A Survey of Passive Image Tampering Detection

Wei Wang, Jing Dong, and Tieniu Tan

National Laboratory of Pattern Recognition,
Institute of Automation, Chinese Academy of Sciences,
P.O. Box 2728, Beijing, P.R. China, 100190
{wwang,jdong,tnt}@nlpr.ia.ac.cn

Abstract. Digital images can be easily tampered with image editing tools. The detection of tampering operations is of great importance. Passive digital image tampering detection aims at verifying the authenticity of digital images without any a prior knowledge on the original images. There are various methods proposed in this filed in recent years. In this paper, we present an overview of these methods in three levels, that is low level, middle level, and high level in semantic sense. The main ideas of the proposed approaches at each level are described in detail, and some comments are given.

Keywords: Image Tampering, Image Tampering Detection, Imaging Process, Image Model.

1 Introduction

Traditionally, a photograph implies the truth of what has happened. However, in today's digital age, sometimes seeing is no longer believing, since our modern life is full of digital images and (maliciously) tampering these digital images is easy and simple by using digital processing tools which are widely available (*e.g. Photoshop*). Many tampered images emerge in news items, scientific experiments and even legal evidences. Therefore, we cannot take the authenticities of images for granted any more. The tools and techniques that can detect image tampering are highly desirable. Although digital watermarking can be used as a tool to provide authenticity to image, like [1,2], it is a fact that most of images that are captured today do not contain digital watermarks. And this situation is likely to continue for the foreseeable future [3]. Furthermore, the effectiveness and robustness of digital watermark for image tampering detection are not testified yet and the third-party is also needed to license watermarks. Hence, passive image tampering detection is more practical and more important. It aims at verifying the authenticity of digital images without any a prior knowledge, like embedding watermarks in original images. In recent years, more and more researchers focus on image tampering detection, especially on passive methods.

Image tampering detection is a branch of image forensics which aims at assessing the authenticity and the origin of images. The tasks of image forensics can be divided into the following six categories: source classification, device linking, processing history recovery, forgery detection and anomaly investigation

A.T.S. Ho et al. (Eds.): IWDW 2009, LNCS 5703, pp. 308–322, 2009.

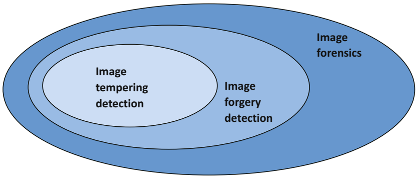

Fig. 1. The relationship among image tampering detection, forgery detection and forensics

[4]. The relationship among (image) tampering detection, forgery detection and forensics can be illustrated in Figure 1. In our opinion, tampering image only means modifying the actual image (either from digital camera, or film camera and then digitally scanned). However, apart from that, forging image also includes computer-generated realistic images.

The past few years have seen a growth of research on passive digital image tampering detection which can be categorized at three levels (similar to those mentioned in [5]):

1. **Low Level.** Methods at this level use statistical characteristics of digital image pixels or DCT coefficients. For example, demosaicing or gamma correction during the image acquiring process will bring consistent correlations of adjacent pixels, whereas tampering will break up this consistency. Investigating double JPEG compression for tampering detection is an example of using statistical characteristics of DCT coefficients. Using a model of authentic images which tampered images do not satisfy for tampering detection also belongs to this level. In short, no semantic information is employed at this level.
2. **Middle Level.** At this level, we detect the trace of tampering operation which has some simple semantic information, like splicing[1] caused sharp edges, blur operation after splicing and inconsistencies of lighting direction, etc.
3. **High Level**, i.e., semantic level. Actually, it is very hard for computer to use semantic information to do tampering detection because the aim of tampering is changing the meaning of image content it originally conveyed. But, sometimes it still works. For example, it does not make sense to have an image in which George W. Bush is shaking hands with Osama bin Laden.

As we know, at least in recent years, computers still have difficulties in high level image analysis. Nevertheless, they can be helpful in middle level and low level analysis. Actually, they are better than human at these two levels [5]. In this paper, we will give an overview of state-of-the-art passive digital image tampering detection techniques. The rest of this paper is organized as follows. In Section 2, we briefly introduce image tampering operation. It is followed by an overview of low level image tampering detection in Section 3 and middle level in Section 4. Finally, our conclusions and discussion will be given in Section 5.

[1] Splicing is defined as a simple cut-and-paste operation of image regions from one image onto the same or another image without performing post-processing.

2 Image Tampering

To detect image tampering, we should know about image tampering operation itself first. In [6], the author divided digital forgery operation into six different categories: compositing, morphing, re-touching, enhancing, computer generating and painting.

