filter array (CFA). The photos are then converted to voltages and subsequently quantized to a digital signal by the A/D converter. The camera reads out the value from the sensors, and performs some post-processing such as CFA interpolation (for the cameras with single sensor), white balance, gamma correction, etc. JPEG compression may be applied to save storage space in the last step. Please refer to [10] for more details.

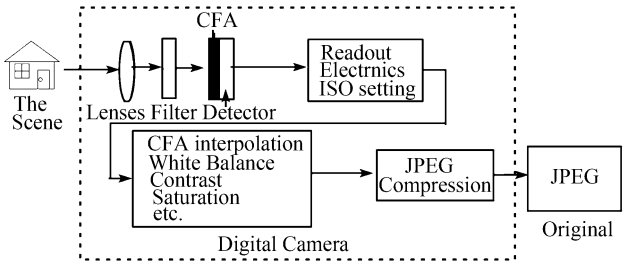

Fig. 5 The operations inside a typical digital camera

The operations shown in Fig. 5 are the standard stages inside a typical digital camera. However, the exact processing details in each stage may be different from that of various models of the cameras. Thus the output images from cameras of different models would be different even getting the same picture frame. In Ref. [11], Kharrazi et al. proposed a blind method for camera model identification based on this assumption. In the method, each output image is represented as a 34-D vector with a number of features, including average pixel value, RGB pairs correlation, energy ratio, etc., that are mainly affected by the color processing/transformation and CFA interpolation, and other features from image quality metrics (IQM). Then a multi-class support vector machine (LibSVM tool, see Ref. [12] for more details) is employed to get a classifier. The images from five different models of camera can be identified. The initial results are encouraging. The accuracy is from 78.71% to 95.24%. Another work related to the effects by various operations inside the camera is the camera response function (CRF). Refer to next subsection "Forgery detection in digital camera images" for more details.

Imaging sensor is the heart of every digital camera. The fingernail-sized sensor contains millions of photosensitive diodes that are arranged in rows and columns at regular intervals, as shown in Fig. 6. The photosensitive diodes called photosites are used to record the brightness of the light that falls on it by accumulating a charge. The charges are then converted into voltage, and subsequently the voltage is quantized to a digital signal. Using the imaging sensor, we can obtain the brightness value at different positions of the scene; therefore a two-dimensional image is recorded.

However, the imaging sensors make a great difference among the different models (or even in the same model) of digital cameras in the sensor manufacturing process. These different characteristics of the sensors can be expected to be unique and inherent to an individual camera, and further to be used for identifying the source of the digital images. Some of the previous literatures [13—19], etc. about the source identification are based on the analysis of the imaging sensors or their implementations.

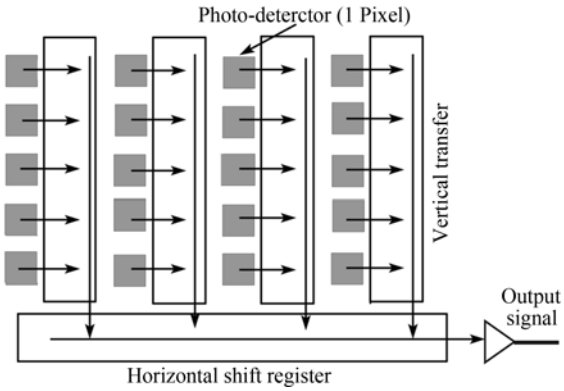

Fig. 6 Scheme of CCD array

i) Based on the defective pixels

In Ref. [13], the authors pointed out that there were some defects pixels in the Charge Coupled Device (CCD) inside the low-cost digital cameras. These defects pixels are at the different places of the CCD according to the different sensors, and thus can be used as the unique evidence for the cameras. As the authors mentioned in the paper, there are some restrictions when using this method. For example, the defects pixels are visible only in the regions that are darker or in the lighter areas if a surface has the same intensity lighting. These defects pixels also depend on the temperature. Furthermore, some post-processing operations such as JPEG compression, etc., may remove or suppress the defective pixels. For the expensive cameras which have better CCDs with fewer errors, the method cannot be applied.

ii) Based on the pattern noise

Some other methods are based on the pattern noise in imaging sensors. The pattern noise is defined as any noise component that survives frame averaging [20], which is another important characteristic of imaging sensors. The pattern noise [14] include two main components: the fixed pattern noise (FPN) and the photo-response non-uniformity noise (PRNU) as shown in Fig. 7. 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. In Ref. [21], the authors used FPN to identify the video camera from videotape images. They recorded 100 black images with each camera by covering the lens, and then the images were accumulated to suppress the effect of the random noise. The results show that some bright dots are observed in the accumulated images, and these bright dots are at different positions for each camera, as shown in Fig. 8. We can see that this method is similar to the method to detect defects pixels

proposed in Ref. [13]. However, FPN is visible only in the dark frames. Furthermore, the noise can be alleviated at a low temperature.

Another main source of the pattern noise in imaging sensor is PRNU. Unlike FPN, which is generated thermally in the sensor even when no light arrives, PRNU is the pixel variation under illumination. FPN is an offset, while PRNU is a gain. Therefore, the primary source of pattern noise remaining in nature images may be PRNU. As illustrated in Fig.7, two sources contribute to PRNU. The main source is pixel non-uniformity (PNU), and the other source is low-frequency defects, which is caused by light refraction on dust particles and optical surfaces, etc. This source is low spatial frequency in nature. Lucks et al. used PNU as an inherent pattern of the imaging sensor for camera identification analogously [15–17]. To verify that a given image p was taken with a specific camera *C*, they first extracted the camera reference pattern P_C, which is an approximation of PNU. The extraction process is as follows: Assume that some images are taken by camera *C*, denoted as $p^{(k)}$, $k = 1, 2, \cdots, N_p$, where $N_p > 50$. For each image $p^{(k)}$, get the noise residuals $n^{(k)} = p^{(k)} - F(p^{(k)})$, where a wavelet-based denoising filter *F* is applied to suppress the effect from the contents of the image and get an approximation of PNU for the image $p^{(k)}$. By averaging the multiple noise residuals $n^{(k)}$ to suppress the random noise, the camera reference pattern $P_C = \Sigma n^{(k)} / N_p$ can be obtained. To determine whether an image *p* is taken by camera *C*, the method calculates the correlation between the camera pattern P_C and the noise residuals *n* of *p*.

$$\rho_C(p) = corr(n, P_C) = \frac{(n - \bar{n}) \cdot (P_C - \bar{P}_C)}{\| n - \bar{n} \| \cdot \| P_C - \bar{P}_C \|}$$

where $\bar{n}$ and $\bar{P}_C$ are the mean value of *n* and P_C, respectively. Lastly, it experimentally determines the distribution of whether the images are taken by *C*, and chooses a proper threshold to make a judgment. The experimental results in Ref. [15] demonstrate that the method is effective without a misclassification when applied to about 3,000 images from nine cameras, with two cameras of the same model, and that it is possible to identify the images even they have been JPEG-compressed. However geometrical operations such as cropping and rotation will cause desynchronization in PNU and decrease the accuracy. Furthermore, it is easy to remove the pattern noise from an image or insert pattern noise into an image from another camera to prevent identification.