In fact, almost all state-of-the-art tampering detection technique aims at compositing operation. With powerful image editing tool (*e.g. Photoshop or lazy snapping* [7]), compositing tampered images is much easier and can result in much more realistic images. It always involves the selection, transformation, composition of the image fragments and the retouching of the final image [8]. Here, we want to emphasize that a tampered image means part of the content of a real image is altered. This concept does not include those wholly synthesized images, e.g. images completely rendered by computer graphics or by texture synthesis. In other words, an image is tampered implies that it must contain two parts: the authentic part and the tampered part [9]. All the algorithms introduced later focus on the tampered images defined here.

3 Low Level Digital Image Tampering Detection

Just like the roles of steganography and steganalysis, tampering creators and detectors are opponents. Since it is not hard to use digital image edit tool to make a sophisticated tampered image, which means less trace of tampering operation can be seen from content of the tampered image, many tempering detection algorithms have to focus on imaging process and image statistical characteristics.

3.1 Detection Based on Imaging Process

As we known, a consumer level digital camera consists of a lens system, sampling filters, color filter array, imaging sensor, color interpolation and post-processor as shown in Figure 2 [10]. The lens system collects and controls the light from the scene. It is essentially composed of a lens and the mechanisms to control exposure, focusing, and image stabilization. The light is then focused onto imaging sensor (CCD or CMOS). Because each imaging sensor element is essentially monochromatic, capturing color images requires separate sensors for each color component. However, due to cost considerations, in most digital cameras, only a single sensor is used along with a color filter array (CFA). The CFA arranges pixels in a pattern so that each element has a different spectral filter. Hence, each element only senses one band of wavelength, and the raw image collected from the imaging sensor is a mosaic of different colors. The missing color values for each pixel need to be obtained through color interpolation (demosaicing) operation. The last part of digital camera is post processing like white point correction, image sharpening, aperture correction, gamma correction and compression. The processing in each stage varies from one manufacturer to the other, and even in different camera models manufactured by the same company [3].

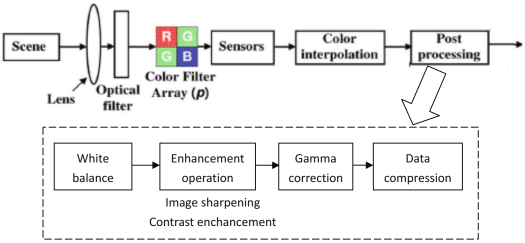

Fig. 2. CCD camera imaging pipeline

As we mentioned above, only one third of the samples in a color images are captured by the camera. The other two thirds are interpolated using color interpolation (demosaicing). This interpolation introduces specific correlations among adjacent pixels of a color image. When tampering a digital image, these correlations may be destroyed or altered. *Popescu* and *Farid* [11] proposed a method based on this judgement. Since the color filters in a CFA are arranged in a periodic pattern, these correlations are periodic. The authors first modeled this interpolated operation linearly. Then, expectation-maximization (EM) algorithm was employed to estimate the probability of pixel being linearly correlated to its neighbors. Finally, the similarity between the probability map of a whole image (or selected window) and corresponding synthetic probability map was calculated to measure the periodic correlations. If the similarity was below a specified threshold, no periodic pattern was assumed to be present in the probability map (i.e. the image region was tampered). In this paper, the authors did some experiments on well-designed images and images acquired from three commercially digital cameras. All the results were promising for non-CFA interpolation detection. The detection method was robust to some operations, like JPEG compression, additive noise, or luminance nonlinearities, to some extent. However, there are some problems such as those listed as follows:

1. Tampered images composed by images from different digital cameras are not tested in their experiment. They have different CFA interpolated regions instead of some CFA interpolated and some non-CFA interpolated regions. Maybe we can expect that the windows including different regions using different interpolation algorithms are lack of the period.
2. If a tampered image is resampled onto a CFA and then reinterpolated, this method will fail. This was also mentioned in the paper, but the authors argued that it required knowledge of the camera's CFA pattern and interpolation algorithm which may be beyond the reach of a novice forger. However, in our opinion, it is harder for detector to achieve it.

To make tampered image more imperceptible, resizing, rotating and stretching are often involved. Although these resampling operations are often imperceptible, they introduce specific correlations into the image. They can be used for tampering detection. Hence, the same authors proposed another approach to detect image tampering based on detecting traces of resampling [12,13]. They used the similar method as that mentioned above to detect the periodic correlations in resampled regions of a tampered image. However, there is a problem. If an authentic image is globally resized with no image content changing, this method will also detect it as tampered image. Besides, other un-resampled parts of the tampered image still have periodic correlations coming from CFA interpolation. Why this method did not detect these regions as having periodic correlations? We think it is because the periodic correlations introduced by resampling and those caused by CFA interpolating are different. In other words, the similarities between a set of synthetic probability maps, which are generated by different resampling parameters, and these CFA interpolated (un-resampled) regions should be quite low so that they can not be detected as resampling regions. Comparing these two techniques, we can find that they seem to be contradictory. One is detect the periodic correlations in resampled regions of a tampered image and the other is detect the lack of periodic correlations in tampered image. Actually, as we just said, the periodic patterns of these two kinds of correlations are different. This may be testified by the similarity between the synthetic probability maps used in these two methods. The similarity score should be very low, if we calculate.

Mahdian and *Saic* [14] also used periodic properties of interpolation caused by resampling for tampering detection. The periodic property of nth derivative (or its variance) of the interpolated signal was demonstrated in this paper. The tampering detection method proposed in this paper was based on a few main steps: ROI selection, signal derivative computation, radon transformation, and searching for periodicity. The detection performance decreased as the order of interpolation polynomial increased, hence, CFA interpolation (most are high order interpolation) were hardly detected by this method. In [15], the authors mentioned that this method was more difficult to detect as each interpolated sample value was obtained as a function of more samples. Furthermore, it also had weak results when the interpolated images were altered by further operations like noise addition, linear or median filtering. In fact, this method has the same problem as [12] has. Noise inconsistency was also used as a clue of tampering occurring [15]. Technique for estimating the variance of the noise on a wavelet component was employed.

Johnson and *Farid* [16] proposed another new approach by inspecting inconsistencies in lateral chromatic aberration as a sign of tampering. Lateral chromatic aberration results from the failure of an optical system to perfectly focus light of different wavelengths. Suppose the positions of short wavelength and long wavelength lighting on the sensor are (x_r, y_r) and (x_b, y_b). Image tampering will lead to inconsistencies in the lateral chromatic aberration, i.e. $(x_r - x_b, y_r - y_b)$. Hence, given an image, the aberration can be estimated from the entire image first, then compare it with estimates from small blocks. Any block that deviates significantly from the global estimate is suspected of having been tampered. The reported experiment results were promising, but for the forensics experiment in their paper, they did not test authentic images. Hence, we do not know about the false alarm rate (the probability of authentic image being detected as tampered image). Besides, this experiment is based on two assumption: only a small portion of an image can be tampered and tampering operation will not significantly affect a global estimate [16].

Inconsistencies of the response function of the camera are used in [5] for tampering detection. *Lin et al.* proposed an approach that computed the response function of the camera by (manual) selecting appropriate patches in different ways. The camera response function is the mapping relationship between the pixel irradiance and the pixel value. The irradiance of the pixel on the edge should be a linear combination of those of the pixels clear off the edges [5]. The linear relationship beaks up among the pixel values because of nonlinear response of the camera. Usually, the camera response function is monotonically increasing with no more than one inflexion point. The response functions of R, G, and B channels are close to each other. Hence, the inverse camera response function, which can recover the linear relationship around edges, is also obey this rules. The features that can reflect these three rules were calculated from each normal or abnormal patch (from tampered part of image) and SVM classifier was used to train to get an effective model in [5]. If the image is tampered, some inverse response functions of the patches along the synthesis edges will become abnormal. However, the author also mentioned that their approach might fail if the component images were captured by the same camera and these components were not synthesized along object edges.

Besides inconsistencies, the absence of some camera intrinsic characteristics can also be used for tampering detection. *Lukáš et al.* [17] used sensor pattern noise to detect digital image forgeries. This method was based on detecting the presence of the camera pattern noise in individual regions in the image. It is a unique stochastic characteristic of imaging sensors. The tampered region was the one that lacks of the pattern noise. This method is only applicable when the tampered image is claimed to have been taken by a known camera or at least, we have other images taken by the camera. In this method, first the camera reference pattern noise was obtained. Then, for a given image, noise residuals and the correlations between noise residuals and camera reference pattern were calculated. Finally, hypothesis testing was used to determining whether the selected regions were tampered or not. Two approaches were proposed in their paper: the user selecting a suspicious area for detecting and automatically searching the tampering area. Lossy compression or filtering can influence the accuracy. *Chen et al* [18] detailed and improved this approach with rigorous mathematical derivation. The detection results are very good. Actually, this approach is device identification mentioned in Section 1. Similarly, *Swaminathan et al.* thought the absence of camera-imposed fingerprints (in-camera and postcamera fingerprints) from a test image indicated that the test image was not a camera output and was possibly generated by other image production processes. Any change or inconsistencies among the estimated in-camera fingerprints, or the presence of new types of postcamera fingerprints suggested that the image has undergone some kinds of processing after the initial capture, such as tampering or steganographic embedding [10]. In-camera fingerprints were estimated using the method mentioned in