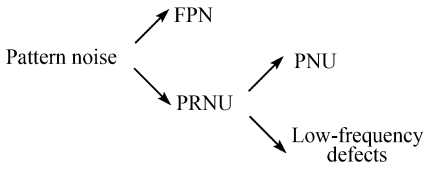

Fig. 7 Pattern noise in CCD

iii) Based on demosaicking techniques

Usually the sensor is the most expensive component in a digital camera. Due to cost considerations, many manufactures employ a single sensor instead of multiple sensors to capture the color scene. Thus the color filter array (CFA) is always applied in front of the sensor to control the band of wavelengths arriving at the CCD array. Figure 9 shows the typical CFA pattern widely used. Note that for each 4×4 block in RGB CFA pattern, only two Green, one Blue, and one Red values are recorded, while the other color components (two Green, three Blue, and three Red values) are missing. In order to reconstruct the full-resolution color scene, some interpolation algorithms will be employed. The estimations are usually carried out by interpolating neighboring pixel values using a weighting matrix around the missing pixel, which are called demosaicking techniques. Some commonly used demosaicking techniques—such as bilinear, smooth hue, median, gradient-based, adaptive color plane, etc.—are described in Ref. [19] and [22]. The correlations may be linear, nonlinear or adaptive. And these different techniques are employed in different models of cameras, which will inevitably introduce a different statistical correlation between the original values and the interpolation values. There are some works to identify the source camera based on CFA demosaicking [19, 23, 24].

Fig. 8 Illustration of fixed pattern noise in different Cameras, (a) Camera One, (b) Camera Two

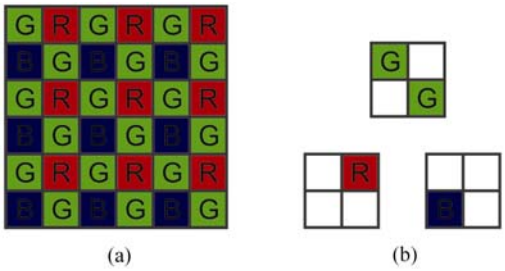

Fig. 9 The popular color filter arrays, (a) RGB, (b) Missing values

In Ref. [19], the authors simply modeled the demosaicking as a linear interpolation. For each sample in $f(x, y)$,

$$f(x, y) = \sum_{u,v=-N}^{N} \alpha_{u,v} f(x+u, y+v) + n(x, y)$$

where α is the coefficients in the $N \times N$ weighting matrix with $\alpha_{(0,0)} = 0$. $n(x, y)$ denotes i.i.d Gaussian noise with zero mean and unknown variable δ^2. To estimate the pattern of the correction between the samples, the EM (expectation/maximization) algorithm has been applied. The algorithm includes two steps: E-step and M-step. In the E-step, the probability of each pixel belonging to an original pixel or to the interpolated one is evaluated. Then in the M-step, the estimation is optimized and updated. The two steps are iterative and always converge. Finally, a 2-D probability map of

hidden patterns that indicates the likelihood of the pixel belonging to an interpolated one and can be employed to identify which CFA interpolation linear coefficients $\vec{a}$ are obtained. The periodicity of the probability map can be used to identify whether the image has undergone CFA interpolation (See Fig. 10), while the linear $\vec{a}$ can be employed to identify which CFA interpolation algorithm has been used. The testing on the artificially generated images with eight demosaicking technologies can be seen in Fig. 11.

3.1.2 Classification of computer graphics and photographic images

Images can be entirely generated by computer. As computer graphics (CG) technologies rapidly develop, CG-rendering software has become more and more sophisticated. Now the level of state-of-the-art technology can make CG images hardly distinguishable from photographic images via human perception. One of the problems related to source identification is the classification of the two types of images. Some methods [25–28] have been proposed to tackle the problem.

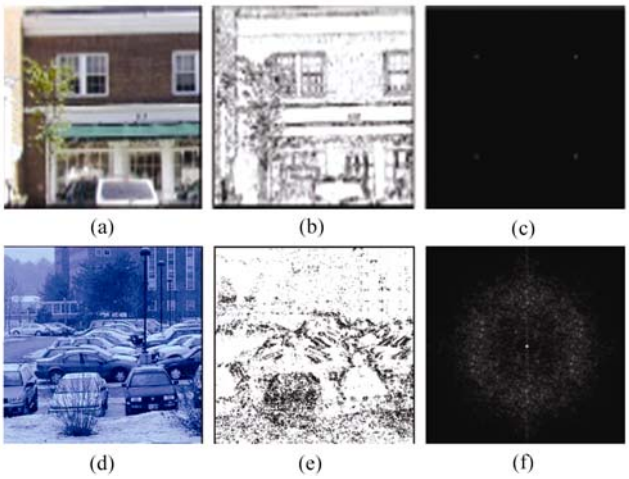

Fig. 10 The probability map of CFA interpolated images will appear a periodic pattern in its Fourier domain, while the No CFA images will not. Figure courtesy of Prof. Hany Farid, (a) CFA image, (b) P, (c) $|(\mathcal{F}(P))|$, (d) No CFA image, (e) P, (f) $|(\mathcal{F}(P))|$

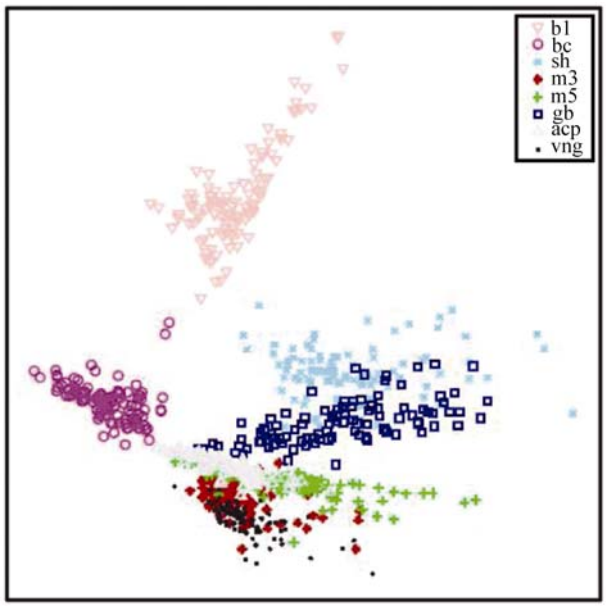

Fig. 11 Let $N = 1$, then each color channel has 8 linear coefficients. Thus a color image can be denoted as a 24-D vector. The 24-D space is then projected on 2-D space using PCA. The 8 interpolation algorithms are also separable. Figure courtesy of Prof. Hany Farid.