[19]. All manipulation operations were considered as filtering. The coefficients of this manipulation filter served as postcamera fingerprints were estimated using blind deconvolution. For a given image, the manipulation filter coefficients were first obtain, and then similarity score between these coefficients and reference pattern was calculated. Finally, threshold was employed to give a decision. This was for global manipulation detection. To locate tampered regions, the authors suggested to divide a test image into several overlapping blocks and estimate the color interpolation coefficients [20] in each block. The k-means clustering algorithm was then employed to cluster these features into two classes. The detection result was satisfying. However, if the test image is composed of more than two kind of camera captured authentic images, clustering two classes will be not reasonable.

Due to JPEG compression is the last step of most digital image devices, both the original and tampered images are possibly stored in this format. Therefore, checking wether a given image having undergone double JPEG compression will be a good method for tampering detection [13]. *Popescu* and *Farid* found that Fourier transforms of DCT histograms of tampered image (with double JPEG compression) had high frequency peaks. *Fu et al.* [21] presented a novel statistical model based on the generalized Benford's to detect double compressed JPEG image. *Luo et al.* [22] designed a blocking artifact characteristics matrix (BACM) and showed that the original JPEG images's BACM exhibited regular symmetrical shape, but for images that were cropped from another JPEG image and resaved as JPEG images, the regular symmetrical property of the BACM was destroyed. Experiments using real tampered images are needed in this method.

However, We should note that the evidence of double JPEG compression does mean tampering occurring. For example, it is possible for a user to simply resave a high quality JPEG image with a lower quality [13]. But if we check the inconsistencies of double JPEG compression image, in other worlds, some regions in the image undergoing twice JPEG compressing and the others undergoing only once or twice compressing with different quality factor, the tampering operation may be detected. Some algorithms checking these inconsistencies are introduced as follows.

Ye et al. believed that when creating a tampered digital image, the resulted image might inherit different kind of compression artifacts from different sources. Hence, these inconsistencies could be used to check image integrity [23]. In their method, suspicious area was selected for evaluation, the other areas were used to estimate the quantization table, and then block artifact measure (BAM) of the image was calculated based on the estimated table. So if blocking inconsistencies are detected, the image will be deemed as suspicious. The block artifact of each block was used to tell where the tampered areas are (high value means high suspicion). *Farid* proposed a technique to detect whether a part of an image was initially compressed at a lower quality than the rest of the image [24]. In his paper, a test image's central region was recompressed at JPEG quality Q_1 lower than its original JPEG quality Q_0. Then it was resaved at various qualities Q_2.

The normalized difference image was calculated as a function of Q_2. The K-S statistic was used to compute the statistical difference between the testing image's central region and the rest of the image. If the K-S statistic for any quality Q_2 exceeded a specified threshold, the image would be classified as manipulated. For an actual tampered image, we can divide the image into several blocks. If the K-S statistic for any quality in any block exceeds the threshold, the image will be classified as tampered image, and the block whose K-S statistic exceeds the threshold will be classified as tampered block.

He et al. [9] proposed a method under an assumption that both tampered and authentic part of a tampered image undergo double JPEG compression. They found that the DCT coefficient histograms of the authentic part had double quantization (DQ) effect (periodic pattern of peaks and valleys), but the histograms of tampered part did not have DQ effects. They thought there were several reasons: the first was that the tampered part might cut from other lossless images; the second was that the DCT grid of the tampered part might mismatch with that of the authentic part; and the third was that $8 * 8$ blocks along the boundary of the tampered part consisted of pixels both from tampered part authentic part. In their paper, for a given image, the periods of the DCT coefficient histograms were firstly calculated. Next, the posteriori probability of a given bin being a tampered block or an authentic block was calculated. And then, a normality map of blocks of image was obtained. Finally, features were extracted from this map using clustering result, and SVM classifier was employed to train and predict. If a test image is detected as tampered one, those blocks whose normalities are below threshold should be considered as tampered ones. The examples shown in the paper were all successfully detected. This method is an excellent working method.

3.2 Detection Based on Image Model

As we know, natural scene images should occupy a highly regularized subspace in the entire image space, and random pixel images take up the rest of the space [8]. If the distribution of the natural scene images is deterministic and fully known, the tampered image is easy to find. However, tampered image creators can also know this distribution, and then they will make a tampered image obeying it so that disable the tampering detection methods using this distribution. Luckily, it is difficult to achieve such perfect distribution. Without a complete model for the natural scene images, the knowledge of the opponent's technique would become a great advantage [8]. Instead of preventing image tampering creators from having a full knowledge of the detection algorithms, the image tampering detectors should make an effort to master image tampering creation process and find some clues to design detection algorithms. In this approach, we need to design a set of features that are sensitive to image tampering and use it to train a model with machine learning algorithms, and then employ this model for predicting the category of a testing image.

Farid and *Lyu* [25] described a statistical model for natural images that is built upon a multi-scale wavelet decomposition. The model consists of first-and higher-order statistics that capture certain statistical regularities of natural images. The image decomposition was based on separable quadrature mirror filters (QMFs). The statistical moments, mean, variance, skewness and kurtosis, of the subband coefficients at each orientation and scale and those of the log error between the actual coefficients and predicted coefficients were combined to form a feature vector of "natural image". In their paper, this image model's effectiveness in steganalysis, distinguishing computer graphics and photograph and classifying live and re-broadcast images were testified by high detection accuracies. However, it was not proofed in tampering detection. In our opinion, it may still work to detection tampering, but only can tell whether a given image is tampered or not. Tampered areas cannot be located with this method. *Bayra et al.* [26] developed several single tools to detect the tampering operation first, and then fused these "weak" detectors together to detect tampering. The feature vectors BSM [27], IQM [28], and HOW [29], which were initially proposed for steganalysis, were used in this paper. In the feature selection process, sequential forward floating search (SFFS) was employed to create a core feature set. *Shi et al.* [30] believed that on one hand, steganography and splicing had different goals and strategies causing different statistical artifacts on images, on the other hand, both of them made the touched (stego and spliced) image different from corresponding original ones. Therefore, they built a natural image model using the features including statistical moments of characteristic functions and Markov transition probabilities from image 2-D array and multi-size block discrete cosine transform 2-D array. A similar approach was proposed in [31]. All the ideas of the methods mentioned above are borrowed from steganalysis. However, how to use such models to distinguish tampered images from stego ones may be a problem.

In the frequency domain, a "natural" signal has weak higher-order statistical correlations. Some "un-natural" correlations will be introduced if this signal is passed through a non-linearity (which would almost surely occur in tampering) [32]. Based on this, *Ng et al.* [33] studied the effects of image splicing on magnitude and phase characteristics of bicoherence (the normalized bispectrum). The difference between means of magnitudes of a test image's bicoherence and its estimating authentic vision's bicoherence and the difference between negative phase entropy of those two were used as features. The classification accuracy was about 63%. The best performance was 71% when these features and edge pixel percentage feature were combined. Theoretical justification for this approach was proposed in [34].

3.3 Other Low Level Image Tampering Detection Algorithms

Although duplicated regions of tampered image can be detected by some of the algorithms mentioned above, there are several targeted techniques for detecting them. Copy-move is a specific type of image tampering, where a part of the image is copied and pasted on another part of the same image. A correlation between the original image part and the pasted one were introduced by copy-move. This correlation can be used as a clue for a detection of this type of tampering [35].

Fridrich et al. [35] chose a block with $B * B$ pixels first, and then slid it by one pixel along row and column. Arriving at each new position, the block values were turned into row vector and stored it into the row of matrix A. The rows of the matrix A were lexicographically ordered. The matching rows were easily searched by going through all rows of the ordered matrix A. For robust matching, quantized DCT coefficients of image were used. *Popescu* and *Farid* [36] applied a principal component analysis (PCA) on small fixed-size image blocks to yield a reduced dimension representation. This representation was robust to minor variations in the image due to additive noise or lossy compression. Similar to [35], duplicated regions were then detected by lexicographically sorting all of the image blocks. The detection accuracy was very good except for the situation that the block sizes are small and the image undergos low JPEG qualities after tampering. *Bayram et al.* [37] proposed to extract features from the image blocks by using Fourier-Mellin Transform. The authors thought these features were not only robust to lossy JPEG compression, blurring, or noise addition, but also to scaling and translation invariant. Both lexicographic sorting method and counting bloom filters were implemented in their paper. Actually, because of using hash function, counting bloom filters can only detected the duplicated blocks which are exactly same.

In fact, using these methods to detect duplicate regions, some flat, uniform areas, such as the sky, may lead to false matches. Furthermore, the more robust the algorithm is, the higher probability of this false matching is.