In Ref. [26], Lyu and Farid presented a classification method for CG images and photographic images based on first-order and higher-order wavelet statistics. The method decomposes the image using a four-level separable quadrature mirror filters, and then extracts the first four order statistics of the subband coefficients. Other statistics features are obtained from the errors in a linear predictor of coefficient magnitude. For each image, 216-D feature vector (72-D for each channel) is collected for capturing regularities of CG images. Both linear and non-linear classifiers are employed to distinguish the CG images and photographic images. The method achieves the detection accuracy of 66.8% with 1.2% false-alarm rate. However, the statistics features cannot give us any insight into how one is rending the CG images, as well as the physics differences between the two image categories.

In Ref. [27], Ng, et al., analyzed the physical differences in generation between CG and photographic images, e.g., the sharp structures in CG images and gamma correction in photographic. They then proposed a geometry-based image model that reveals the differences. For source identification, the method extracts the geometry features based on the rigid body moments. Finally, an SVM classifier [12] is employed. The experimental results show the effect of the proposed method with a classification accuracy of 83.5%, which outperforms the prior methods. Another contribution of their work is that they created an image benchmark for the classification problem of CG and photographic images. The dataset includes four component image sets about thousands of

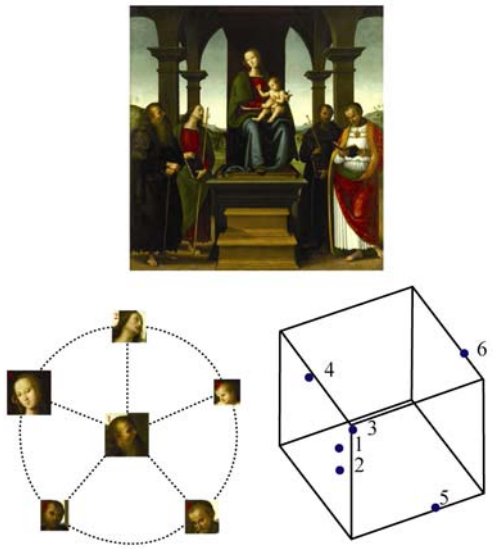

Fig. 12 The scanned version of *Madonna with Child* by Perugino (top). Six faces are observed (bottom left). The results of analyzing the six faces show that first three faces cluster, while the remaining faces are distinct (bottom right). This clustering pattern illuminates that there are at least four hands contributing to this painting. Figure courtesy of Prof. Hany Farid.

images (see [29] and [30] for more details).

3.1.3 Other issues in source identification

Passive forensics can also be used as a computational technique for art authentication such as in the detection of forgeries and recovery of different artists within a single work (the “many hands” problem). In Ref. [31], Lyu, et al., proposed a computational tool for art authentication based on wavelet decomposition. The method first converts the drawings or paintings to digital images with high-resolution digital scans, then extracts the first-order and higher-order statistics features [25] of wavelet coefficients, which can be served as the “handwriting” of the art for art authentication. They applied the technique to distinguish 8 authentic arts from Bruegel (one of greatest painters among the Flemish) and five imitations. Furthermore, they employed the technique to analyze the “many hands” problem, as illustrated in Fig. 12. The preliminary results show that the method is efficient, and both tests convince expert authentications. Other similar literatures can be found in Refs. [32, 33].

3.2 Detection of image alteration

As the image-editing and computer graphics technologies become more and more sophisticated [34-36], user-friendly software—such as Adobe PhotoShop, PaintShop, and GIMP—is widely used in our daily life. Tampering with an image without any obvious traces is no longer a hard task even for average users, and thus would result in some complicated legal issues e.g. Ref. [37]. Generally speaking, image alteration does not prove malicious tampering, as in the cases of color/contrast adjustment for image enhancement, and file format conversion for saving storage space. These manipulations do not fundamentally change the contents of the original image, while malicious tampering will alter the meaning of the image, such as removing, adding and modifying an object in a scene. Malicious manipulations, in collaboration with subsequent operations such JPEG compression, contrast adjustment, blurring, etc., would make forgeries hard to detect. Therefore image-alteration detection can determine whether the images are original and help us with further analysis.

3.2.1 Operation history in JPEG

JPEG is a commonly used compression standard [38] and has been found in many applications. Most digital cameras export this file format. Detecting this type of images may play an important role in countering image forgery.

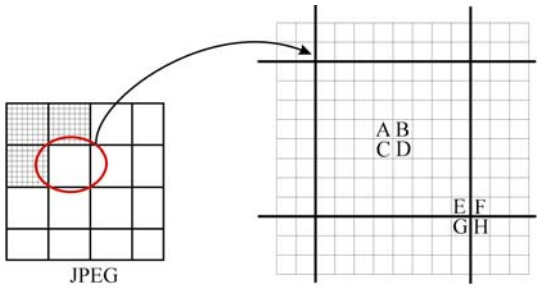

Fig. 13 Blocking artifacts detection in JPEG

In Ref. [39] and [40], Fan et al. proposed a method to identify the bitmap compression history; that is, given an image which is saved in bitmap format, to determine whether it has been previously JPEG-compressed, and further to estimate which quantization matrix has been used. The original intention of the paper was not for tampering detection. However, it can provide us indirect evidence for image forensics. The method assumes that if there is no compression the pixel differences across blocks should be similar to those within blocks, while they should be different due to block artifacts if the image has been JPEG-compressed. As shown in Fig.13, we can calculate the differences within a block and spanning across a block boundary. For each block, we compute

$$Z' = |A+D-B-C|, \quad Z'' = |E+H-F-G|.$$

We then compute the normalized histograms $H_I(n)$, $H_{II}(n)$ of the Z', Z'' respectively. The blocking signature measure is

$$K = \sum_n |H_I(n) - H_{II}(n)|.$$

The method can detect the image with the quality factor (Q-factor) as high as 95. Fig.14 illustrates the differences in

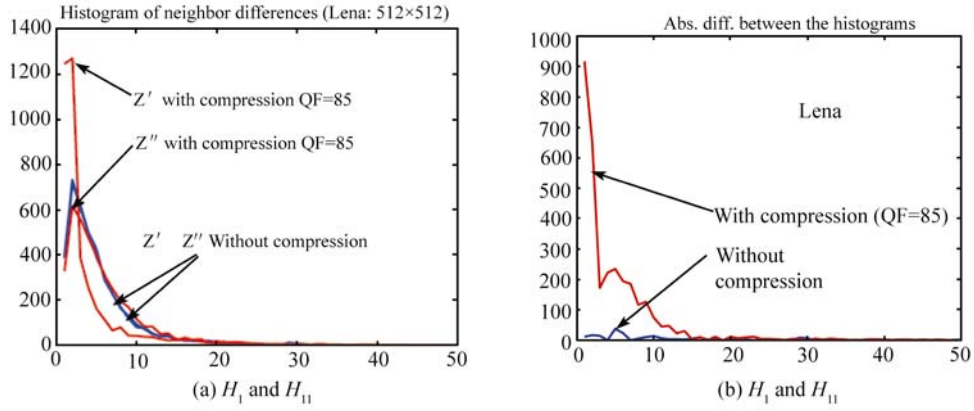

Fig. 14 Comparing compressed (red) and uncompressed (blue) Lena. (a) shows the histogram of H_I and H_{II} . (b) shows the difference between H_I and H_{II}. Notice that H_I and H_{II} are much different in the compressed image, while they remain the same in the uncompressed image

histogram (unnormalized) for the Lena image. After detecting a compression signature, the authors presented a method for maximum likelihood estimation (MLE) of JPEG quantization steps and showed the reliability via experimental results. Another simpler method for estimating the quantization steps can be found in the appendix of Ref. [41]. Fridrich, et al., used the following formula $E_i(q)$ to measure the compatibility of the i-th DCT coefficients with the quantization step q.