4 Middle Level Digital Image Tampering Detection

As we know, some image tampering operation will leave some semantic cues that can be used for us to detect tampering, such as splicing caused edges which are sharper and less smooth than other original edges in image. And sometimes there are inconsistencies of lighting direction in the composited image. In this section, we will introduce some techniques that utilize these semantic clues to detect tampering.

Chen et al. [38] thought that spliced image may introduce a number of sharp transitions such as lines, edges and corners. Phase congruency, which had been known as a sensitive measure of these sharp transitions, were used as features for splicing detection. In addition, statistical moments of characteristic functions of wavelet subbands were also employed. Consequently, the proposed scheme extracted image features from 2-D phase congruency and wavelet characteristic functions of image and its predict-error image. Though the experiment results are not bad, feature extraction is time consuming. Actually, both low level and middle level features are used in this method.

Blurring is a very common process in digital image tampering. It could be used to conceal the influence caused by splicing or to remove unwanted defects. Hence, if a suspectable blurring operation is detected in a image, we may say that it may undergo tampering operation. *Hsiao et al.* [39] proposed local blur estimation method. Firstly, a quality factor of blur percentage of whole image was quantified, and then a mapping function between it and threshold (which will be used for determine which parts of image are blurry) was estimated. Therefore, given an image, we can estimate its quality factor first, and then use the mapping function to calculate the threshold. Finally with this threshold we can tell which part of the image is blurry. We should note that there are also blurry parts of authentic image, hence this method cannot provide direct answer to the tampered area. However, if there are blurred regions appearing oddly in focused regions, we should highly doubt these regions [39].

In [40], *Johnson* and *Farid* considered the use of light source direction inconsistencies across an image to detect image tampering. The light source direction was estimated from a given image. Surfaces of known geometry (e.g., plane, sphere, cylinder, etc.) in the image were manually partitioned into approximately eight small patches first, and next three points near the occluding boundary were selected for each patch and fitted with a quadratic curve. And then, the surface normals of each patch were estimated from these curves. Finally, the infinite light source (local and multiple light source can be considered as a single virtual light source) direction was estimated from the surface normals. Hence, if there is inconsistencies of light direction in an image, it will be regard as tampered image. However, there is a restriction in this method, i.e., we should select the patches manually. Another problem is when pictures of both the original and tampered objects were taken under similar lighting or non-directional lighting conditions, the method does not work. The authors proposed another approach [41] which was appropriate in more complex lighting environments containing multiple light sources or non-directional lighting (e.g., the sky on a cloudy day). An arbitrary lighting environment was expressed as a non-negative function on the sphere to make the estimation of the coefficients of lighting environment easy. For tampering detection, an error measure between estimated lighting environments of two different objects in an image was computed. If the error is larger than the threshold, the image will be detected as tampered one. Similarly, they proposed a method to detect tampering through specular highlights on the eye because they were a powerful cue to the shape, color and location of the light source [42]. The known geometry of the eye was exploited to estimate the camera calibration parameters. Then the surface normal of eye and camera view direction were calculated so that the light source direction was worked out.

5 Discussions and Conclusions

There is a growing need for digital image tampering detection. Many techniques, some of which were introduced in this paper, have been proposed to address various aspects of digital image tampering detection. From this survey, we can find that most proposed tampering detection methods aim at detecting inconsistencies in an image, and the majority of them belong to the low level category. Although many of these techniques are very promising and innovative, they have limitations and none of them by itself offers a definitive solution [43].

Actually, with growing attention, image tampering detection encounters some attacks. A targeted attack is a method that avoids traces detectable with one particular forensic technique which the developer of the attack usually knows. *Kirchner* and *Bohme* [44] aimed at attacking against a specific technique to detect trace of resampling in uncompressed images proposed by *Popescu* and *Farid* [12]. They proposed three types of attacks in their paper. Conversely, universal attacks try to maintain or correct as many statistical properties of the image as possible to conceal manipulation even when presented to unknown forensic tools. In this sense, a low quality JPEG compression of tampered images can be interpreted as universal attack [44]. Forensic and counter-forensic techniques play a cat-and-mouse role. Thereby we can believe that such competition is mutually beneficial.

Therefore, we can hope that as more detection tools are developed it will become increasingly more difficult to create convincing tampered digital images. Besides, as the suit of detection tools expands we believe that it will become increasingly harder to target attack each of the detection schemes [13]. However, there are several issues requiring attention when we want to propose new approaches.

1. **Public Image Database and Performance Evaluation**. With more and more tampering detection algorithms being proposed, performance comparison cannot be ignored. Consequently, public image database is urgently needed and it should cover as many kinds of authentic images and diverse tampering manners as possible. The only one public image set [45] is for splicing detection and is a little bit simple. In addition, criteria are required when we compare performances of different algorithms, like ROC curves and location accuracy of tampered region.
2. **Usability.** Many proposed approaches can only detect some kinds of tampering operations. Furthermore, some of them are tested on well-designed tampered images. If we expect image tampering detection techniques to be of practical importance, usability can not be ignored.
3. **Detection Strategy.** There are several techniques based on checking whether some parts of an image undergo some operations that may occur in image tampering. But it will cause some problems. For example, if an authentic image undergoes global scaling or blurring, but image content does not change, these techniques will also consider the authentic image as tampered. Hence, checking inconsistencies of some statistical characteristics of an image for tampering detection is a wise choice.

As image tampering detection is just at its infancy stage, there is still much work to be done and some ideas can be borrowed from other research areas, like techniques developed for camera identification. Also, knowledges from computer vision, signal processing, computer graphics, pattern recognition and imaging process will be needed for further analysis [8].

Acknowledgments. The work presented in this paper was supported by Nature Science Foundation of China (Grant No.60603011).

References

1. Kundur, D., Hatzinakos, D.: Digital watermarking for telltale tamper proofing andauthentication. Proceedings of the IEEE 87(7), 1167–1180 (1999)
2. Rey, C., Dugelay, J.: A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing 2002(6), 613–621 (2002)
3. Sencar, H.T., Memon, N.: Overview of state-of-the-art in digital image forensics, part of indian statistical institute platinum jubilee monograph series titled 'statistical science and interdisciplinary research (2008)
4. Chen, M., Fridrich, J., Goljan, M., Lukas, J.: Determining image origin and integrity using sensor noise. IEEE Transactions on Information Forensics and Security 3(1), 74–90 (2008)
5. Lin, Z., Wang, R., Tang, X., Shum, H.Y.: Detecting doctored images using camera response normality and consistency. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 1087–1092 (2005)
6. 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)
7. Li, Y., Sun, J., Tang, C., Shum, H.: Lazy snapping. In: International Conference on Computer Graphics and Interactive Techniques, pp. 303–308. ACM, New York (2004)
8. Ng, T.T., Chang, S.F., Lin, C.Y., Sun, Q.: Passive-blind image forensics. In: Multimedia Security Technologies for Digital Rights Management. Elsevier, Amsterdam (2006)
9. He, J., Lin, Z., Wang, L., Tang, X.: Detecting doctored JPEG images via DCT coefficient analysis. In: Leonardis, A., Bischof, H., Pinz, A. (eds.) ECCV 2006. LNCS, vol. 3953, pp. 423–435. Springer, Heidelberg (2006)
10. Swaminathan, A., Wu, M., Liu, K.: Digital image forensics via intrinsic fingerprints. IEEE Trans. Info. Forensics and Security 3(1), 101–117 (2008)
11. Popescu, A., Farid, H.: Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing 53(10), 3948–3959 (2005)
12. Popescu, A., Farid, H.: Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on Signal Processing 53(2), 758–767 (2005)
13. Popescu, A., Farid, H.: Statistical tools for digital forensics. In: 6th International Workshop on Information Hiding, pp. 128–147. Springer, Heidelberg (2004)
14. Mahdian, B., Saic, S.: Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security 3(3), 529–538 (2008)
15. Mahdian, B., Saic, S.: Detection and description of geometrically transformed digital images. In: Proc. SPIE, Media Forensics and Security, vol. 7254, pp. 72540J–72548J (2009)
16. Johnson, M., Farid, H.: Exposing digital forgeries through chromatic aberration. In: Proceedings of the 8th workshop on Multimedia and security, pp. 48–55. ACM, New York (2006)
17. Lukáš, J., Fridrich, J., Goljan, M.: Detecting digital image forgeries using sensor pattern noise. In: Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 6072, pp. 362–372 (2006)
18. Chen, M., Fridrich, J., Goljan, M., Lukas, J.: Determining image origin and integrity using sensor noise. IEEE Transactions on Information Forensics and Security 3(1), 74–90 (2008)