$$E_i(q) = \frac{1}{T}\sum_{k=1}^{T}\left| d_k(i) - q \times \text{int}\,eger\_round\frac{d_k(i)}{q}\right|.$$

where $d_k(i)$ is the DCT coefficients, $0 \leqslant i \leqslant 63$, $k = 1, \cdots, T$ from all unsaturated 8×8 blocks. If the image has been previously JPEG-compressed, there are some local minimum values at the corresponding quantization step q and at all integer divisors of q. The maximum of these values is the estimation of the quantization step q, as shown in Fig. 15. Both methods mentioned above are based on the DCT coefficients. Since most of the energy of nature images is in the low frequencies and many higher frequencies coefficients are always quantized to zero, it is expected that there are sufficient statistics to determine quantization steps in high-frequency comments. Note that the situation may also happen in the detection of double JPEG and the estimation of the primary quantization matrix in double JPEG-compressed images. Other works about the estimation of the original operation parameters in JPEG, such as compression color space, can be found in Ref. [42–44].

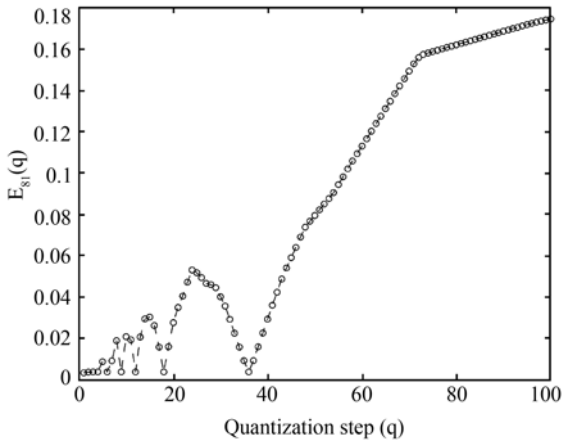

Fig. 15 The compatibility function of the 35-th DCT coefficients (gray baboon with quality factor 75) with quantization step q from 1 to 100. Observe that the local minimum values are at the position 36, 18, 12, 9, 6, 4, 3, 2 and 1, which suggests that the quantization step is 36

Another issue about JPEG forgeries is the detection of double JPEG compression. In Ref. [45], Lukas et al. proposed a method to estimate the primary (previous) quantization matrix from a double-compressed JPEG image. In Ref. [46], Popescu, et al., presented a method to determine whether the image has been double JPEG-compressed. Both works are based on the periodicity in the histogram of DCT coefficients that is introduced by double JPEG compression. Fig. 16 illustrates the specific artifacts of double JPEG images. As mentioned in Ref. [45], however, there are some theoretical limitations to make it impossible to detect double JPEG-compressed images using the method. For example, if the first quantization step q_1 is a divisor of the second quantization step q_2, or more especially when $q_1 = q_2$, the periodicity in the histogram of DCT coefficients would not occur, thus the method would fail in these situations.

In Ref. [47], Fu, et al., applied the first digit law (Benford's law) to estimate the JPEG-compression history and detect double-compressed JPEG images. The authors demonstrated that the probability distribution of the first digit of the DCT coefficients in original JPEG images (single-compressed) followed a Benford-like logarithmic law, and proposed the generalized Benford's law to precisely describe the distributions of the original JPEG images with different Q-factors.

$$p(x) = N\log_{10}\left(1+\frac{1}{s+x^q}\right),\ x = 1, 2, \cdots, 9$$

where N is a normalization factor. s and q are the model parameters. Note that when $N = 1$, $s = 0$, and $q = 1$, the generalized formula is reduced to the normal form of Benford's law. The proposed model is then tested on the UCID (An Uncompressed Colour Image Database [48]). The curves shown in Fig. 17 (a) are the mean distributions of the first digit in single JPEG-compressed images. The parameters of the proposed model are achieved using the curve fitting tool box. The experiment results show that the model fits the actual curves perfectly and the sum of square errors is only around 10^{-6}. The authors also demonstrated that the law was very sensitive to double JPEG compression with different quality factors. As shown in Fig. 17 (b), the first digit of the DCT coefficients in double JPEG-compressed images will not follow the law; thus, the Benford's law can be used as a signature for detecting double JPEG processing.

Besides that, in Ref. [49], Luo et al. proposed the blocking artifact characteristics matrix (BACM) M to detect the cropped and JPEG-recompressed block, which always occurs in a composite or region-duplication image. The BACM exhibits a regular symmetrical shape for original JPEG images, while the regular symmetrical property would be destroyed after cropping and recompressing operations, as shown in Fig. 18. They also demonstrate successful performance of the method in experiments.

3.2.2 Region-duplication/spliced images detection

One of the common image tamperings 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 post-processing 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 robust-

ness against various post-processing operations is the main problem of the detection algorithm. The prior literatures proposed in Ref. [50–52] are all based on block matching. First, the methods divide an image into small blocks, extract the features for each block, and then identify possible duplicated regions by comparing their similarities. The main difference of these methods is the choice of the features. In Ref. [50], Fridrich, et al., analyzed the DCT coefficients for each block. Popescu, et al., employed the principal component analysis (PCA) to reduce the image blocks into a PCA feature vector. In Ref. [52], Luo et al. extracted seven features for each block. Their experimental results demonstrated that the method can resist more post-processing operations.

Another common tampering method is splicing [53]. Unlike region-duplication, image splicing is defined as a simple joining of image fragments, which always come from two or more different images. Fig. 19 demonstrates the differences between region-duplication and splicing. Open benchmark data for splicing images was created by NG et al. [54]. The data set includes 1845 image blocks with a fixed size of 128×128 pixels. It has 933 authentic and 912 spliced images with diverse content and realistic splicing conditions.

Several researchers have investigated the problem of splicing detection [55–60]. In Ref. [55], Farid proposed a method based on a statistical model for nature images. The method first decomposes the test image with three-level wavelet and calculates the first four statistical moments for each nine high-frequency subbands as features. The same operations are performed for the prediction of wavelet coefficients to obtain other 36-D features. So 72-D feature vector can be generated for each test image. Finally, an SVM classifier is applied.

Bicoherence is a normalized version of the bispectrum. It is sensitive to the non-Gaussian signal and is successfully used for detecting human-speech splicing [61]. In Ref. [56],

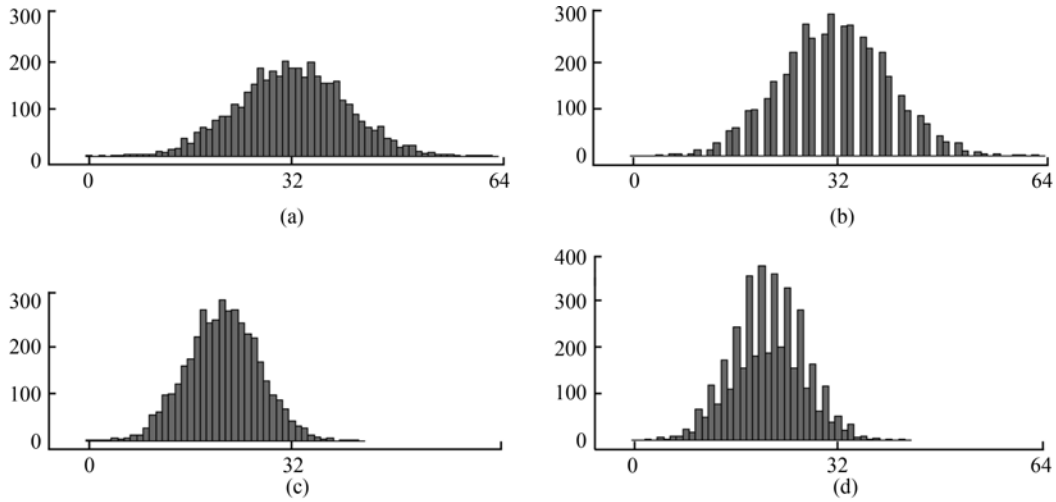

Fig. 16 Periodicity in the histogram of DCT coefficients, (a) step =2, (b) step1=3, step2=2, (c) step =3, (d) step1=2, step2=3. Figure courtesy of Prof. Hany Farid.

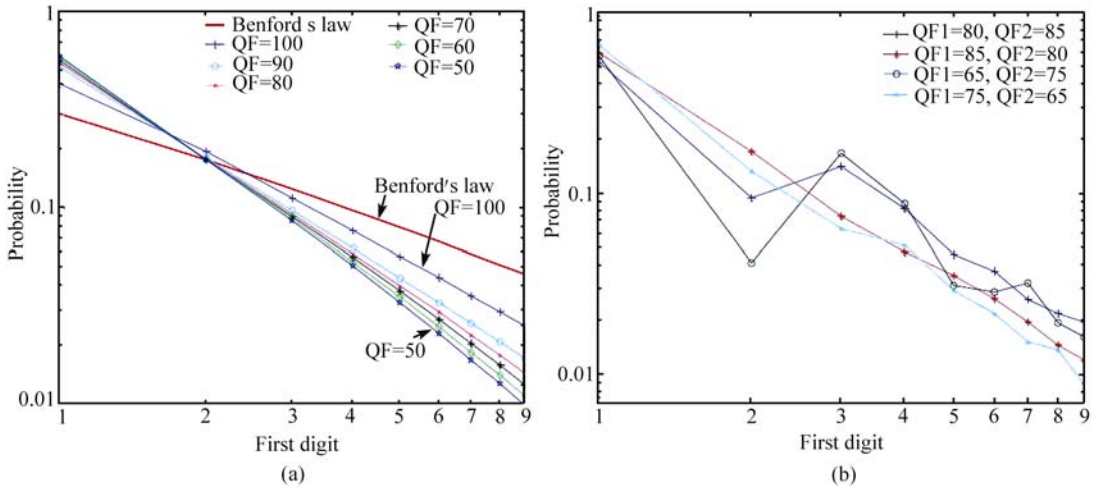

Fig. 17 Benford's Law for JPEG coefficients. a) Mean distributions of the first digit of JPEG coefficients in UCID with single compression; b) Mean distributions of the first digit of JPEG coefficients in UCID with different Q-factors combination. All of the curves are log-log scaled for display purpose. Figure courtesy of Prof. Shi.

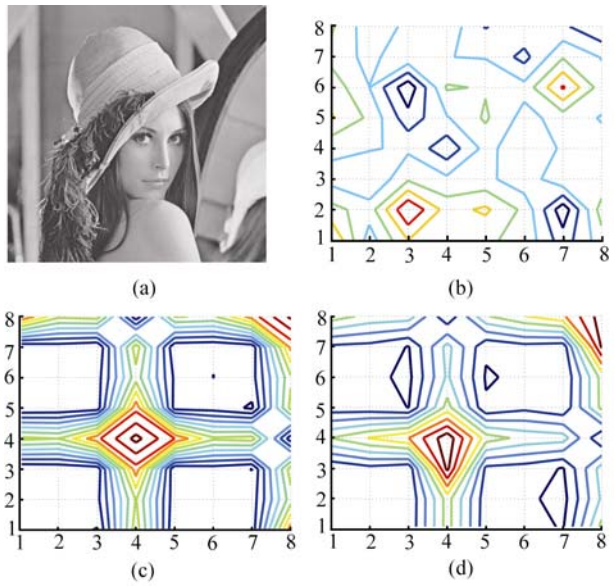

Fig. 18 (a) Lena, (b) comparing the contour of $M(x, y)$ in uncompressed Lena, (c) original JPEG image with quality factor 85, (d) original JPEG image with QF1 = 50 has been cropped 2 rows and 3 columns and recompressed with QF2 = 85

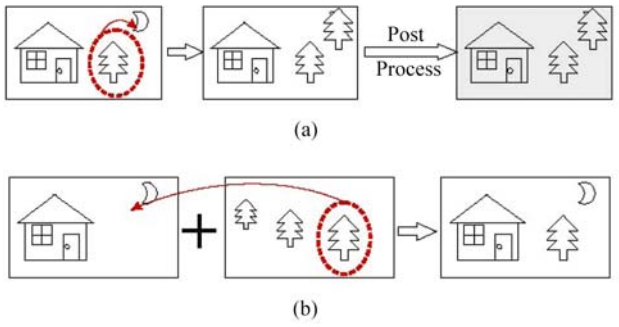

Fig. 19 Different models between (a) Region-duplication and (b) Splicing

Ng, et al. extended the bicoherence-based method for detecting image splicing. In order to improve the detection performance, two methods were proposed: estimating the bicoherence features of authentic images and incorporating image features that characterize the variance of the feature performance. Finally, an SVM classifier is employed. The detection accuracy evaluated on the image data set [54] is about 70%.

Lighting inconsistency always occurs in a composite image, as demonstrated in Fig. 20. When combining image fragments from different images, light conditions are hard to match. Therefore, light detection for different parts in an image can be employed to identify the splicing of images. In Ref. [58], Johnson and Farid proposed a technique to detect a spliced image based on the light inconsistencies.

In Ref. [59], Hsu and Chang presented a semi-automatic method to detect image splicing based on geometry invariants and camera characteristic consistency. The method allows users to select suspicious regions in an image and then detects the CRF of each region based on geometry invariants used in Ref. [62]. Finally, it checks whether the CRFs are consistent with each other using cross-fitting techniques. CRF inconsistency implies splicing.

In Ref. [60], Chen, et al., presented a novel splicing detection approach based on phase congruency and statistical moments of characteristic function. Image splicing would introduce many “non-linear” signals especially at locations in which sharp image transitions, such as lines, edges, and corners. This will lead to high phase congruency. Besides the phase features, the moments of wavelet characteristic functions [63] have been employed to extract the features for splicing detection. The features including 24 phase features and 96 moment features for each test image and its prediction-error image are extracted from the subbands of three-level wavelet decomposition. Lastly, SVM [12] is used for classification. The experimental results have shown that the phase congruency, in collaboration with statistical moments, can effectively capture the discontinuities due to splicing. The detection accuracy evaluated on the image data set [54] is about 82.32%, outperforming the method in Ref. [56].

Fig. 20 Forgery example with light inconsistency. The estimate direction for Kerry is 123°, while the direction for Fonda is 86° . Figure courtesy of Prof. Hany Farid

3.2.3 Forgery detection in digital camera images

Some works about image-alternation detection are based on the inherent characteristics introduced by digital cameras, e.g., Ref. [17, 24, 62, 64].

In Ref. [17], Lukas et al. presented an automatic approach to detect the tampered region based on the pattern noise, which is a unique stochastic characteristic of imaging sensors, as mentioned in source identification. The regions that lack the pattern noise are highly suspected to be forgeries.

The CFA interpolation algorithm is one of the special operations inside digital cameras. The CFA patterns are not only employed for the identification of different types of cameras, but also serve as a signature for image alternation. When tampering with an image, it may destroy the underlying statistical correlation introduced by CFA interpolation. The inconsistent patterns imply the image alternation [19], as shown in Fig. 21.

Camera response function (CRF) [65] is another important characteristic of digital cameras. The function maps the light energy incident r on the image sensor to the intensity R of the final output image. The non-linear function $R = f(r)$ regards the camera as a black box, and the output value R is

Fig. 21 The original and altered images are shown on the top row, the probability map of the altered image is on the bottom left. The detection results (bottom right) show that the tampered region on the probability map lacks the periodicity in its Fourier domain. Figure courtesy of Prof. Hany Farid.

a collective effect of all the internal operations in the camera. Since different camera models employ different operations or different parameters in the same operation, CRF may possibly serve as an inherent feature of a camera model. Furthermore, the inconsistent CRFs of the image patches inside an image can be used as evidence of forgeries. In Ref. [66], Farid described a technique for blind inverse gamma correction assuming that the transformation of the image irradiance is a gamma function $g(u)=u^{\gamma}$. In Ref. [67], Lin and Zhang presented a novel method for blind estimation of CRF from a grayscale image based on the uniform distribution of the image irradiance in local edge regions. In Ref. [62], Ng, et al., proposed that the differential invariants, i.e. the transform and geometry invariants, could be employed to recover CRF from a single channel image. In Ref. [59], the authors identified the splicing image based on CRF detection. In Ref. [68], Lin, et al., presented a method for detecting a doctored image based on CRF abnormality.

Chromatic aberration widely exists in various optical imaging systems. It behaves as the inability to focus light of different wavelengths in a digital camera. 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. 22 shows the splitting of short (solid blue) and long wavelength (dash red) light in 1-D and 2-D situation. In Ref. [69], Johnson and Farid used a first-order approximation to model the lateral aberration as follow.

$$x_r = \alpha(x_b - x_0) + x_0, \quad y_r = \alpha(y_b - y_0) + y_0$$

where the parameter α 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 [70]. 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

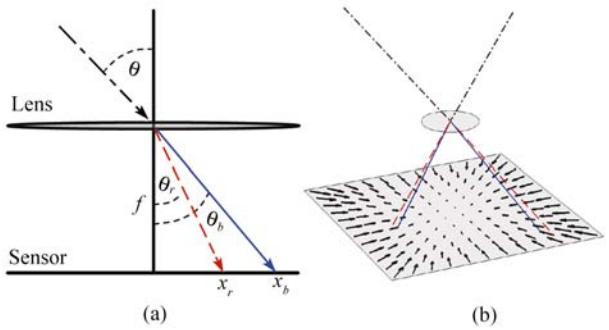

Fig. 22 Chromatic aberration, (a) 1-D, (b) 2-D. Figure courtesy of Prof. Hany Farid

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.

3.2.4 Other issues on image alteration detection

Some of other works about image-alternation detection, such as detecting re-sampling images, images with inconsistent noise patterns, rebroadcast image detection, double MPEG-compression detection in Video, forgery detection in scientific images, etc., can be found in Refs. [25, 71–76].

4 Concluding remarks

Passive technology for image forensics is a new research area. Unlike the signature-based and watermark-based methods, the new method is blind without extra side information in detection. The inherent pattern of the image can be served as a non-intrusive “watermark” for source identification and alternation detection. Therefore pattern selection is crucial in this technology.

Recently, several research groups have started to investigate passive technology, and some works have been reported. As mentioned above, previous literatures can be classified into two main categories: identification of image source and detection of image alteration. Although some of the existing methods succeed in reaching a relatively high accuracy, there are still some weaknesses to be improved on. First of all, most of state-of-art are fragile to some post-processing. As passive technology is mainly based on detection of the inherent pattern, pattern removal and pattern reinsertion would prevent detection. For example, in source-camera identification based on pattern noise [15], there are some ways to prevent identification, such as removing the pattern noise from the image, extracting the pattern noise from another camera and then adding it to an image to confuse identification, etc. However, some of these operations are beyond the ability of average users, such as pattern noise extraction, Re-JPEG artifacts removal, CFA re-interpolation, chromatic aberration reparation, make the lighting consistency by virtual light source(s) and so on, which require the attacker mastering some professional knowledge about digital cameras, image processing, computer graphics, etc. Furthermore, any post-processing performed on the tampered

image may introduce new or more inconsistencies into the image and thus may leave other traces for detection. Therefore the new technology may be effective in most situations.

Secondly, standard image dataset and benchmark are in urgent demand for evaluating the proposed methods. For example, the estimation of the parameters employed inside a digital camera requires an image dataset including various models of camera with different acquisition settings. For the splicing detection evaluation, we need to create the image dataset with more realistic operations. For the problem of identifying computer-generated and digital-camera images, the dataset should include higher photorealism computer graphics with the same scenes as photographic images. To reduce the effects of the software and physics apparatus, the CG images should be generated by different software programs, and the photographic images should be captured by different models of cameras, etc.

Also, some of the proposed methods are under too many constraints. For example, the methods for the image-splicing detection do not consider post-processing at all. However, when creating a forged image, the attacker could apply some operations such as edge blurring, adding noise, and lossy compression, etc., after the simple joining of image regions. And such post-processing will inevitably decrease the detection accuracy. In double JPEG detection, the method assumes repeated JPEG compression with different quantization matrices. Thus, all the prior methods may fail when recompressing with the same quantization matrix. Furthermore, most of the passive technologies are dependent on statistical features of the image. If a small portion of an image has been manipulated, the statistical features may not be altered. Thus the tampered region should be large enough to be detected when using some of the passive technologies.

Passive technology for image forensics is still in its infancy. There are many open issues. For example, finding more robust statistical features to resist the various post-processing and creating image benchmarks to set up a fair evaluation system. Besides that, when tampering with an image or creating a CG, we must use editing software. However, such software programs are diverse due to the different implements inside them. For instance, when editing JPEG images, IJG, Adobe Photoshop, GIMP and matlab may be used. According to our experiments, even in decompressing the same image, the outputs are different. The inherent patterns introduced by editing software may be used as signature for image forensics. Furthermore, most the prior literatures focus on the forgery detection. However, the forgery detection and tampering technology are interactional, just like the relationship between steganalysis and steganography. The advanced image manipulation technologies combining with image processing, computer vision and computer graphics need to be further investigated for making the forgery more realistic and harder to detect. Lastly, the passive method in collaboration with the active approach (signature-based, watermark-based) may play an important role in the field of image forensics.

Acknowledgements This study was supported by the National Natural Science Foundation of China (Grant Nos. 60325208, 90604008, 60633030), 973 Program (2006CB303104), NSF of Guangdong (04205407). The authors would like to thank Prof. Hany Farid and Prof. Yun Q. Shi for providing us some sample images from their works, and Yi Situ for proofreading the paper.

References

1. Farid H. Digital doctoring: How to tell the real from the fake, Significance, 2006, 3(4):162–166
2. http://www.cs.dartmouth.edu/farid/research/digitaltampering/
3. Light K, Fonda, Kerry, Photo Fakery. The Washington Post, Saturday 28 Feb. 2004
4. Voice of the Mirror. Sorry. we were hoaxed: Iraqi PoW abuse pictures handed to us WERE fake. Daily Mirror Newspaper, 15 May 2004
5. Zhu B, Swanson M, Tewfik A. When seeing isn't believing [multimedia authentication technologies]. IEEE Signal Processing Magazine, Mar. 2004, 21(2): 40–49
6. Hartung F, Kutter M. Multimedia watermarking techniques. Proc. IEEE, July 1999, 87(7): 1079–1107
7. Ng T T, Chang S F, Lin C Y, et al. Multimedia Security Technologies for Digital Rights, chap. Passive-Blind image forensic, Elsvier, 2006
8. http://www.exif.org
9. Farid H. Digital image ballistics from jpeg quantization. Tech. Rep. TR2006-583, Department of Computer Science, Dartmouth College, 2006
10. Adams J, Parulski K, Spaulding K. Color processing in digital cameras. IEEE Micro, Nov.-Dec. 1998, 18(6): 20–30
11. Kharrazi M, Sencar H, Memon N. Blind source camera identification. In: Proceedings of ICIP'04, 24-27 Oct. 2004, 1: 709–712
12. Chang C, Lin C. LIBSVM: A library for support vector machines. Software available at:http://www.csie.ntu.edu.tw/˜cjlin/libsvm, 2001
13. Geradts Z J, Bijhold J, Kieft M, et al. Methods for identification of images acquired with digital cameras. In: SPIE Enabling Technologies for Law Enforcement and Security, 2001, 4232(1): 505–512
14. Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Trans. Information Forensics and Security, June 2006, 1(2): 205–214
15. Lukas J, Fridrich J, Goljan M. Determining digital image origin using sensor imperfections. In: Proceedings of SPIE Electronic Imaging, Image and Video Communications and Processing 2005, 2005, 5685(1): 249–260
16. Lukas J, Fridrich J, Goljan M. Digital "bullet scratches" for images. In: Processings of ICIP '05, 11-14 Sept. 2005, 3: 65–68
17. Lukas J, Fridrich J, Goljan M. Detecting digital image forgeries using sensor pattern noise. In: Processings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, 16-20 Jan. 2006, 6072(1): 60720Y
18. Swaminathan A, Wu M, Liu K J R. Non-intrusive forensic analysis of visual sensors using output images. In: Proceedings of ICASSP'06, Toulouse, France, 14-19 May 2006, 5: 401–404
19. Popescu A, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Trans. Signal Processing, 2005, 53(10): 3948–3959
20. Holst G C. CCD Arrays, Cameras, and Displays. 2nd ed. JCD Publishing & SPIE Pres, USA, 1998
21. Kurosawa K, Kuroki K, Saitoh N. Ccd fingerprint method-

identification of a video camera from videotaped images. In: Processings of ICIP'99, 24-28 Oct. 1999, 3: 537–540
22. Adams J J E. Interactions between color plane interpolation and other image processing functions in electronic photography. In: C.N. Anagnostopoulos, M.P. Lesser, eds., Proceedings of SPIE Electronic Imaging, Cameras and Systems for Electronic Photography and Scientific Imaging, 1995, 2416(1): 144–151
23. Bayram S, Sencar H, Memon N, et al. Source camera identification based on cfa interpolation. In: Proceedings of ICIP'05, 11-14 Sept. 2005, 3: 69–72
24. Swaminathan A, Wu M, Liu K J R. Component forensics of digital cameras: A non-intrusive approach. In: Proceedings of Conference on Information Sciences and Systems (CISS), Princeton, NJ, Mar. 2006, 1194–1099
25. Lyu S. Natural Image Statistics for Digital Image Forensics. Ph.D. thesis, Department of Computer Science, Dartmouth College, Hanover, NH, 2005
26. Lyu S, Farid H. How realistic is photorealistic? IEEE Trans. Signal Processing, 2005, 53(2): 845–850
27. Ng T T, Chang S F, Hsu J, et al. Physics-motivated features for distinguishing photographic images and computer graphics. In: Proceedings of ACM Multimedia, Singapore, Nov. 2005, 5: 239–248
28. Dehnie S, Sencar T H, Memon N. Digital image forensics for identifying computer generated and digital camera images. In: Proceedings of ICIP'06, Polytechnic University, 2006, 2313–2316
29. Ng T T, Chang S F, Hsu J, et al. Columbia photographic images and photorealistic computer graphics dataset. ADVENT Technical Report 205-2004-5, Columbia University, Feb. 2005
30. Ng T T, Chang S F. An online system for classifying computer graphics images from natural photographs. In: Proceedings of SPIE Electronic Imaging, USA, Jan. 2006, 6072:397–405
31. Lyu S, Rockmore D, Farid H. A digital technique for art authentication. Proc. National Academy of Sciences, 2004, 101(49): 17006–17010
32. Lyu S, Rockmore D, Farid H. Wavelet analysis for authentication, in Art+Math=X, Boulder, CO, 2005
33. Farid H, Lyu S. Higher-order wavelet statistics and their application to digital forensics. In: IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), Madison, Wisconsin, 2003
34. Wei L Y. Texture Synthesis by Fixed Neighborhood Searching. Ph.d. dissertation, Stanford University, Nov. 2001
35. Criminisi A, Perez P, Toyama K. Region filling and object removal by exemplar-based image inpainting. IEEE Trans. Image Processing, Sept. 2004, 13(9): 1200–1212
36. Bertalmio M, Sapiro G, Caselles V, et al. Image inpainting. In: Proceedings of ACM SIGGRAPH'2000, 2000, 417–424
37. Farid H. Creating and detecting doctored and virtual images: Implications to the child pornography prevention act. Technical Report TR2004-518, Department of Computer Science, Dartmouth College, 2004
38. Wallace G. The jpeg still picture compression standard. IEEE Trans. Consumer Electronics, Feb. 1992, 38(1): xviii–xxxiv
39. Fan Z, de Queiroz R.Maximum likelihood estimation of jpeg quantization table in the identification of bitmap compression history. In: Proceedings of ICIP '00, 10-13 Sept. 2000, 1: 948–951
40. Fan Z, de Queiroz R. Identification of bitmap compression history: Jpeg detection and quantizer estimation..IEEE Trans. Image Processing, Feb. 2003, 12(2): 230–235
41. Fridrich J, Goljan M, Du R. Steganalysis based on jpeg compatibility. In: Proceedings of SPIE Electronic Imaging, Multimedia Systems and Applications, 2001, 4518(1): 275–280
42. Neelamani R, Baraniuk R, de Queiroz R. Compression color space estimation of jpeg images using lattice basis reduction. In: Proceedings of ICIP '01, 7-10 Oct. 2001, 1: 890–893
43. Neelamani R, de Queiroz R, Fan Z, et al. Jpeg compression history estimation for color images. In: Proceedings of ICIP '03, 14-17 Sept. 2003, 3: 245–248
44. Neelamani R, de Queiroz R, Fan Z, et al. Jpeg compression history estimation for color images. IEEE Trans. Image Processing, June 2006, 15(6): 1365–1378
45. Lukas J, Fridrich J. Estimation of primary quantization matrix in double compressed jpeg images. In: Proceedings of DFRWS, Cleveland, OH, USA, 5-8 Aug. 2003
46. Popescu A. Statistical Tools for Digital Image Forensics. Ph.D. thesis, Department of Computer Science, Dartmouth College, Hanover, NH, 2005
47. Fu D D, Shi Y Q, Su W. A generalized Benford's law for jpeg coefficients and its applications in image forensics. In: Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, 2007 (in press), 6505: 58
48. Schaefer G, Stich M. Ucid: an uncompressed color image database. In: Proceedings of SPIE Electronic Imaging, Storage and Retrieval Methods and Applications for Multimedia, 2003, 5307(1): 472–480
49. Luo W Q, Qu Z H, Huang J W, et al. A novel method for detecting cropped and recompressed image block. In: Proceedings of ICASSP'07, 2007(in press)
50. Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. In: Processings of DFRWS, Cleveland, OH, USA, 5-8 Aug. 2003
51. Popescu A, Farid H. Exposing digital forgeries by detecting duplicated image regions, Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, 2004
52. Luo W Q, Huang J W, Qiu G P. Robust detection of region-duplication forgery in digital image. In: Proceedings of ICPR'06, 20-24 Aug. 2006, 4: 746–749
53. Ng T T, Chang S F. A model for image splicing. In: Proceedings of ICIP '04, 24-27 Oct. 2004, 2: 1169–1172
54. Ng T T, Chang S F. A data set of authentic and spliced image blocks. ADVENT Technical Report 203-2004-3, Columbia University, June 2004
55. Farid H. A picture tells a thousand lies, New Scientist, 6 Sept. 2003, 179(2411): 38–41
56. Ng T T, Chang S F, Sun Q. Blind detection of photomontage using higher order statistics. In: Proceedings of International Symposium on Circuits and Systems, 23-26 May 2004, 5: 688–691
57. Ng T T, Chang S F. Blind detection of digital photomontage using higher order statistics. ADVENT Technical Report 201-2004-1, Columbia University, June 2004
58. Johnson M, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: Proceedings of ACM the 7th workshop on Multimedia and Security Workshop, New York, NY, 2005, 1–10
59. Hsu Y F, Chang S F. Detecting image splicing using geometry invariants and camera characteristics consistency. In: Proceedings of ICME'06, Toronto, Canada, July 2006
60. Chen W, Shi Y Q, Su W. Image splicing detection using 2-d phase

congruency and statistical moments of characteristic function. In: Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, 2007(to appear), 6505: 27

61. Farid H. Detecting digital forgeries using bispectral analysis. Tech. Rep. AIM-1657, AI Lab, Massachusetts Institute of Technology, 1999
62. Ng T T, Chang S F, Tsui M P. Camera response function estimation from a single-channel image using differential invariants. ADVENT Technical Report 216-2006-2, Columbia University, Mar. 2006
63. Shi Y Q, Xuan G R, Zou D, et al. Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. In: Proceedings of ICME'05, 6-8 July 2005, 4
64. Swaminathan A, Wu M, Liu K J R. Image tampering identification using blind deconvolution. In: Proceedings of ICIP '06, Atlanta, GA, Oct. 2006, 2311–2314
65. Grossberg M, Nayar S. What is the space of camera response functions?. In: Proceedings of CVPR'03, 18-20 June 2003, 2: 602–609
66. Farid H. Blind inverse gamma correction, IEEE Trans. Image Processing, 2001, 10(10): 1428–1433
67. Lin S, Zhang L. Determining the radiometric response function from a single grayscale image. In: Proceedings of CVPR'05, 20-25 June 2005, 2: 66–73
68. Lin Z C, Wang R R, Tang X O, et al. Detecting doctored images using camera response normality and consistency. In: Proceedings of CVPR'05, 20-25 June 2005, 1: 1087–1092
69. Johnson M, Farid H. Exposing digital forgeries through chromatic aberration. In: Proceedings of ACM the 8th workshop on Multimedia and Security Workshop, Geneva, Switzerland, 2006, 48–55
70. Willson R, Shafer S. What is the center of the image? In: Proceedings of CVPR'93, 15-17 June 1993, 670–671
71. Popescu A, Farid H. Statistical tools for digital forensics. In: 6th International Workshop on Information Hiding, Toronto, Canada, May 2004, 3200: 128–147
72. Popescu A, Farid H. Exposing digital forgeries by detecting traces of re-sampling. IEEE Trans. Signal Processing, 2005, 53(2): 758–767
73. Wang W, Farid H. Exposing digital forgeries in video by detecting double mpeg compression. In: Proceedings of ACM the 8th workshop on Multimedia and Security Workshop, Geneva, Switzerland, 2006, 37–47
74. Farid H. Exposing digital forgeries in scientific images. In: Proceedings of ACM the 8th workshop on Multimedia and Security Workshop, Geneva, Switzerland, 2006, 29–36
75. Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In: Proceedings of ICIP'04, 24-27 Oct. 2004, 4: 2645–2648
76. Johnson M, Farid H. Metric measurements on a plane from a single image. Technical Report TR2006-579, Department of Computer Science, Dartmouth College, 2006