19. Swaminathan, A., Wu, M., Liu, K.: Non-intrusive component forensics of visual sensors using output images. IEEE Transactions on Information Forensics and Security 2(1), 91–106 (2007)
20. Swaminathan, A., Wu, M., Liu, K.: Component forensics of digital cameras: A non-intrusive approach. In: Annual Conference on Information Sciences and Systems, pp. 1194–1199 (2006)
21. Fu, D., Shi, Y., Su, W., et al.: A generalized Benford's law for JPEG coefficients and its applications in image forensics. In: Proc. of SPIE Security, Steganography, and Watermarking of Multimedia Contents., vol. 6505, pp. 47–58 (2007)
22. Luo, W., Qu, Z., Huang, J., Qiu, G.: A novel method for detecting cropped and recompressed image block. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), vol. 2, pp. 217–220 (2007)
23. Ye, S., Sun, Q., Chang, E.: Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In: IEEE International Conference on Multimedia and Expo, pp. 12–15 (2007)
24. Farid, H.: Exposing digital forgeries form jpeg ghosts. IEEE transactions on information forensics and security 4(1), 154–160 (2009)
25. Farid, H., Lyu, S.: Higher-order wavelet statistics and their application to digital forensics. In: IEEE Conference on Computer Vision and Pattern Recognition Workshop (2003)
26. Bayram, S., Avcıbaş, İ., Sankur, B., Memon, N.: Image manipulation detection. Journal of Electronic Imaging 15(4), 1–17 (2006)
27. Avcibas, I., Memon, N., Sankur, B.: Steganalysis using image quality metrics. IEEE transactions on Image Processing 12(2), 221–229 (2003)
28. Avcibas, I.: Image steganalysis with binary similarity measures. EURASIP Journal on Applied Signal Processing 2005(17), 2749–2757 (2005)
29. Lyu, S., Farid, H.: Steganalysis using higher-order image statistics. IEEE Transactions on Information Forensics and Security 1(1), 111–119 (2006)
30. Shi, Y.Q., Chen, C.-H., Xuan, G., Su, W.: Steganalysis versus splicing detection. In: Shi, Y.Q., Kim, H.-J., Katzenbeisser, S. (eds.) IWDW 2007. LNCS, vol. 5041, pp. 158–172. Springer, Heidelberg (2008)
31. Shi, Y., Chen, C., Chen, W.: A natural image model approach to splicing detection. In: Proceedings of the 9th workshop on Multimedia & security, pp. 51–62. ACM Press, New York (2007)
32. Farid, H.: Detecting digital forgeries using bispectral analysis. Technical report, MIT AI Memo AIM-1657, MIT (1999)
33. Ng, T.T., Chang, S.F., Sun, Q.: Blind detection of photomontage using higher order statistics. In: IEEE International Symposium on Circuits and Systems, vol. 5, pp. 688–691 (2004)
34. Ng, T.T., Chang, S.F.: A model for image splicing. In: IEEE International Conference on Image Processing, vol. 2, pp. 1169–1172 (2004)
35. Fridrich, J., Soukal, D., Lukas, J.: Detection of copy-move forgery in digital images. In: Digital Forensic Research Workshop (2003)
36. Popescu, A., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. Technical report, Department of Computer Science, Dartmouth College
37. Bayram, S., Sencar, H.T., Memon, N.: An efficient and robust method for detecting copy-move forgery. In: IEEE International Conference on Acoustics, Speech, and Signal Processing. (2009)

38. Chen, W., Shi, Y., Su, W.: Image splicing detection using 2-d phase congruency and statistical moments of characteristic function. In: Security, Steganography and Watermarking of Multimedia Contents IX, Proceeding. of SPIE, San Jose, CA, USA (2007)
39. Hsiao, D., Pei, S.: Detecting digital tampering by blur estimation. In: International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 264–278 (2005)
40. Johnson, M., Farid, H.: Exposing digital forgeries by detecting inconsistencies in lighting. In: Proceedings of the workshop on Multimedia and security, pp. 1–10 (2005)
41. Johnson, M., Farid, H.: Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security 2(3), 450–461 (2007)
42. Johnson, M., Farid, H.: Exposing digital forgeries through specular highlights on the eye. In: International Workshop on Information Hiding (2007)
43. Gloe, T., Kirchner, M., Winkler, A., Böhme, R.: Can we trust digital image forensics? In: Proceedings of the 15th international conference on Multimedia, pp. 78–86. ACM, New York (2007)
44. Kirchner, M., Bohme, R.: Tamper hiding: Defeating image forensics. In: Furon, T., Cayre, F., Doërr, G., Bas, P. (eds.) IH 2007. LNCS, vol. 4567, pp. 326–341. Springer, Heidelberg (2008)
45. Ng, T., Chang, S., Sun, Q.: A data set of authentic and spliced image blocks. Technical report, DVMM, Columbia University (2004), http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm