Hindawi Publishing Corporation
ISRN Signal Processing
Volume 2013, Article ID 496701, 22 pages
http://dx.doi.org/10.1155/2013/496701

*Review Article*

# An Overview on Image Forensics

**Alessandro Piva**

*Department of Electronics and Telecommunications, University of Florence, Via S. Marta 3, 50139 Firenze, Italy*

Correspondence should be addressed to Alessandro Piva; alessandro.piva@unifi.it

Received 6 November 2012; Accepted 26 November 2012

Academic Editors: L. Fan and S. Kwong



The aim of this survey is to provide a comprehensive overview of the state of the art in the area of image forensics. These techniques have been designed to identify the source of a digital image or to determine whether the content is authentic or modified, without the knowledge of any prior information about the image under analysis (and thus are defined as passive). All these tools work by detecting the presence, the absence, or the incongruence of some traces intrinsically tied to the digital image by the acquisition device and by any other operation after its creation. The paper has been organized by classifying the tools according to the position in the history of the digital image in which the relative footprint is left: acquisition-based methods, coding-based methods, and editing-based schemes.

## 1. Introduction

Images, unlike text, represent an effective and natural communication media for humans, due to their immediacy and the easy way to understand the image content. Historically and traditionally, there has been confidence in the integrity of visual data, such that a picture printed in a newspaper is commonly accepted as a certification of the truthfulness of the news, or video surveillance recordings are proposed as probationary material in front of a court of law.

With the rapid diffusion of inexpensive and easy to use devices that enable the acquisition of visual data, almost everybody has today the possibility of recording, storing, and sharing a large amount of digital images. At the same time, the large availability of image editing software tools makes extremely simple to alter the content of the images, or to create new ones, so that the possibility of tampering and counterfeiting visual content is no more restricted to experts. Finally, current software allows to create photorealistic computer graphics that viewers can find indistinguishable from photographic images [1, 2] or also generate hybrid generated visual content.

In summary, today a visual digital object might go during its lifetime, from its acquisition to its fruition, through several processing stages, aimed at enhancing the quality, creating new content by mixing pre existing material, or even tampering with the content. As a consequence of all previous facts, doctored images are appearing with a growing frequency in different application fields, and thus today's digital technology has begun to erode the trust on visual content, so that apparently "seeing is no longer believing" [3–5]. All these issues will get worse as processing tools become more and more sophisticated.

This situation highlights the need for methods that allow the reconstruction of the history of a digital image in order to verify its truthfulness and assess its quality. Two questions about the history and credibility of an image can be raised: was the image acquired by the device it is claimed to be sensed with? Is the image still depicting the captured original scene? The first question is of major interest when the knowledge of which is the source of the image represents the evidence itself, for example, since it allows to know the user or device that made the picture; the second question has more general interest. Answering to those queries is relatively easy when the original image is known. In practical cases, though, almost no information can be assumed to be known a priori about the original image. Investigators need, therefore, to authenticate the image history in a blind way.

To find an answer to the previous issues, the research community interested in multimedia content security has proposed several approaches that can be first of all classified into active and passive technologies, as represented

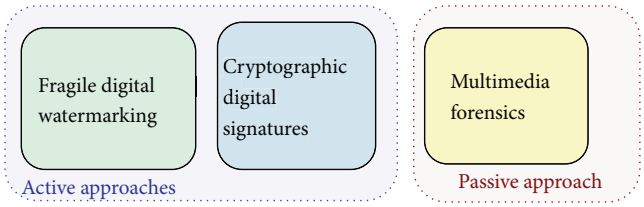


Figure 1: A scheme representing the possible approaches for the assessment of the history and credibility of a digital image.

in Figure 1, where by "active" we mean that for the assessment of trustworthiness, some information that has been computed at the source side (i.e., in the camera), during the acquisition step, is exploited, whereas with the term "passive," a solution which tries to make an assessment only having the digital content at disposal is to be intended.

Active approaches are based on the idea of trustworthy camera [6, 7], proposed in the past as a way to grant the authenticity of digital images. A trustworthy camera computes a digital watermark [8–10] or a digital signature [11, 12] from the image at the instant of its acquisition, and any later modification of the image can be detected by checking the value of the digital watermark or digital signature at the moment of its fruition. A major drawback of active solutions is that digital cameras are specially equipped with a watermarking chip or a digital signature chip that, exploiting a private key hard-wired in the camera itself, authenticates every image the camera takes before storing it on its memory card. The implementation of a trustworthy camera would require the manufacturers to define a common standard protocol, a requirement too hard to be satisfied: this would constraint the application of such solutions only to very limited scenarios.

To overcome the previous problems, recently, a novel method for authenticating the contents of digital images has evolved quickly, that does not need any prior information about the image and thus is defined as passive. The technology, defined multimedia forensics [13–15], relies on the observation that each phase of the image history, from the acquisition process, to its storing in a compressed format, to any post processing operation leaves a distinctive trace on the data, as a sort of digital fingerprint. It is then possible to identify the source of the digital image or determine whether it is authentic or modified by detecting the presence, the absence, or the incongruence of such features intrinsically tied to the digital content itself.

Multimedia forensics descends from the classical forensic science, that studies the use of scientific methods for gaining probative facts from physical or digital evidences. The task of multimedia forensic tools is to expose the traces left in multimedia content by each step of its life, by exploiting existing knowledge on digital imaging and in multimedia security research. The research activity in this domain started a few years ago and increased very much in the last months, thus justifying the need for a a comprehensive overview of the state of the art in digital image forensics to allow a neophyte to come into this field with some help.

In this survey, it has been chosen to classify the forensic techniques according to the position in the history of the digital image in which the relative footprint is left. So, after the introductory Section 2 where the possible history of a digital image, divided into a chain of processing steps, is modelled, the core of the survey is composed by three sections, each related to one of the steps in which the image history has been divided: Section 3 will analyze acquisition-based fingerprints, Section 4 coding-based traces, and Section 5 editing-based features. The previous sections are built as self-contained as possible, notwithstanding the fact that footprint detection usually requires the joint analysis of different processing phases, as it will be highlighted when appropriate. In Section 6, the attention is then focused on antiforensics, that is on methods that try to fool the forensic analysis tools presented in the previous sections. Finally, in Section 7, some future challenges in the field are proposed, and the conclusions are drawn.

## 2. Digital Image Life Cycle

As indicated in Figure 2, the history of a digital image can be represented as a composition of several steps, collected into three main phases: acquisition, coding, and editing. During acquisition, the light coming from the real scene framed by the digital camera is focused by the lenses on the camera sensor (a CCD or a CMOS), where the digital image signal is generated. Before reaching the sensor, however, the light is usually filtered by the CFA (Color Filter Array), a thin film on the sensor that selectively permits a certain component of light to pass through it to the sensor. In practice, to each pixel, only one particular main color (Red, Green, or Blue) is gathered. The sensor output is successively interpolated to obtain all the three main colors for each pixel, through the so-called demosaicing process, in order to obtain the digital color image. The obtained signal undergoes additional in-camera processing that can include white balancing, color processing, image sharpening, contrast enhancement, and gamma correction.

With coding, the processed signal is stored to the camera memory; to save storage, in most cameras, the image is lossy compressed, and for commercial devices, the JPEG format is usually the preferred one.

Finally, the generated image can be postprocessed, for example, to enhance or to modify its content. Any image editing can be applied to an image during its life: the most used ones are geometric transformation (rotation, scaling, etc.), blurring, sharpening, contrast adjustment, image splicing (the composition of an image using parts of one or more parts of images), and cloning (or copy-move, the replication of a portion of the same image). Finally, after editing, very often the image is saved in JPEG format, so that a recompression will occur.

The funding idea of image forensics is then that inherent traces (like digital fingerprints or footprints) are left behind in a digital image during both the creation phase and any other successive process happening during its history. These digital traces can thus be extracted and analyzed for

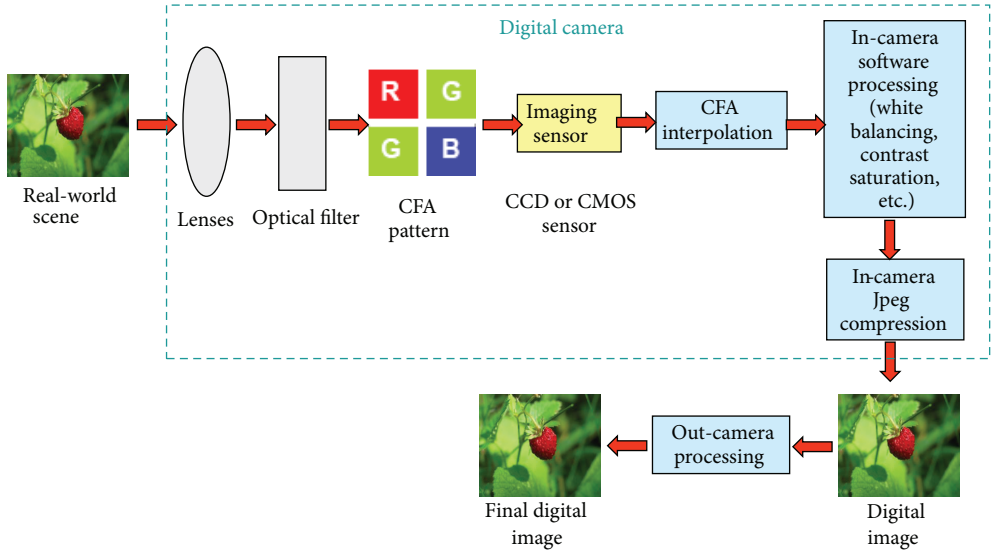


Figure 2: A scheme representing the steps composing the usual life cycle a digital image undergoes.

understanding the history of digital content. According to the previous representation of the image life cycle, we will have then acquisition fingerprints, coding fingerprints, and editing fingerprints.

*Acquisition Fingerprints*. Each component in a digital acquisition device modifies the input and leaves intrinsic fingerprints in the final image output, due to the specific optical system, image sensor, and camera software. The image acquisition pipeline is common for most of the commercially available devices; however, since each step is performed according to specific manufacturer choices, the traces can depend on the particular camera brand and/or model. This means that each stage of the camera introduces imperfections or intrinsic image regularities which leave tell-tale footprints in the final image that, in a similar way to the grooves made in gun barrels that introduce somewhat distinct markings to the bullet fired, represent a signature of the camera type or even of the individual device into the image (in the literature, this property is defined as *image ballistic*). In addition, we will see that the presence of inconsistencies in these artifacts can be taken as evidence of tampering.

*Coding Fingerprints*. Lossy compression inevitably leaves itself characteristic footprints, which are related to the specific coding architecture. As it will be described later, most of the literature has focused on studying the processing history of JPEG-compressed images, by noting that consecutive applications of JPEG introduce a different fingerprint with respect to a single compression. Also for this kind of traces, we will see that the presence of inconsistencies in the coding artifacts present into an image can be taken as an evidence of tampering.

*Editing Fingerprints*. Each processing applied to the digital image, even if not visually detectable, modifies its properties leaving peculiar traces accordingly to the processing itself.

The previous traces can then be used for two main aims: source identification and tampering detection. In the case of source identification, some kind of ballistic analysis is performed; some acquisition traces are usually extracted from the image under analysis and then compared with a dataset of possible fingerprints specific for each class/brand/model of devices: the most similar fingerprint in the dataset indicates the device that took the image. In the case of forgery detection, the aim is to expose traces of semantic manipulation, according to two possible strategies: detecting inconsistencies or the absence of acquisition and coding fingerprints within the considered image indirectly reveals that some postprocessing destroyed them; detecting the presence of editing fingerprints representing a given postprocessing directly reveals the manipulation.

## 3. Image Acquisition

Much of the research efforts in this area have been focused on characterizing each particular stage composing the camera acquisition process, as summarized in the previous section: traces left by the lens, the sensor, and the Color Filter Array.

On the other hand, image acquisition is also performed with digital scanners, and many of the techniques developed for camera footprint analysis have been translated to their scanner equivalents. In addition, images could also be printed and recaptured, so that a digital to analog (D/A) conversion has to be considered. Finally, rendering of photorealistic computer graphics (PRCGs), requiring the application of a physical light transport and a camera acquisition models, can be thought of as a third acquisition modality.

*3.1. Lens Characteristics.* Each acquisition device model presents individual lens characteristics; since, due to the design and manufacturing process, lens produce several types of aberrations, they leave unique traces on the images being

captured that can be used to link an image to a particular device or to discover the presence of image modifications.

Among these aberrations, in [16], lateral chromatic aberration is investigated. This lens aberration causes different light wavelengths to focus on shifted points in the image plane represented by the sensor, when the source light is off the optical axis, resulting in a misalignment between color channels, as summarized in Figure 3.

By assuming that the lateral chromatic aberration is constant within each of the three color channels and by using the green channel as a reference, the aberrations between the red and green channels and between the blue and green channels are estimated. In particular, the lateral chromatic aberration is represented as a low-parameter model consisting of three parameters, two for the center of the distortion and one for the magnitude of the distortion; the estimation of these model parameters is framed as an image registration problem. Johnson and Farid detect image forgeries by looking for the presence of local deviations or inconsistencies in these models with respect to the parameters obtained for the whole image: image tampering is then detected if an inconsistency is found.

In [17], for the purpose of source mobile phone identification, the previous algorithm is modified: the distortion parameters of the chromatic aberration of the whole image are estimated, and the extracted features are fed into a support vector machine (SVM) classifier to identify the source that acquired the image under analysis. In [18], the intrinsic radial distortion due to the lens shape is used instead of camera source identification. Lens characterization is pushed further in [19], where dust patterns are modeled by means of a Gaussian intensity loss model, enabling the identification of a single device from an image.

The method proposed by Yerushalmy and Hel-Or in [20] is mostly based on a type of artifact known as Purple Fringing Aberration (PFA) that, although having a much more complex origin, is stronger and more visible (in the form of a blue-purple halo near the edges of objects in the image) than lateral chromatic aberration. Again, inconsistencies in the direction of these artifacts are used for tampering detection.

*3.2. Sensor-Based Footprints.* Sensor pattern noise is mainly due to imperfections of the image sensor resulting in slight differences between the sensed scene and the image acquired by the camera [21]. The dominating component of sensor pattern noise is the photoresponse nonuniformity (PRNU) noise, due to a combination of factors including imperfections during the CCD/CMOS manufacturing process, silicone inhomogeneities, and thermal noise. PRNU is a high frequency multiplicative noise, generally stable throughout the camera's lifetime in normal operating conditions, that is, unique to each camera. These properties make it adapt not just for device identification, but also for single device linking and, if inconsistencies in the PRNU pattern within the image are found in certain regions, for forgery detection.

The following simplified model for the image signal can be assumed [22]:

$$\mathbf{I} = \mathbf{I}^{(0)} + \mathbf{K}\mathbf{I}^{(0)} + \Psi, \tag{1}$$

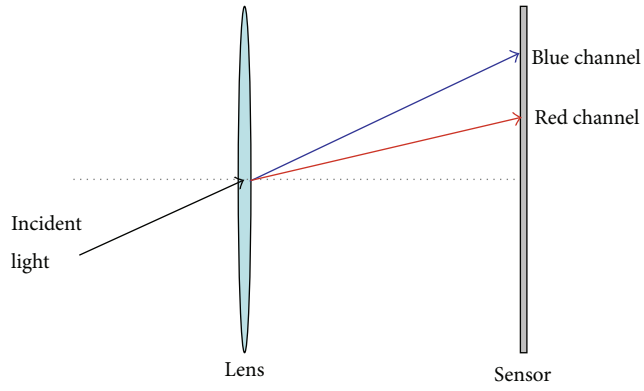


Figure 3: A sketch of the lateral chromatic aberration.

where $\mathbf{I}$ is the signal in a selected color channel, $\mathbf{I}^{(0)}$ denotes the captured light in absence of any noise or imperfections, $\mathbf{K}$ is a zero-mean noise-like signal responsible for PRNU, and $\Psi$ is a combination of random noise components.

To improve the quality of the extracted PRNU, an estimate of the noiseless image $\mathbf{I}^{(0)}$ can be removed from $\mathbf{I}$ by subtracting from both sides of (1) a filtered version of $\mathbf{I}$, $F(\mathbf{I})$, obtained through a denoising filter $F$:

$$\mathbf{W} = \mathbf{I} - F(\mathbf{I}) = \mathbf{I}\mathbf{K} + \Phi, \tag{2}$$

where $\Phi$ is the sum of $\Psi$ and two additional terms introduced by the denoising filter. The idea is that the image $\mathbf{I}$ contains a noiseless contribution, that takes account of the scene content and of a noise term. Ideally, by removing the denoised image from $\mathbf{I}$, only the noise terms $\mathbf{KI}$ and $\Psi$ should remain in $\mathbf{W}$, but indeed other noise terms left by the denoising filter will be present.

By assuming to have a set of $N$ images $\mathbf{I}_k$ acquired by the same camera and to apply the previous procedure to these images to obtain the terms $\mathbf{W}_k$, the maximum likelihood predictor for $\mathbf{K}$ is then formulated as [23]

$$\mathbf{K} = \frac{\sum_{k=1}^{N} \mathbf{W}_k \mathbf{I}_k}{\sum_{k=1}^{N} (\mathbf{I}_k)^2}. \tag{3}$$

Supposing to have a set of $M$ devices, this process has to be repeated for each $i$th acquisition device (where $i = 1, \ldots, M$), in such a way to build a database of PRNUs $\mathbf{K}_i$, identifying each available camera. Now, if it is requested to identify which camera has taken a given image $\mathbf{I}'$, it is requested to extract the noise term $\mathbf{W}' = \mathbf{I}' - F(\mathbf{I}')$ and then to compute a correlation between this noise term and each PRNU, as shown in Figure 4:

$$\rho_i = \mathbf{I}'\mathbf{K}_i \otimes \mathbf{W}', \tag{4}$$

where $\otimes$ denotes normalized correlation.

The PRNU achieving the maximum correlation, or the one higher than a given threshold, will identify the source of the image.

Most of the successive work in this area focuses on making the PRNU estimation more robust. In [24], different

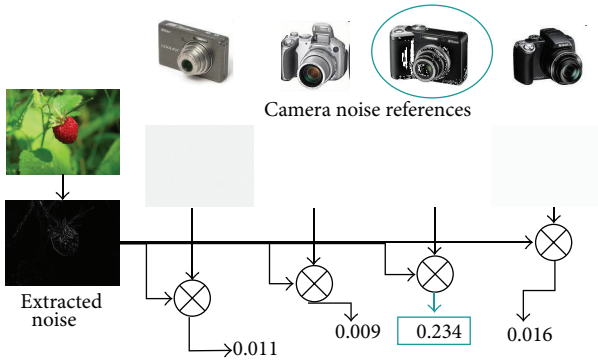


Figure 4: The scheme showing how it is possible to identify the source camera acquiring a given camera, by correlating the noise term of the image with the PRNU of each device.

denoising filters are evaluated. In [23], controlled camera-specific training data is used to obtain a maximum likelihood PRNU predictor. Robustness is further investigated in [25], where the task of PRNU identification after attacks of a nontechnical user is tested and in [26, 27], where the extraction of PRNU is carried out by considering the presence of interpolation noise introduced by the CFA.

The algorithm is also tested in more realistic settings. In [28], the PRNU is estimated exclusively based on regions of high SNR between estimated PRNU and total noise residual to minimize the impact of high frequency image regions. Similarly, in [29, 30], the authors propose a scheme that attenuates strong PRNU components which are likely to have been affected by high frequency image components. In [31], a combination of features from the extracted footprint, including block covariance and image moments, are used for camera classification purposes.

In [32], the problem of complexity is investigated, since the complexity of footprint detection is proportional to the number of pixels in the image. The authors developed "digests" which allow for fast search algorithms to take place within large image databases.

Inconsistencies in the extracted sensor noise pattern can also be used to reveal if a part of the image does not come from the expected device. Indeed, if a portion of an image taken with a camera is replaced with another taken from a different device, the PRNU mask in that region will be inconsistent with the one of the original camera. Thus, a two-hypothesis (tampered/nontampered with) test can be performed block-wise over the image, in order to locally assess its integrity and to reveal the position of regions that have been tampered with. Experiments reported in [23] show that this method is effective (true-positive rate for tampered pixels around 85%, false positive around 5%) provided that the image under analysis has not been heavily compressed: performance is good provided that the image was compressed using JPEG at a quality factor greater than 75.

*3.3. CFA Patterns.* Along with PRNU, another important artifact left by cameras during acquisition is that due to the presence of the Color Filter Array. Indeed, excluding professional triple-CCD/CMOS cameras, the incoming light is filtered by the *Color Filter Array* (CFA) before reaching the sensor (CCD or CMOS), as shown in Figure 5, so that for each pixel, only one particular color is gathered. As a consequence, one-third of the image only is sensed directly.

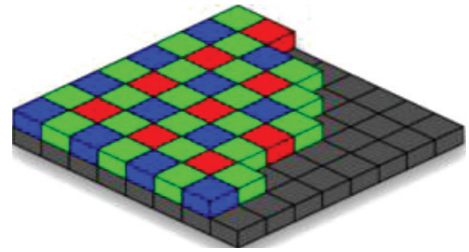

Figure 5: An example of Color Filter Array.

To obtain the missing pixel values for the three color layers, an interpolation process, also referred to as *demosaicing*, is applied starting from a single layer containing a mosaic of red, green, and blue pixels. This process leaves specific correlations in the image pixels that can be detected.

Works considering CFA demosaicing as fingerprint can be divided in two main classes: algorithms aiming at estimating the parameters of the color interpolation algorithm and the structure of the pattern filter and algorithms aiming at evaluating the presence/absence of demosaicing traces.

Algorithms within the first class are mostly intended to classify different source cameras, since each camera brand could adopt different CFA configurations and different interpolation schemes. The second class focuses on forgery detection: ideally, an image coming from a digital camera, in the absence of any successive processing, will show demosaicing artifacts; on the contrary, demosaicing inconsistencies between different parts of the image, as well as their absence in all or part of the analyzed image, will put image integrity in doubt.

Popescu and Farid [33] proposed a technique for detecting the presence of CFA interpolation in an image by assuming a linear interpolation kernel, a simplistic but effective hypothesis compared to complex methods adopted in commercial devices, and using an Expectation-Maximization (EM) algorithm to estimate its parameters (i.e., filter coefficients) as well as the pattern of the filter. The method determines a $p$-map, which gives for each pixel the probability of being correlated to neighboring pixels, according to the currently estimated kernel. Depending on the actual CFA pattern, some pixels are interpolated, whereas others are directly acquired. Hence, the correlation map exhibits a periodic behavior, which is clearly visible in the Fourier domain. Such an analysis can be applied to a given image region, to detect the presence of tampering; however, a minimum size is needed for assuring the accuracy of the results: authors tested their algorithms on $256 \times 256$ and $512 \times 512$ sized areas. This approach is less robust to JPEG compression compared with the one based on PRNU but is characterized by a lower false-positive rate. Gallagher in [34] observed that the variance of the second derivative of an interpolated signal is periodic: he thus looked for the

periodicity in the second derivative of the overall image by analyzing its Fourier transform. Successively, for detecting traces of demosaicing, Gallagher and Chen proposed in [35] to apply Fourier analysis to the image after high pass filtering, for capturing the presence of periodicity in the variance of interpolated/acquired coefficients. The procedure has been tested only up to $64 \times 64$ image blocks, whereas a variation yielding a pixel-by-pixel tampering map is based on a 256-point discrete Fourier transform computed on a sliding window, thus lacking resolution.

Dirik and Memon [36] also exploit CFA interpolation artifacts for determining image integrity. They propose two methods for checking the presence of demosaicing artifacts. The first consists in estimating the CFA pattern of the source digital camera. The image is simply reinterpolated assuming many different patterns, and the pattern which leads to the smallest mean square error is chosen. The second method leverages the low pass nature of common demosaicing kernels, which is expected to suppress the variance of underlying PRNU noise. Therefore, the presence of demosaicing artifacts is detected by comparing the change of variance of sensor noise in interpolated pixels and in directly acquired pixels. Similarly, in [37], an SVM was trained to predict the camera model used for acquisition. Swaminathan et al. in [38] propose a method for source camera identification by the estimation of the CFA pattern and interpolation kernel, while in [39] the same authors exploit the inconsistencies among the estimated demosaicing parameters as proof of tampering: a known CFA pattern is used within an iterative process to impose constraints on the image pixels. These constraints are then used to check whether the image has undergone further manipulation.

Other works are devoted to a more realistic formulation of the problem. In [40], Bayram et al. detect and classify traces of demosaicing by jointly analyzing features coming from two previous works [33, 34], in order to identify the source camera model. In [41] also, PRNU noise features and CFA interpolation coefficients are used jointly to estimate source type and camera model. In [42, 43], the demosaicing formulas are estimated, by employing a partial second-order image derivative correlation model, under the assumption that each region is interpolated differently by the acquisition device depending on its structural features. In [44], Fan et al. propose a neural network framework for recognizing the demosaicing algorithms in raw CFA images and use it for digital photo authentication. In [45], the concrete CFA configuration is determined (essentially the order of the sensed RGB components), in order to decrease the degrees of freedom in the estimation process. In [46], by means of a local analysis of CFA, image forgeries are identified whenever the presence of CFA interpolation is not present. Starting from such an assumption, a new feature is proposed, that measures the presence/absence of these artifacts even at the smallest $2 \times 2$ block level, thus providing as final output a forgery map indicating with fine localization the probability of the image to be manipulated.

*3.4. Other Camera Footprints.* In terms of individual camera footprints, each camera sensor has an individual radiometric response, which is normally shared across cameras of the same brand. This was characterized in [47] from a single greyscale image. It was also achieved in [48] with geometric invariants and planar region detection.

Finally, source classification is addressed in [49] where structural and color features are used to differentiate between real and computer generated images. PRCG recapturing attacks are examined, and countermeasures provided.

In [50], Hsu and Chang explore the usage of another kind of camera artifact, that is, the camera response function (CRF), which maps in a nonlinear way the scene irradiance to image brightness. The basic idea is to look for inconsistencies in the artifacts. The image is automatically segmented, the CRF is estimated on locally planar irradiance points (LPIPs) near to region borders, and a comparison among the estimated functions for distinct regions sharing the same border is performed. Various statistics of these errors are used as features for training an SVM classifier. Results achieve 90% recall with 70% precision, but these values are obtained on a challenging real-world dataset.

*3.5. D-A Reacquisition.* One of the easiest methods to elude forensics analysis consists in recapturing forged and printed images. In these cases, the PRNU and CFA footprints of the camera would be authentic, and all the low level details would have been lost. Moreover, it is shown in [51] that people in general are poor at differentiating between originals and recaptured images, thus giving particular importance to photo recapture detection.

Some approaches have thus been devoted to recapture detection, which can be indicative of prior tampering. In [52], high frequency specular noise introduced when recapturing printouts is detected. A combination of color and resolution features is identified and used for SVM classification of original photos and their recaptured versions in [51]. In [53], a combination of specularity distribution, color histogram, contrast, gradient, and blurriness is used.

The problem of original camera PRNU identification from printed pictures is studied in [54], highlighting the impact of unknown variables, including paper quality, paper feed mechanisms, and print size.

Finally, a large database containing photo recaptured from several widespread low-end camera models was presented in [55] and made publicly available for performance comparison.

*3.6. Scanner Acquisition.* Similarly to camera footprints, scanner footprints can be used for device identification and linking. Moreover, scanned image tampering detection is of particular importance, since legal establishments such as banks accept scanned documents as proofs of address and identity [56].

In [57], noise patterns from different types of reference images are extracted in an attempt to extract a characteristic scanner PRNU equivalent. In [58], cases where scanner PRNU acquisition might be difficult are considered, for example, due to the lack of uniform tones and the dominance of saturated pixels, such as in text documents. Image features

based on the letter "e" are extracted, clustered together, and classified with an SVM. Individual footprints are examined in [59], where scratches and dust spots on the scanning plane result in dark and bright spots in the image.

*3.7. Rendered Image Identification.* Some algorithms have been proposed to distinguish automatically between real and synthetic images. The main hypothesis is that some statistical characteristics is fundamentally different between cameras and CG software. In [60], the residual noise is studied; in [61], statistics of second-order difference signals from HSV images are checked for classification. In [62], a combination of chromatic aberration and CFA presence in images is determined, as nontampered PRCG images would not present CFA demosaicing traces. In [63], Hidden Markov Trees using DWT coefficients are employed to capture multiscale features for PRCG/real image classification. Finally, in [49], a method is presented that takes into account a combination of features based on the inability of CG renderers to correctly model natural structures such as fractals and to reproduce a physically accurate light transport model, yielding classification accuracies of 83.5%.

## 4. Image Coding

Lossy image compression is one of the most common operations which is performed on digital images. This is due to the convenience of handling smaller amounts of data to store and/or transmit. Indeed, most digital cameras compress each picture directly after taking a shot. Due to its lossy nature, image coding leaves characteristic footprints, which can be detected. Although revealing coding-based footprints in digital images is in itself relevant, these traces are fundamentally a powerful tool for detecting forgeries; we will then also describe forgery-detection leveraging coding-based footprints.

*4.1. Standard JPEG.* Nowadays, JPEG is the most common and widespread compression standard [64]. Compression is performed on the following three basic steps.

(i) Discrete cosine transform (DCT): an image is divided into $8\times8$ nonoverlapping blocks. Each block is shifted from unsigned integers with range $[0, 2^b-1]$ to signed integers with range $[-2^{b-1}, 2^{b-1}-1]$, where $b$ is the number of bits per pixel (typically $b = 8$). Each block is then DCT transformed in order to obtain the coefficients $Y(i, j)$, where $i$ and $j(1 \le i, j \le 8)$ are the row and column indexes within a block.

(ii) Quantization: the DCT coefficients obtained in the previous step are quantized according to a quantization table which must be specified as an input to the encoder. Quantization is defined as division of each DCT coefficient $Y(i, j)$ by the corresponding quantizer step size $\Delta(i, j)$, followed by rounding to the nearest integer. That is,

$$Z(i,j) = \operatorname{sign}(Y(i,j)) \operatorname{round}\left(\frac{|Y(i,j)|}{\Delta(i,j)}\right). \quad (5)$$

Thus, the reconstructed value at the decoder is

$$Y_Q(i,j) = \Delta(i,j) \cdot Z(i,j). \quad (6)$$

The quantization table is *not* specified by the standard. In many JPEG implementations, it is customary to define a set of tables that can be selected specifying a scalar quality factor $Q$. This is the case, for instance, of the quantization tables adopted by the independent JPEG group, which are obtained by properly scaling the image-independent quantization table suggested in Annex $K$ of the JPEG standard with a quality factor $Q \in [1, 100]$.

The purpose of quantization is to achieve compression by representing DCT coefficients at a target precision, so as to achieve the desired image quality. Since quantization is not invertible, this operation is the main source of information loss.

(iii) Entropy coding: DCT-quantized coefficient are losslessly coded and written to a bitstream. A common coding procedure is variable length coding by means of properly designed Huffman tables.

*4.2. Algorithms for the Identification of Compression History.* In several scenarios, a digital image is available in the pixel domain as bitmap format, without any knowledge about prior processing. In these cases, it can be interesting to know the image history and, in particular, to detect whether that image had been previously compressed and which were the compression parameters being used. The underlying idea of forensic methods coping with this problem is that block-based image coding, like JPEG, leaves characteristic compression traces in the pixel domain or in the transform domain, that can be revealed.

*4.2.1. Pixel Domain-Based Features.* In the pixel domain, block-based image coding schemes introduce blockiness. Indeed, several methods aiming at estimating blockiness are proposed in the literature.

The authors of [65, 66] describe a method capable of revealing artifacts also when very light JPEG compression is applied, that is, with quality factor $Q$ as high as 95. The proposed algorithm is based on the idea that if the image has not been compressed, the pixel differences across $8 \times 8$ block boundaries should be similar to those within blocks. Then, it is possible to build two functions, $Z'$ and $Z''$, taking into account inter- and intrablock pixel differences. The energy of the difference between the histograms of $Z'$ and $Z''$ is compared to a threshold, and if it is higher that this threshold, the presence of prior compression is deduced.

In [67], the authors model a blocky image as a nonblocky image interfered with a pure blocky signal. Then, the estimation of blockiness in a blind way is turned into the problem of evaluating the power of the blocky signal without accessing the original image. In order to achieve this goal, the absolute value of the gradient between each column or row of the image is computed separately. The power of the blocky signal can be estimated in order to reveal its presence.

In a similar way, in [68] first, block size and block locations are identified. In this respect, the vertical and horizontal gradients are computed, and their periodicity due to gradient peaks at block boundaries is also estimated in the frequency domain using the DFT. Gradient peak locations enable estimating block positions. After the block localization step, a metric for blockiness distortion evaluation is computed, employing a weighting scheme based on the local gradient energy.

Tjoa et al. propose in [69] another method exploiting the periodicity of the directional gradient to estimate the block size. In particular, the authors subtract a median filtered version to the gradient, in order to enhance the peaks, and then apply a threshold based on the sum of the gradients, aimed at avoiding spurious peaks caused by edges from objects in the image. The period of the resulting function is computed using a maximum likelihood estimation scheme commonly adopted for pitch detection.

*4.2.2. Transform Domain-Based Features.* In the transform domain, block-based image coding schemes modify the histogram of transformed coefficients, such that several methods analyzing the shapes of these functions are proposed in the literature.

In [70], the authors derive a method based on the observation that in a JPEG-compressed image, the integral of the DCT coefficient histogram in the range $(-1, +1)$ is greater than the integral in the range $(-2, -1] \cup [+1, +2)$, with quantization steps that are equal to or larger than 2. By examining, as feature, the ratio between the first and the second integral, it is possible to verify that its value, in case of JPEG-compressed image, will be close to zero, and it would be much smaller than that of the corresponding uncompressed one. So, JPEG compression is detected when the ratio is smaller than a given threshold.

A more general approach is discussed in [71], where the aim is to identify the history of source coding operations applied to digital images. In particular, three different image source encoders are considered: transform-based coding (both discrete cosine transform and discrete wavelet transform based), subband coding, and differential image coding (DPCM). Given a decoded image which has been source encoded once, the image is analyzed in order to answer which compression scheme was used to compress the image. The designed algorithm first finds the presence of footprints left by a general block-based encoder. To this end, the gradient between adjacent pixel values is computed: the possible presence of periodicity of this feature is an evidence of a block-based editing. If evidence of block-based coding is found, a similarity measure for each of the previous coding schemes is computed in order to detect the one being used: transform coding is characterized by comb-shaped histograms of the coefficients in the transform domain; subband coding is characterized by the presence of ringing artifacts near image edges; finally, differential image coding is characterized by the whiteness of the residual obtained from the difference between the encoded image and its denoised version. The method giving the highest similarity measure is the candidate encoder, and next the coding parameters are estimated.

*4.3. Algorithms for the Estimation of Quantization Step.* If the image under analysis has been detected as being previously compressed using JPEG, the next problem is to estimate the compression parameters used. In the case of JPEG, this means estimating the used quality factor $Q$ or the whole quantization matrix $\Delta(i, j)$, $1 \leq i, j \leq 8$.

Most of the methods proposed in the literature observe the fact that the histogram of DCT coefficients has a characteristic comb-like shape, where the spacing between successive peaks is related to the adopted quantization step size.

The scheme proposed in [65, 66] exploits a distinctive property of the histogram of DCT coefficients. Specifically, it shows that the envelopes of such histograms can be approximated by means of a Gaussian distribution for DC coefficients (the DCT coefficient $Y(1, 1)$) and a Laplacian distribution for AC coefficients (the other 63 DCT coefficients). Leveraging this observation, the quality factor is estimated through a maximum likelihood (ML) approach.

In [72], the authors propose a method for estimating the elements of the whole quantization table. To this end, separate histograms are computed for each DCT coefficient subband. Analyzing the periodicity of the power spectrum of the histogram, it is possible to extract the quantization step $\Delta(i, j)$ for each subband. Periodicity is detected with a method based on the second-order derivative applied to the histograms. Moreover, possible blocking artifact inconsistencies may tell the presence of tampering.

In [70], the authors propose novel forensic schemes to identify whether a bitmap image has previously been JPEG compressed, estimate the quantization steps, and detect the quantization table. The key idea is that when a JPEG image is reconstructed in the pixel domain, pixel values are rounded to integers. As a consequence, the histograms of DCT coefficients $(\widetilde{Y_Q}(i, j))$ computed from decoded pixel values are not exactly comb shaped, but they are blurred with respect to those obtained directly after quantization $(Y_Q(i, j))$. In this way, it is possible to estimate the quantization step for each DCT frequency by looking at peaks distances in such rounded coefficients histograms.

In the case of color image compression, it is known that distinct quantization tables can be used for each color component. In [73], the authors target the problem of estimating these quantization tables. First, they introduce a MAP estimation method for extracting the quantization step size in grayscale images, exploiting the periodicity of DCT coefficients histograms, by refining the algorithm already proposed in [66]. Then, they extend the solution to color

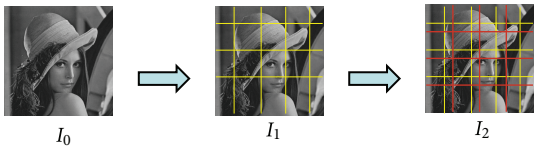


Figure 6: An example of nonaligned double JPEG (NA-DJPG) compression: the uncompressed image $I_0$ is first compressed, with a block grid shown in yellow, obtaining a single compressed image $I_1$; this image is again compressed, with a block grid shown in red, misaligned with the previous one, obtaining the final image $I_2$.

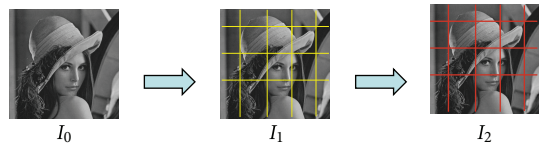


Figure 7: An example of aligned double JPEG (A-DJPG) compression: the uncompressed image $I_0$ is first compressed, with a block grid shown in yellow, obtaining a single compressed image $I_1$; this image is again compressed, with a block grid shown in red, aligned with the previous one, obtaining the final image $I_2$.

images: in this situation, the periodicity of the histogram is revealed only when the image is transformed to the correct colorspace, and interpolation artifacts are removed.

*4.4. Double JPEG.* The JPEG format is adopted in most of the digital cameras and image processing tools, thus we can expect that a manipulated content will often be a recompressed JPEG image. Thus, the presence of tampering can be detected by analyzing proper artifacts introduced by JPEG recompression occurring when the forged image is created; in particular, such artifacts can be categorized into two classes, according to whether the second JPEG compression adopts a discrete cosine transform (DCT) grid aligned with the one used by the first compression, as shown in Figure 7 or not, as shown in Figure 6. The first case will be referred to as aligned double JPEG (A-DJPG) compression, whereas the second case will be referred to as nonaligned double JPEG (NA-DJPG) compression.

The vast majority of proposed algorithms for detection of double JPEG compression are based on JPEG artifacts belonging only to *one* of the possible classes outlined previously, whereas only few look for features belonging to both classes. We will then cluster these works according to that classification.

*4.4.1. Detection of A-DJPG Compression.* Based on the observation that in natural images the distribution of the first digit of DCT coefficients in single JPEG compressed images follows the generalized Benford's law [74], in [75, 76], two detection methods are proposed. Experimental results have shown that each compression step alters the statistics of the first digit distribution. As a consequence, the fitting provided by the generalized Benford's law is decreasingly accurate with the number of compression steps.

The performance of these methods, however, does not seem adequate, and their results are outperformed by later works: for example, in [77], starting from the observation that recompression induces periodic artifacts and discontinuities in the image histogram, a set of features is derived from the pixels histogram to train an SVM allowing to detect an A-DJPG compression; in [78], the histogram of a subset of 9 DCT coefficients is also used to train an SVM and make the same detection. These two last approaches, however, have been tested only for secondary quality factors set to 75 or 80.

A major set of solutions include all those algorithms that rely on the shape of the histogram of DCT coefficients.

A promising idea is the one introduced by Lukáš and Fridrich in [79]: here, it is proposed to detect the presence of double-aligned JPEG compression by observing that consecutive quantizations introduce periodic artifacts into the histogram of DCT coefficients; these periodic artifacts are visible in the Fourier domain as strong peaks in medium and high frequencies and are defined as double quantization (DQ) effect. These peaks in the histogram assume different configurations according to the relationship between the quantization steps of the first and of the second compression. Specifically, special attention is paid to the presence of the so-called double peaks and missing centroids (those with very small probability) in the DCT coefficient histograms, as they are said to be robust features providing information about the primary quantization.

Given a JPEG file with the quantization matrix $\text{Qstep}_2$, to decide if the file was previously JPEG compressed with a different quantization matrix $\text{Qstep}_1$, their approach works as follows: as the first step, the histograms of absolute values of all analyzed DCT coefficients are computed from the image under investigation $\mathbf{I}$. The image is then cropped (in order to disrupt the structure of JPEG blocks) and compressed with a set of candidate quantization tables. The cropped and compressed images are then recompressed using $\Delta_2$; finally, compute the histograms of absolute values of DCT coefficients from the double-compressed cropped images. The estimator chooses the quantization table such that the resulting histogram is as close as possible to that obtained from the image $\mathbf{I}$. The concept of DQ effect is analyzed in more detail by Popescu and Farid in [80], where the artifacts introduced by double compression are quantified thanks to a newly proposed statistical model.

Starting from these two works, several improvements and modifications have been proposed in the literature; per brevity, these works are only cited; see [81–84].

Let us note that [83] produce as output a fine-grained map indicating the tampering probabilities for each $8 \times 8$ image block.

In [85], a different approach to detect areas which have undergone a double-aligned JPEG compression is proposed. The scheme exploits the property of idempotency that characterizes the operators involved in the coding process: reapplying the same coding operations on a test image would lead to a new image that results to be highly correlated with the image under examination. In practice, the method works by recompressing the image under analysis at several

quantization factors and then comparing these differently compressed versions of the image with the possibly tampered one; if the same quality factor of the one used for the tampered area is adopted, a spatial local minima, the so-called JPEG ghosts, will appear in correspondence with the forgery. This method works only if the tampered region has a lower quality factor than the rest of the image and can detect very small tampered regions, but it requires the suspect region to be known in advance.

*4.4.2. Detection of NA-DJPG Compression.* It is possible to exploit blocking artifacts in order to understand whether the reconstructed image has been compressed twice. These solutions rely on the fact that it is highly probable that in a tampered image, the original part of it exhibits regular blocking artifacts, while the pasted one does not, since the second compression was not aligned with the first. Starting from an idea proposed in [66] to detect blocking artifacts, in [86], an $8 \times 8$ blocking artifact characteristics matrix (BACM) is computed in the pixel domain to measure the symmetrical property of the blocking artifacts in a JPEG image; an asymmetric BACM will reveal the presence of misaligned JPEG compressions. Some features, cumulated over the whole image, are extracted from the BACM and fed to a classifier in order to distinguish regions in which blocking artifacts are present from those in which they are not. If the suspected region (which is known by hypothesis) does not exhibit blocking artifacts, then it is classified as tampered. Results are good only when the quality factor of the last compression is much higher than the one used for the first. Furthermore, the method is reliable only when the tampered region is very large, that is, above $500 \times 500$ pixels. The previous algorithm is modified in [87] to localize the tampered regions, without knowing them in advance.

In [88], the blocking artifacts in the pixel domain are again investigated. As a first step, a measure of the blockiness of each pixel is calculated applying a first-order derivative in the 2D spatial domain. From the absolute value of this measure, a linear dependency model of pixel differences is carried out for the within-block and across-block pixels. In order to estimate the probability of each pixel following this model, an EM algorithm is used. Finally, by computing the spectrum of the probability map obtained in the previous step, the authors extract several statistical features, fed to an SVM; this method shows higher performance with respect to [86].

Another approach covering the NA-DJPG case is proposed in [89]. There, by assuming that the image signal is the result of the superposition of different components that are mixed together in the resulting image, independent component analysis (ICA) is adopted to identify the different contributions and separate them into independent signals. Tampering identification is still performed by means of a classifier. Results are improved with respect to [86] by 5%, especially when tampered regions are small.

A recent work addressing the presence of NA-DJPG is the one proposed by Bianchi and Piva in [90, 91], which does not rely on any classifier. Instead, a simple threshold detector is employed. The main idea behind the method is that of detecting NA-DJPG compression by measuring how DCT coefficients cluster around a given lattice (defined by the JPEG quantization table) for any possible grid shift. When NA-DJPG is detected, the parameters of the lattice also give the primary quantization table. Results obtained in this work show an improvement with respect to [86, 89]: a forged region of $256 \times 256$ pixels is sufficient to equal the best results presented in previous works, and good performance (over 90%) is obtained even in the presence of similar first and second quantization factors. Consequently, this method retains good performances even when the last quantization is coarse, for example, corresponding to a quality factor equal to 70. In [92], the same authors present a tampering localization algorithm that, unlike previous approaches, does not need to manually select a suspect region to test the presence or the absence of NA-JPG artifacts. Based on a new statistical model of DCT coefficients, the probability for each $8 \times 8$ DCT block to be forged is automatically derived. Experimental results, considering different forensic scenarios, demonstrate the validity of the proposed approach.

By relying on the property of idempotency of the coding process, in [93], Xian-zhe et al. present a method for identifying tampering and recompression in a JPEG image based on the requantization of transform coefficients. Similarly to [85], the main idea relies on the fact that in case the image has been compressed twice after tampering and the analyst identifies the right quantization steps of the first compression, most parts of the reconstructed image result to be highly correlated with the analyzed image. However, copied parts of the image might exhibit poor correlation due to the desynchronization of DCT blocks.

*4.4.3. Detection of Both A-DJPG and NA-DJPG Compression.* Recently, Chen and Hsu [94] have proposed a detection method which is able to detect either block-aligned or misaligned recompression by combining periodic features in spatial and frequency domains that are modified by recompression. In particular, the scheme computes a set of features to measure the periodicity of blocking artifacts, perturbed in presence of NA-DJPG compression, and a set of features to measure the periodicity of DCT coefficients, perturbed when an A-DJPG compression is applied; this set of nine periodic features is used to train a classifier allowing to detect if an image has undergone a double JPEG compression. Experimental results show that this method outperforms the scheme proposed in [86] for the NA-DJPG case and the schemes in [76, 83] for the other case.

In [95], a forensic algorithm able to discriminate between original and forged regions in JPEG images, under the hypothesis that the tampered image presents a double JPEG compression, either aligned (A-DJPG) or nonaligned (NA-DJPG) is presented. Based on an improved and unified statistical model characterizing the artifacts that appear in the presence of both A-DJPG and NA-DJPG, the proposed algorithm automatically computes a likelihood map indicating the probability for each $8 \times 8$ DCT block of being doubly compressed. The validity of the proposed method has been

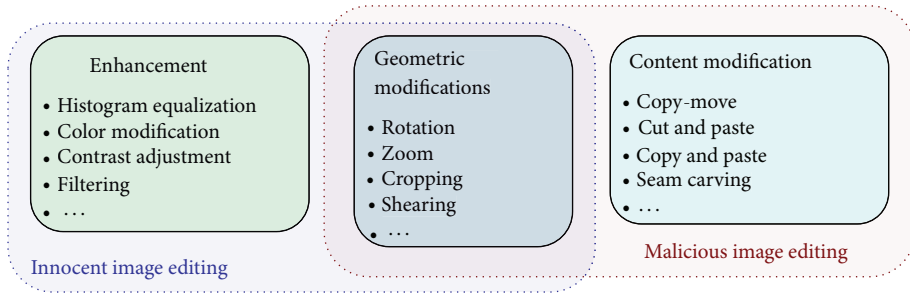


Figure 8: Main types of editing operators applicable to images.

assessed by evaluating the performance of a detector based on thresholding the likelihood map: the results show that, defined as $QF_1$ and $QF_2$ the quality factors of the first and the second compression, the proposed method is able to correctly identify traces of A-DJPG compression unless $QF_2 = QF_1$ or $QF_2 \ll QF_1$, whereas it is able to correctly identify traces of NA-DJPG compression whenever $QF_2 > QF_1$, and there is a sufficient percentage of doubly compressed blocks. The effectiveness of the proposed method is also confirmed by tests carried on realistic tampered images.

## 5. Image Editing

By image editing, any processing applied to the digital media is meant. There are many different reasons for modifying an image: the objective could be, for example, to improve its quality or to change its semantic content. In the former case, the processed image will carry the same information as the original one, but in a more usable/pleasant way. Hence, we refer to this kind of editing as "innocent." Conversely, in the latter case, the semantic information conveyed by the image is changed, usually by adding or hiding something. We refer to this kind of editing as "malicious."

Figure 8 provides a simple classification of three categories of editing operators, along with some examples for each identified class: some operators are likely to be used only for innocent editing, like enhancement operators, while others are clearly intended for malicious attacks. In the middle, there are geometrical operators (e.g., cropping) that can be employed either for slight postproduction editing or for changing the represented scene.

Concerning malicious modifications, the most important are surely the copy-move attacks and cut-and-paste attacks. Copy-move is one of the most studied forgery techniques: it consists in copying a portion of an image (of arbitrary size and shape) and pasting it in another location of the same image. Clearly, this technique is useful when the forger wants either to hide or duplicate something that is already present in the original image. Cut-and-paste, or *splicing*, is the other important image forgery technique: starting from two images, the attacker chooses a region of the first and pastes it on the second, usually to alter its content and meaning. Splicing is probably more common than copy-move, because it is far more flexible and allows the creation of images with a very different content with respect to the original. This is demonstrated also by the huge amount of work on this topic.

In the following, we will discuss forensic techniques that search for traces, left by editing operators, that can be grouped into traces left at "signal level" (in the course of processing, changes induced on the media leave some usually invisible footprints in its content) and into inconsistencies left at "scene level" (e.g., shadows, lights, reflections, perspective, and geometry of objects).

Clearly, inconsistencies at signal level and at scene level are somewhat complementary: a forgery that is invisible from the scene level point of view could be detectable using tools working at signal level and vice versa. Furthermore, it is clear that while tools working at signal level can detect nonmalicious processing like contrast enhancement, tools working at scene level are unlikely to do so.

*5.1. Signal Processing-Based Techniques.* This section discusses methods that detect image editing by using signal processing-based tools designed to reveal footprints left during the editing phase.

*5.1.1. Copy-Move Detection.* Copy-move attacks have been defined at the beginning of Section 5. Since the copied parts are from the same image, some components (e.g., noise and color) will be compatible with the rest of the image, so that this kind of attack is not detectable using forensic methods that look for incompatibilities in statistical measures. Properly designed methods have thus been proposed to cope with this manipulation. First of all, such techniques will have to cope with the problem of the computational complexity, since the direct application of an exhaustive search of cloned areas would be too expensive. In addition, it has to be considered that the cloned areas could be not equal, but just similar, since the tamperer in creating the forgery could exploit image processing tools to hide the tampering. Therefore, the forgery detection method should be designed in order to be robust with respect to this set of possible modifications.

Several approaches to copy-move detection were proposed: a block matching procedure was presented by Fridrich et al. in [96], which inspired the development of several other works in this direction; according to this proposal, instead of looking for the whole duplicated region, the image is

segmented into overlapping square blocks, and then similar connected image blocks are looked for. By assuming that the cloned region is bigger that the block size, and thus that this region is composed by many overlapping cloned blocks, each cloned block will be moved with the same shift, and thus the distance between each duplicated block pair will be the same, as well. Therefore, the forgery detection will look for a minimum number of similar image blocks within the same distance and connected to each other to form two image areas exhibiting same shape.

All the analyzed methods follow the same block matching-based procedure: an $M \times N$ image is first segmented into $N_b = (M - b + 1) \times (N - b + 1)$ overlapping square blocks of size $b \times b$, slid each by one pixel from the upper left corner to the lower right corner. From each block, a set of $F$ features is extracted and properly quantized, to remove possible slight differences between cloned blocks. Assuming that similar blocks are represented by similar features, a matching process, based on the lexicographically sorting, is then applied to the block feature vectors to find the duplicated blocks. Finally, a forgery decision is made by checking if there are more than a certain number of block pairs connected to each other within a same shift, to take into account that most of the natural images would have many similar blocks.

All works following this approach differ just on the kind of features selected to represent each image block. In [96], it is proposed to adopt the block discrete cosine transform (DCT) coefficients, in [97], color-related features are used; in [98], Popescu and Farid propose to use a principal component analysis of pixels to achieve a more compact representation of each block which speeds up search. Later, Bayram et al. [99] introduced the use of Fourier-Mellin transform (FMT) as block signature, since FMT is invariant to rotation and scaling. Wu et al. [100] recently proposed the use of Log-Polar Fourier transform as signature to yield invariance to rotation and scaling.

Hailing et al. introduced a completely different approach [101], which is based on scale-invariant feature transform (SIFT) local features. The basic concept is to use SIFT descriptors [102] to find matching regions within the same image. The main difficulties are choosing an appropriate matching strategy and properly partitioning image keypoints into subsets (in order to search for matching between their elements). The idea of using SIFT has been later exploited in [103, 104].

Although copy-move forgeries have already received a lot of attention and inspired a large number of papers, the detection of this kind of attack remains a challenging problem. Indeed, many open issues are still to be explored such as, for example, understanding which is the original patch, between two copies, improving performance in detecting small copied regions, and making detection techniques more content independent (up to now, attacks on very smooth regions, e.g., depicting the sky, are usually considered false positives).

*5.1.2. Resampling Detection.* Users very often apply to an image geometric transformations like a resizing and/or rotation. These operators apply in the pixel domain, affecting the position of samples, so the original image must be *resampled* to a new sampling lattice. Resampling introduces specific correlations in the image samples, which can be used as an evidence of editing. Resampling detection techniques can be exploited for detecting both benign editing (e.g., scaling or rotation of the whole image) as well as malicious editing (by checking if only a certain region has been resized, thus altering the information carried by the image).

Popescu and Farid [105] proposed a method to detect periodic correlations introduced in the image by common resampling kernels, which is very similar to the one introduced by the same authors in [33]. In their approach, the Expectation-Maximization algorithm is applied to estimate the interpolation kernel parameters, and a probability map (called $p$-map) that is achieved for each pixel provides its probability to be correlated to neighbouring pixels. The presence of interpolated pixels results in the periodicity of the map, clearly visible in the frequency domain. Accuracy of the method is very high, provided that the image has not been compressed.

Meanwhile, Gallagher in [34] observed that the variance of the second derivative of an interpolated signal is periodic: he thus looked for the periodicity in the second derivative of the overall image by analyzing its Fourier transform. Although derived from different bases, Popescu's method and Gallagher's one are closely related, as demonstrated by Kirchner in [106, 107]. In these papers, it is demonstrated how the variance of prediction residuals of a resampled signal can be used to describe periodic artifacts in the corresponding $p$-map, and it is proposed a simplified detector, much faster than the one in [105], while achieving similar performance. Further studies by the same authors are reported in [108, 109]. Based on Gallagher's ideas, the periodicity of the second (or other order) derivative is further studied by other authors, among which we mention [110–114].

Another approach to resampling detection has been developed by Mahdian and Saic [115], that studied the periodic properties of the covariance structure of interpolated signals and their derivatives. The core of the proposed scheme is a Radon transform applied to the derivative of the investigated signal, followed by a search for periodicity.

Another new approach is presented by the same authors in [116] where the periodic patterns introduced in images by interpolation are detected using cyclostationarity analysis, detecting specific correlations between its spectral components. Further studies of this application of cyclostationarity analysis can be found in [117, 118].

*5.1.3. Enhancement Detection.* Today, it is becoming more and more difficult to find images which are published without having undergone at least some enhancement operation like smoothing, contrast enhancement, histogram equalization, and median filtering.

An interesting approach to the detection of median filtering has been proposed by Kirchner and Fridrich in [119]. The basic idea is that median filtered images exhibit so-called "streaking artifacts," that is, pixels in adjacent rows

or columns share the same value. These artifacts can be analyzed by considering first-order differences for groups of two pixels and then studying their corresponding histograms. This simple approach yields extremely high detection rates, provided that images are not compressed. To cope with JPEG postcompression, they presented another first-order difference-based detector which utilized the subtractive pixel adjacency matrix (SPAM) features [120]. Another algorithm for the detection of median filtering is the one proposed in [121], that outperforms the one in [119]. The key observation of this work is that the two-dimensional median filter significantly affects either the order or the quantity of the gray levels contained in the image area encompassed by the filter window.

Several works have been proposed by Stamm and Liu, aiming at detecting and estimating contrast enhancement and histogram equalization in digital images. The first of these works targets the detection of the enhancement operation [122], while in [123], an extension is provided in order to estimate the actual mapping induced by the contrast enhancement operator. In both cases, the key idea is to reveal footprints left in the image by the operator, which consist in the formation of sudden peaks and zeros in the histogram of pixel values. These techniques were originally thought for enhancement detection, but they have also been successfully applied to splicing localization in [124] by the same authors.

*5.1.4. Seam Carving Detection.* The basic idea of *seam carving* [125] is to automatically detect, if any, paths of pixels (seams) of the image along which no relevant content is present. If detected, these paths are eliminated, and the image size is reduced. We may think of this technique as a sort of content-dependent cropping.

Two works have been proposed to detect if an image has undergone this kind of processing by Sarkar et al. [126] and Fillion and Sharma, respectively [127]. In [126], changes in pixel values near the removed seams are searched by building a Markov model for the co-occurrence matrix in the pixel and frequency domain and used as features to train a classifier. In [127], a classifier is fed with three features: one takes into account how energy is distributed in the image histogram; the second exploits the fact that applying another seam carving to an image reveals if low energy seams have already been removed; and the third is based on statistical moments of the wavelet transform.

*5.1.5. General Intrinsic Footprints.* Differently from previous approaches, the methods described in the following are focused on finding general footprints left in the signal without considering the particular phenomena that caused the presence of these effects. The key idea in these works is that manipulations like splicing bring anomalies in the image statistics, which make them distinguishable from the original ones. This kind of approach usually allows to detect many different kinds of tampering at the price of lower accuracy.

One of the first approaches in this direction was proposed by Avcibas et al. [128], who select four image quality metrics (the two first-order moments of the angular correlation and two first-order moments of the Czenakowski measure) and create a set of manipulated images to which various kinds of processing are applied, like scaling, rotation, brightness adjustment, and histogram equalization. They feed all these features, extracted by the datasets of original and manipulated images, to a linear regression classifier. Experiments show a very high accuracy.

Starting from the idea that a splicing operation may introduce a number of sharp transitions such as lines, edges, and corners, Chen et al. [129] employ a classifier, fed with three categories of features highlighting the presence of such traces: statistical moments of the characteristic function (CF) of the image, moments of the wavelet transform of the CF, and low-order statistics of the 2D-phase congruency. Accuracy, computed over a well-known splicing dataset (the Columbia Image Splicing Detection Evaluation Dataset), is on the average still below 85%.

Again, to detect the presence of splicing, Shi et al. [130] use a classifier trained with statistical moments of the image itself, of the DCT of the image (performed block-wise with various block dimensions), and statistical moments of the LL subband of the wavelet transform. Performances, computed over the same Columbia Image Splicing Detection Evaluation Dataset, are better than in previous works, reaching a level of accuracy around 90%.

A comprehensive approach has been developed by Swaminathan et al. [39]. In this work, intrinsic footprints of the in-camera processing operations are estimated through a detailed imaging model and its component analysis. Editing applied to the image is modeled as a manipulation filter, for which a blind deconvolution technique is applied to obtain a linear time-invariant approximation and to estimate the intrinsic footprints associated with these postcamera operations. If the estimated postcamera operations are far from being identity functions, the image is classified as tampered. Reported accuracy values are not very high.

*5.2. Geometry/Physics-Based Techniques.* Up to now, we have presented only works that tackle editing detection from a signal processing point of view, that is, using statistical tools and models. In this section, we introduce a "geometry/physics-based" approach that, instead of looking at signal properties, reveals inconsistencies introduced by tampering at the "scene" level (e.g., inconsistencies in lighting, shadows, colors, perspective, etc.). One of the main advantages of these techniques is that, being fairly independent on low-level characteristics of images, they are extremely robust to compression, filtering, and other image processing operations, remaining applicable even when the quality of the image is low.

The basic consideration underlying these techniques is that it is really difficult to create forgeries that are consistent from a geometric/physic point of view. This leads to the fact that most forgeries will likely contain slight errors, that, whether not visible to the human eye, can be detected by applying proper analysis.

Notice that the kinds of inconsistencies searched by these methods are likely to be introduced when a cut-and-paste attack is performed. Conversely, a copy-move attack is usually hard to reveal especially when targeted to hide something. Finally, it is worth to highlight that it is not easy to objectively assess the performance of these techniques because, being human assisted, they cannot be tested on massive amounts of data. As a consequence, while each work shows very good results on all of the reported examples, the validity of the proposed methods in different scenarios is not easy to predict.

*5.2.1. Splicing Detection Based on Lighting/Shadows.* One of the most common problems when creating a forgery is to take into account how objects present in the scene interact with the light source. Cutting an object from a photo and pasting it into another requires to adapt object illumination and to introduce consistent shadows in the scene. When this is not done, inconsistencies in lighting direction and shadows can reveal that the forged image is not real.

The first issue when trying to find the light source direction in a scene is that it is not easy to extract three-dimensional (3D) surface normals from a single image; in [131], a simplifying solution is proposed: only the 2D surface normals at the occluding object boundary are considered, so that only two of the three components of the light direction are estimated. Although there remains an ambiguity, the extracted information is still sufficient in many cases to understand if an object has been spliced into the scene. As a further simplification, it is assumed that the surfaces of objects are Lambertian (the surface reflects light isotropically), have a constant reflectance value, and are illuminated by a point light source infinitely far away. A quadratic error function, embodying the simplified imaging model is minimized using standard least squares estimation to yield the light direction. This computation can be repeated for different objects or people in the scene to verify the consistency of lighting. In [132], the same authors propose to estimate 3D light direction by exploiting spotlight reflections in human eyes to check if two persons in the same image have been actually taken from different photos. Again, the same authors consider the presence of multiple light sources, diffuse lighting or directional lighting, in [133], where they try to estimate the lighting environment taking some simplifying hypothesis (i.e., infinitely distant light sources, Lambertian surfaces, etc.) under which a nine-dimensional model is sufficient to describe mathematically the illumination of the scene. Inconsistencies in the lighting model across an image are then used as evidence of tampering.

Riess and Angelopoulou [134] propose a different approach to lighting-based tampering detection, by presenting a method for locally estimating the color of the illuminant from a single image. The image is first segmented in regions of similar color. A user selects suspect regions among these, and a map is generated which shows how much each region is illuminated consistently with respect to the dominant illuminant colors.

As stated before, inconsistencies in shadows are a good indicator of tampering. In [135], Zhang et al. proposed two methods to detect inconsistencies in shadows. The first method is based on shadow geometry, using a planar homology to check consistencies of shadows size and directions. The second exploits shadow photometry, specifically shadows matte values, which often turn out to be useful in discriminating pasted shadows from original ones. The experimental results demonstrate the efficiency of the method.

In [136], a method for detecting tampered objects based on photometric consistency of illumination in shadows is proposed. Focusing on the outdoor scenes where the single distant light source assumption is valid, the method measures some color characteristics of shadows by the shadow matte value. The shadow boundaries and the penumbra shadow region in an image are first extracted, then shadow matte values for each of the sampled shadows are estimated, and the presence of inconsistencies reveals tampering. Experimental results confirm the effectiveness of the proposed method.

*5.2.2. Splicing Detection Based on Inconsistencies in Geometry/Perspective.* As stated before, the human brain is not good at evaluating the geometrical consistency of a scene. Some works have thus been developed to detect the presence of inconsistencies in the geometrical and perspective setting of the scene in an image. Of course, this problem is ill conditioned because of the mapping from 3D coordinates to image coordinates during acquisition. Nevertheless, in simplified contexts, some interesting results can be achieved.

As a first example in this class, in [137], textured plane orientation is found by analyzing the nonlinearities introduced in the spectrum by perspective projection, which can be used to detect photo recapture.

Starting from the observation that into an original acquired scene the projection of the camera center onto the image plane (the principal point) is near the center of the image, in [138], the authors demonstrate that in the presence of translation of a person or of an object, the principal point is shifted proportionally. Differences in the estimated principal point across the image can then be used as an evidence of manipulation.

When the image manipulation involves adding or changing of text, it is usually easy to obtain a perceptually convincing fake; however, it is likely that the rules of perspective projection will be violated. In [139], a technique for determining if typed text on a sign or billboard obeys the rules of perspective projection is proposed. When a sign or a billboard is present in an image, it usually shows some writings arranged on a planar surface. This, together with a careful estimation of the character type which is used in writings, allows to estimate the planar homography for that surface, which is compared to the one extracted from the image using, for example, other planar objects present in the image. If the transformations are not consistent, it is highly probable that the writing is fake.

Another interesting approach has been proposed by Kakar et al. in [140]. The method is based on discrepancies in motion blur in the image, usually caused by the slow speed

of the camera shutter relative to the object being imaged. The proposed algorithm resorts to a blur estimation through spectral characteristics of image gradients, which can detect inconsistencies in motion blur.

In [141], the author proposed to detect the presence of spliced object by observing that while pasting an object into an image, it is difficult to properly size it in such a way to respect the principles of visual perception. A perspective constraint-based method to compute the height ratio of two objects in an image without any knowledge of the camera parameters is then presented. The height ratio can be found by a vanishing line of the plane on which both objects of interest are situated. Once the estimated ratio exceeds a tolerable interval, a forged region is identified.

## 6. Image Antiforensics

Research in multimedia forensics has recently start focusing on antiforensics or counterforensics, that is, on techniques with which a knowledgeable adversary might want to impede making forensic analysis [142]. Antiforensic techniques operate by disguising manipulation fingerprints and/or falsifying device-specific fingerprints introduced during acquisition.

In [142], antiforensic schemes have been classified as targeted or universal methods. A method is defined targeted if it aims at removing traces detectable with one particular forensic tool, assumed to be known by the attacker. On the contrary, a method is universal if it tries to maintain as many image features as possible similar to the ones of an unaltered content, in order to conceal manipulations even to unknown forensic algorithms. Actually, most of the proposed counterforensic schemes are targeted, since they were designed to delete the traces left by a particular acquisition or processing operation happened during the history of the digital content, as it will be shortly reviewed here.

To hide fingerprints left by image resampling due to geometrical operations like resizing or rotation, in [143], a set of attacks have been proposed: since the main idea to detect resampling is to look for the presence of periodic linear dependencies between pixels in a close neighborhood, nonlinear filtering or small geometrical distortions are applied to distort such condition; this allows to disguise resampling detection schemes like the one proposed in [105].

Other antiforensic operations have been designed to remove or to falsify the photoresponse nonuniformity (PRNU) fingerprint left in digital images by sensor imperfections. In [144], a removal attack is proposed, based on the application of flat fielding; next, a fingerprint-copy attack is proposed: a fake camera fingerprint is estimated from a set of acquired images and pasted onto an image from a different camera (where the removal attack has already been carried out) with the aim to introduce a false source camera identification. A countermeasure against such attack, named Triangle Test, has been introduced in [145]; however, a more sophisticated behavior of the attacker is studied in [146] allowing to invalidate such new countermeasure.

A method to synthetically create or restore a color filter array (CFA) fingerprint in digital images is proposed in [147]. This attack can be useful to conceal traces of manipulation that disrupted the CFA pattern.

A lot of work has been concentrated on the study of methods allowing to hide traces left by a compression operation. Stamm et al. proposed in [148] a method for removing the quantization artifacts left on DCT coefficients in JPEG-compressed images. The main idea is to modify the comb-shaped distribution of DCT coefficients in JPEG-compressed images, in such a way to restore a Laplacian distribution, which typically arises in uncompressed natural images, by adding a dithering noise signal in the DCT domain. In [149], the approach is extended to hide quantization footprints left by a wavelet-based coding scheme, like JPEG2000, to fool the scheme in [71]. However, in [150], it is demonstrated that this attack induces a loss of perceived image quality, with respect to both the original (uncompressed) and to the JPEG-compressed image. The authors propose a perceptually modified version of the attack, taking into account the level of "just-noticeable distortion" (JND) that can be sustained by each DCT coefficient. The same authors in [151] show that it is possible to detect this kind of attack by measuring the noisiness of images obtained by recompressing the forged image at different quality factors. Other detectors of the dithering attack on DCT coefficients are proposed in [152], analyzing the magnitude and the number of zeros in high frequency AC coefficients. Stamm et al. proposed also a deblocking method to remove blocking artifacts caused by JPEG compression in [153], to disguise the forensic detector proposed in [66]; the attack consists in smoothing the JPEG-compressed image with a median filter, and then adding a low-power white noise signal to the filtered image.

All previous antiforensic methods have each been designed to disguise a particular forensic method, by devising targeted attacks against a specific kind of traces. On the contrary, universal attacks appear to be a much more difficult task, since it is requested to maintain plausible image statistics that the attacker does not fully know, in such a way that he/she will never be sure that the manipulation did not leave detectable artifacts. In this category, in [154], a counterforensic technique for hiding traces left on the image histogram by any processing operation is proposed, by assuming that the forensic scheme to be disguised is based on first-order statistics only. Moreover, there are the works [155, 156], where game-theoretic models are introduced trying to build a general framework that takes into account the interplay between forensic and antiforensic techniques. In the first one, a game-theoretic model for the source-identification problem with known statistics is introduced; in the second, the game theoretic framework is used to determine the probability that a forgery will be detected when both attacker and detector use optimal strategies.

## 7. Conclusions

In this survey, image forensic tools have been reviewed, by classifying them according to the position in the history of

the digital image in which the relative footprint is left. It has been highlighted how image acquisition footprints arise from the overall combination of individual traces left by each single stage in the acquisition process cascade. Tools based on these traces are characterized by high success rates; however, they normally require images captured under controlled conditions or a multitude of images available for a single device. This is not always possible, especially taking into account low-cost devices with high noise components.

Significantly, limited attention has been devoted to characterization of fingerprints arising from chains of acquisition stages, even though the few methods that considered simultaneously more than one processing stage enjoyed increased classification performance [26, 41]. This would suggest that focus on the complete acquisition system would be desirable for the design of algorithms working in real application scenarios.

Concerning coding-based footprints, most of the literature has focused on studying the processing history of JPEG-compressed images, proposing methods to detect whether an image was JPEG compressed, to determine the quantization parameters used and to reveal traces of double JPEG compression.

Editing-based traces can be searched either at a "statistical level," by analyzing the media in some proper domain, or at the "scene level," for example, by looking for inconsistencies in shadows or lighting. The second class is more robust to enhancement or compression operations, but they are not completely automatic.

Let us highlight that in the current literature, in most of the presented works, each of the previous stages in the image life cycle has been considered in isolation, in such a way that each digital footprint has been analyzed regardless of the remaining processing stages. This leaves scope for a more complicated analysis of operator chains. Some methods have been presented where cues from more than one stage are simultaneously taken into account, albeit based on either heuristics or black-box classifiers, rather than on a formal understanding of cascading operators. This approach has been proven to boost the accuracy of device identification algorithms [26, 41, 157]. However, much work still remain to be done.

Another problem to consider is that, in most cases, tampering is obtained by applying a small set of processing tools, hence only a part of the available trace detectors will reveal the presence of tampering. Furthermore, it may happen that the positive answer of one algorithm inherently implies the negative answer of another because they search for mutually excluding traces. Finally, trace detectors often give uncertain if not wrong answers, since their performance are far from ideal. For these reasons, taking a final decision about the authenticity of an image relying on the output of a set of forensic tools is not a trivial task. This problem can be addressed in different ways as illustrated, for the steganalysis problem, in [158]. According to [158], there are basically three kinds of approaches to fusion. The first is to perform fusion at the *feature* level: each tool extracts some features from the data, then a subset of these feature is selected and used to train a global classifier. The second is to consider the output of the tools (usually a scalar) as they are and fuse them (*measurement* level). The last approach consists in fusing the output of the tools after they have been thresholded (*abstract* level).

Most of the existing works are based on the first approach; a hybrid approach has been investigated in [159], but still focusing on feature fusion. A problem with fusion at the feature level is the difficulty of handling cases involving a large number of features (curse of dimensionality) and the difficulty to define a general framework, since ad hoc solutions are needed for different cases.

In order to get around the previous problems, it is possible to perform fusion at the measurement level, delegating the responsibility of selecting features and training classifiers (or other decision methods) to each single tool, thus keeping the fusion framework more general and easy to extend while avoiding to lose important information about tool response confidences, as would happen when fusing at the *abstract* level. In [160], a fusion framework based on the Dempster-Shafer's "theory of evidence" (DS Theory) [161] that focuses exclusively on fusion at the measurement level has been presented. The proposed framework exploits knowledge about tool performances and about compatibility between various tool responses and can be easily extended when new tools become available. It allows both a "soft" and a binary (tampered/nontampered) interpretation of the fusion result and can help in analyzing images for which taking a decision is critical due to conflicting data. In [162], a decision fusion framework based on the fuzzy theory is proposed. The proposed framework permits to cope with the uncertainty and lack of precise information typical of image forensics, by leveraging on the widely known ability of the fuzzy theory to deal with inaccurate and incomplete information. These are the first proposals in this area, but still much work remains to be carried out to obtain an effective and performing image forensic tool working in real applications, without a strong participation of a human operator.

## Acknowledgments

This work was partially supported by the REWIND Project, funded by the Future and Emerging Technologies (FET) programme within the 7FP of the EC, under Grant 268478 (http://www.rewindproject.eu/). The author would like to acknowledge all the project partners for their effort in carrying out the state-of-the-art review of the general field of multimedia forensics, whose results are reported in the deliverable "state-of-the-art on multimedia footprint detection," available online at the project website.

## References

[1] G. W. Meyer, H. E. Rushmeier, M. F. Cohen, D. P. Greenberg, and K. E. Torrance, "An experimental evaluation of computer graphics imagery," *ACM Transactions on Graphics*, vol. 5, no. 1, pp. 30–50, 1986.

[2] "Fake or foto," 2012, http://area.autodesk.com/fakeorfoto.

[3] H. Farid, "Digital doctoring: how to tell the real from the fake," *Significance*, vol. 3, no. 4, pp. 162–166, 2006.

[4] B. Zhu, M. Swanson, and A. Tewfik, "When seeing isn't believing [multimedia authentication technologies] ," *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 40–49, 2004.

[5] "Photo tampering throughout history," 2012, http://www.fourandsix.com/photo-tampering-history/.

[6] G. L. Friedman, "Trustworthy digital camera: restoring credibility to the photographic image," *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 905–910, 1993.

[7] P. Blythe and J. Fridrich, "Secure digital camera," in *Proceedings of the Digital Forensic Research Workshop (DFRWS '04)*, pp. 17–19, 2004.

[8] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2001.

[9] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*, Signal Processing and Communications, Marcel Dekker, 2004.

[10] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Water—Marking and Steganography*, Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition, 2008.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla, USA, 1st edition, 1996.

[13] H. Farid, "Image forgery detection," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16–25, 2009.

[14] T. Van Lanh, K. S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A survey on digital camera image forensic methods," in *Proceedings of the IEEE International Conference onMultimedia and Expo (ICME '07)*, pp. 16–19, July 2007.

[15] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389–399, 2010.

[16] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *Proceedings of the 8th workshop on Multimedia & Security*, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, Eds., pp. 48–55, ACM, Geneva, Switzerland, September 2006.

[17] L. T. Van, S. Emmanuel, and M. S. Kankanhalli, "Identifying source cell phone using chromatic aberration," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07)*, pp. 883–886, Beijing, China, July 2007.

[18] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," *Optics Express*, vol. 14, pp. 11551–11565, 2006.

[19] A. E. Dirik, H. T. Senear, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 539–552, 2008.

[20] I. Yerushalmy and H. Hel-Or, "Digital image forgery detection based on lens and sensor aberration," *International Journal of Computer Vision*, vol. 92, no. 1, pp. 71–91, 2011.

[21] J. Janesick, *Scientific Charge-Coupled Devices*, Spie Press Monograph, SPIE Press, 2001.

[22] J. Fridrich, "Digital image forensic using sensor noise," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 26–37, 2009.

[23] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[24] I. Amerini, R. Caldelli, V. Cappellini, F. Picchioni, and A. Piva, "Estimate of PRNU noise based on different noise models for source camera Identification," *International Journal of Digital Crime and Forensics*, vol. 2, no. 2, pp. 21–33, 2010.

[25] K. Rosenfeld and H. T. Sencar, "A study of the robustness of PRNU-based camera identification," in *Proceedings of the Media Forensics and Security I, part of the IS&T-SPIE Electronic Imaging Symposium*, vol. 7254 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2009.

[26] C.-T. Li and Y. Li, "Digital camera identification using colour-decoupled photo response non-uniformity noise pattern," in *Proceedings of the International Symposium on Circuits and Systems (ISCAS '10)*, pp. 3052–3055, IEEE, Paris, France, May 2010.

[27] C.-T. Li and Y. Li, "Color-decoupled photo response non-uniformity for digital image forensics," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, pp. 260–271, 2012.

[28] B.-B. Liu, Y. Hu, and H.-K. Lee, "Source camera identification from significant noise residual regions," in *Proceedings of the International Conference on Image Processing (ICIP '10)*, pp. 1749–1752, IEEE, Hong Kong, China, September 2010.

[29] C.-T. Li, "Source camera identification using enahnced sensor pattern noise," in *Proceedings of the IEEE International Conference on Image Processing (ICIP '09)*, pp. 1509–1512, IEEE, Cairo, Egypt, November 2009.

[30] C.-T. Li, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, 2010.

[31] T. Filler, J. Fridrich, and M. Goljan, "Using sensor pattern noise for camera model identification," in *Proceedings of the International Conference on Image Processing (ICIP '08)*, pp. 1296–1299, IEEE, San Diego, Calif, USA, October 2008.

[32] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in *Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium*, N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. Delp, Eds., vol. 7541 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2010.

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

[34] A. C. Gallagher, "Detection of linear and cubic interpolation in JPEG compressed images," in *Proceedings of the Canadian Conference on Computer and Robot Vision*, pp. 65–72, May 2005.

[35] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW '08)*, pp. 1–8, June 2008.

[36] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proceedings of the International Conference on Image Processing (ICIP '09)*, pp. 1497–1500, IEEE, Cairo, Egypt, November 2009.

[37] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on CFA interpolation," in *Proceedings of the IEEE International Conference on Image Processing 2005 ( ICIP '05)*, pp. 69–72, September 2005.

[38] A. Swaminathan, M. Wu, and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–105, 2007.

[39] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101–117, 2008.

[40] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models based on demosaicing artifacts," *Digital Investigation*, vol. 5, no. 1-2, pp. 49–59, 2008.

[41] C. McKay, A. Swaminathan, H. Gou, and M. Wu, "Image acquisition forensics: forensic analysis to identify imaging source," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '08)*, pp. 1657–1660, IEEE, Las Vegas, Nev, USA, March-April 2008.

[42] H. Cao and A. C. Kot, "Accurate detection of demosaicing regularity from output images," in *Proceedings of the International Symposium on Circuits and Systems (ISCAS '09)*, pp. 497–500, IEEE, 2009.

[43] H. Cao and A. C. Kot, "Accurate detection of demosaicing regularity for digital image forensics," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 899–910, 2009.

[44] N. Fan, C. Jin, and Y. Huang, "A pixel-based digital photo authentication framework via demosaicking inter-pixel correlation," in *Proceedings of the 11th ACM Workshop on Multimedia Security (MM&Sec '09)*, pp. 125–129, September 2009.

[45] M. Kirchner, "Efficient estimation of cfa pattern configuration in digital camera images," in *Proceedings of the Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium*, N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. Delp, Eds., vol. 7541 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2010, 754111.

[46] P. Ferrara, T. Bianchi, A. de Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of cfa artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1566–1577, 2012.

[47] S. Lin and L. Zhang, "Determining the radiometric response function from a single grayscale image," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '05)*, vol. 2, pp. 66–73, June 2005.

[48] T. T. Ng, S. F. Chang, and M. P. Tsui, "Using geometry invariants for camera response function estimation," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '07)*, pp. 1–8, Minneapolis, Minn, USA, June 2007.

[49] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," in *Proceedings of the 13th Annual ACM International Conference on Multimedia*, H. Zhang, T.-S. Chua, R. Steinmetz, M. S. Kankanhalli, and L. Wilcox, Eds., pp. 239–248, ACM, 2005.

[50] Y. F. Hsu and S. F. Chang, "Camera response functions for image forensics: an automatic algorithm for splicing detection," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 816–825, 2010.

[51] H. Cao and A. C. Kot, "Identification of recaptured photographs on lcd screens," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 1790–1793, IEEE, Dallas, Tex, USA, March 2010.

[52] H. Yu, T.-T. Ng, and Q. Sun, "Recaptured photo detection using specularity distribution," in *Proceedings of the International Conference on Image Processing (ICIP '08)*, pp. 3140–3143, IEEE, San Diego, Calif, USA, October 2008.

[53] X. Gao, T.-T. Ng, B. Qiu, and S. F. Chang, "Single-view recaptured image detection based on physics-based features," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '10)*, pp. 1469–1474, IEEE, July 2010.

[54] M. Goljan, J. Fridrich, and J. Lukáš, "Camera identification from printed images," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, E. J. Delp III, P. W. Wong, J. Dittmann, and N. D. Memon, Eds., vol. 6819 of *Proceedings SPIE*, San Jose, Calif, USA, January 2008.

[55] X. Gao, B. Qiu, J. Shen, T. T. Ng, and Y. Q. Shi, "A smart phone image database for single image recapture detection," in *Proceedings of the 9th International Workshop on Digital Watermarking (IWDW '10)*, H.-J. Kim, Y. Q. Shi, and M. Barni, Eds., vol. 6526 of *Lecture Notes in Computer Science*, Springer, Seoul, Korea, October 2010.

[56] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 476–491, 2009.

[57] C.-H. Choi, M.-J. Lee, and H.-K. Lee, "Scanner identification using spectral noise in the frequency domain," in *Proceedings of the International Conference on Image Processing (ICIP '10)*, pp. 2121–2124, IEEE, Hong Kong, China, September 2010.

[58] N. Khanna and E. J. Delp, "Intrinsic signatures for scanned documents forensics: effect of font shape and size," in *Proceedings of the International Symposium on Circuits and Systems (ISCAS '10)*, pp. 3060–3063, IEEE, Paris, France, May-June 2010.

[59] A. E. Dirik, H. T. Sencar, and N. Memon, "Flatbed scanner identification based on dust and scratches over scanner platen," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1385–1388, IEEE, Taipei, Taiwan, April 2009.

[60] S. Dehnie, T. Sencar, and N. Memon, "Digital image forensics for identifying computer generated and digital camera images," in *Proceedings of the IEEE International Conference on Image Processing I(CIP '06)*, pp. 2313–2316, IEEE, October 2006.

[61] W. Li, T. Zhang, E. Zheng, and X. Ping, "Identifying photorealistic computer graphics using second-order difference statistics," in *Proceedings of the International Conference on Fuzzy Systems and Knowledge Discovery (FSKD '10)*, M. Li, Q. Liang, L. Wang, and Y. Song, Eds., pp. 2316–2319, IEEE, 2010.

[62] A. E. Dirik, S. Bayram, H. T. Sencar, and N. D. Memon, "New features to identify computer generated images," in *Proceedings of the IEEE International Conference on Image Processing (ICIP '07)*, vol. 4, pp. 433–436, IEEE, 2007.

[63] F. Pan and J. Huang, "Discriminating computer graphics images and natural images using hidden markov tree model," in *Proceedings of the 9th International Workshop on Digital Watermarking (IWDW '10)*, H.-J. Kim, Y. Q. Shi, and M. Barni, Eds., vol. 6526 of *Lecture Notes in Computer Science*, pp. 23–28, Springer, Seoul, Korea, October 2010.

[64] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 1, 1992.

[65] Z. Fan and R. de Queiroz, "Maximum likelihood estimation of JPEG quantization table in the identification of bitmap compression history," in *Proceedings of the International Conference on Image Processing (ICIP '00)*, pp. 948–951, September 2000.

[66] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 230–235, 2003.

[67] Z. Wang, A. C. Bovik, and B. L. Evans, "Blind measurement of blocking artifacts in images," in *Proceedings of the International*

*Conference on Image Processing (ICIP '00)*, vol. 3, pp. 981–984, 2000.

[68] H. Liu and I. Heynderickx, "A no-reference perceptual blockiness metric," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '08)*, pp. 865–868, March- April 2008.

[69] S. Tjoa, W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Block size forensic analysis in digital images," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '07)*, pp. I633–I636, April 2007.

[70] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 480–491, 2010.

[71] W. S. Lin, S. K. Tjoa, H. V. Zhao, and K. J. R. Liu, "Digital image source coder forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 460–475, 2009.

[72] S. Ye, Q. Sun, and E. C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07)*, pp. 12–15, IEEE, Beijing, China, July 2007.

[73] R. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R. G. Baraniuk, "JPEG compression history estimation for color images," *IEEE Transactions on Image Processing*, vol. 15, no. 6, pp. 1365–1378, 2006.

[74] F. Benford, "The law of anomalous numbers," *Proceedings of the American Philosophical Society*, vol. 78, no. 4, pp. 551–572, 1938.

[75] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," in *Proceedings of the 9th Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, vol. 6505 of *Proceedings SPIE*, pp. 1–11, San Jose, Calif, USA, January 2007.

[76] B. Li, Y. Q. Shi, and J. Huang, "Detecting doubly compressed JPEG images by using mode based first digit features," in *Proceedings of the IEEE 10th Workshop on Multimedia Signal Processing (MMSP '08)*, pp. 730–735, October 2008.

[77] X. Feng and G. Doërr, "JPEG recompression detection," in *Media Forensics and Security II*, vol. 7541 of *Proceedings of the SPIE*, January 2010, 75410J.

[78] T. Pevný and J. Fridrich, "Detection of double-compression for applications in steganography," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 247–258, 2008.

[79] J. Lukáš and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proceedings of the Digital Forensics Research Conference (DFRWS '03)*, 2003.

[80] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proceedings of the 6th International Workshop on Information Hiding*, pp. 128–147, Springer, Berlin, Germany, 2004.

[81] J. He, Z. Lin, L. Wang, and X. Tang, "Detecting doctored JPEG images via DCT coefficient analysis," *Lecture Notes in Computer Science*, vol. 3953, pp. 423–435, 2006.

[82] T. Pevny and J. Fridrich, "Estimation of primary quantization matrix for steganalysis of double-compressed JPEG images," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819 of *Proceedings of SPIE*, January 2008, 681911.

[83] Z. Lin, J. He, X. Tang, and C. K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition*, vol. 42, no. 11, pp. 2492–2501, 2009.

[84] T. Bianchi, A. D. Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '11)*, pp. 2444–2447, May 2011.

[85] H. Farid, "Exposing digital forgeries from JPEG ghosts," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 154–160, 2009.

[86] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '07)*, vol. 2, pp. 217–220, April 2007.

[87] M. Barni, A. Costanzo, and L. Sabatini, "Identification of cut & paste tampering by means of double-JPEG detection and image segmentation," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '10)*, pp. 1687–1690, IEEE, Paris, France, May-June 2010.

[88] Y. L. Chen and C. T. Hsu, "Image tampering detection by blocking periodicity analysis in JPEG compressed images," in *Proceedings of the IEEE 10th Workshop on Multimedia Signal Processing (MMSP '08)*, pp. 803–808, October 2008.

[89] Z. Qu, W. Luo, and J. Huang, "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '08)*, pp. 1661–1664, IEEE, Las Vegas, Nev, USA, March-April 2008.

[90] T. Bianchi and A. Piva, "Detection of non-aligned double jpeg compression with estimation of primary compression parameters," in *Proceedings of the 18th IEEE International Conference on Image Processing (ICIP '11)*, pp. 1929–11932, September 2011.

[91] T. Bianchi and A. Piva, "Detection of nonaligned double jpeg compression based on integer periodicity maps," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 842–848, 2012.

[92] T. Bianchi and A. Piva, "Analysis of non-aligned double jpeg artifacts for the localization of image forgeries," in *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS '11)*, pp. 1–6, November-December 2011.

[93] M. Xian-zhe, N. Shao-zhang, and Z. Jian-chen, "Tamper detection for shifted double jpeg compression," in *Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '10)*, pp. 434–437, October 2010.

[94] Y. L. Chen and C. T. Hsu, "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 396–406, 2011.

[95] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of jpeg artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1003–1017, 2012.

[96] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copymove forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, 2003.

[97] W. Q. Luo, J. W. Huang, and G. P. Qiu, "Robust detection of regionduplication forgery in digital image," in *Proceedings of the International Conference on Pattern Recognition (ICPR '06)*, pp. 746–749, 2006.

[98] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515,

Dartmouth College, Computer Science, Hanover, NH, USA, 2004.

[99] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1053–1056, IEEE, Taipei, Taiwan, April 2009.

[100] Q. Wu, S. Wang, and X. Zhang, "Detection of image regionduplication with rotation and scaling tolerance," in *Proceedings of the International Conference on Computer and Computational Intelligence (ICCCI '10)*, J.-S. Pan, S.-M. Chen, and N. T. Nguyen, Eds., vol. 6421 of *Lecture Notes in Computer Science*, pp. 100–108, 2010.

[101] H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," in *Proceedings of the Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA '08)*, vol. 2 of *IEEE Computer Society*, pp. 272–276, Wuhan, China, December 2008.

[102] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proceedings of the International Conference on Computer Vision (ICCV '99)*, pp. 1150–1157, 1999.

[103] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, and G. Serra, "Geometric tampering estimation by means of a sift-based forensic analysis," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 1702–1705, IEEE, Dallas, Tex, USA, March 2010.

[104] X. Pan and S. Lyu, "Detecting image region duplication using sift features," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 1706–1709, IEEE, Dallas, Tex, USA, March 2010.

[105] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, 2005.

[106] M. Kirchner, "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue," in *Proceedings of the 10th ACM Workshop on Multimedia and Security (MM&Sec '08)*, A. D. Ker, J. Dittmann, and J. J. Fridrich, Eds., pp. 11–20, ACM, September 2008.

[107] M. Kirchner and T. Gloe, "On resampling detection in recompressed images," in *Proceedings of the 1st IEEE International Workshop on Information Forensics and Security (WIFS '09)*, pp. 21–25, December 2009.

[108] M. Kirchner, "On the detectability of local resampling in digital images," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, E. J. Delp, P. W. Wong, J. Dittmann, and N. Memon, Eds., vol. 6819 of *Proceedings of SPIE*, February 2008.

[109] M. Kirchner, "Linear row and column predictors for the analysis of resized images," in *Proceedings of the 12th ACM Multimedia Security Workshop (MM&Sec '10)*, pp. 13–18, September 2010.

[110] S. Prasad and K. R. Ramakrishnan, "On resampling detection and its application to detect image tampering," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '06)*, pp. 1325–1328, July 2006.

[111] B. Mahdian and S. Saic, "On periodic properties of interpolation and their application to image authentication," in *Proceedings of the International Symposium on Information Assurance and Security*, pp. 439–446, 2007.

[112] W. Weimin, W. Shuozhong, and T. Zhenjun, "Estimation of rescaling factor and detection of image splicing," in *Proceedings of the 11th IEEE International Conference on Communication Technology (ICCT '08)*, pp. 676–679, November 2008.

[113] N. Dalgaard, C. Mosquera, and F. Pérez-González, "On the role of differentiation for resampling detection," in *Proceedings of the International Conference on Image Processing (ICIP '10)*, pp. 1753–1756, The Institute of Electrical and Electronics Engineers, Hong Kong, China, September 2010.

[114] G. S. Song, Y. I. Yun, and W. H. Lee, "A new estimation approach of resampling factors using threshold-based peak detection," in *Proceedings of the IEEE International Conference on Consumer Electronics (ICCE '11)*, pp. 731–732, January 2011.

[115] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 529–538, 2008.

[116] B. Mahdian and S. Saic, "A cyclostationarity analysis applied to image forensics," in *Proceedings of the Workshop on Applications of Computer Vision (WACV '09)*, pp. 1–6, December 2009.

[117] D. Vazquez-Padín, C. Mosquera, and F. Pérez-González, "Two-dimensional statistical test for the presence of almost cyclostationarity on images," in *Proceedings of the 17th IEEE International Conference on Image Processing (ICIP '10)*, pp. 1745–1748, September 2010.

[118] D. Vazquez-Padín and F. Pérez-González, "Prefilter design for forensic resampling estimation," in *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS '11)*, November-December 2011.

[119] M. Kirchner and J. J. Fridrich, "On detection of median filtering in digital images," in Memon et al," in *Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium*, N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. Delp, Eds., vol. 7541 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2010, 754110.

[120] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 215–2224, 2010.

[121] H.-D. Yuan, "Blind forensics of median filtering in digital images," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1335–11345, 2011.

[122] M. C. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in *Proceedings of the International Conference on Image Processing (ICIP '08)*, pp. 3112–3115, IEEE, San Diego, Calif, USA, October 2008.

[123] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 1698–1701, IEEE, Dallas, Tex, USA, March 2010.

[124] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492–506, 2010.

[125] S. Avidan and A. Shamir, "Seam carving for content-aware image resizing," *ACM Transactions on Graphics*, vol. 26, no. 3, article 10, 2007.

[126] A. Sarkar, L. Nataraj, and B. S. Manjunath, "Detection of seam carving and localization of seam insertions in digital images," in *Proceedings of the 11th ACM Multimedia Security Workshop (MM&Sec '09)*, pp. 107–116, September 2009.

[127] C. Fillion and G. Sharma, "Detecting content adaptive scaling of images for forensic applications," in *Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium*, N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. Delp, Eds., vol. 7541 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2010, 75410.

[128] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "A classifier design for detecting image manipulations," in *Proceedings of the International Conference on Image Processing (ICIP '04)*, pp. 2645–2648, October 2004.

[129] W. Chen, Y. Q. Shi, and W. Su, "Image splicing detection using 2-D phase congruency and statistical moments of characteristic function," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, Proceedings of SPIE, February 2007.

[130] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," in *Proceedings of the ACM Workshop on Multimedia Security (MM&Sec '07)*, D. Kundur, B. Prabhakaran, J. Dittmann, and J. J. Fridrich, Eds., pp. 51–62, ACM, 2007.

[131] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in *Proceedings of the ACM Workshop on Multimedia and Security*, pp. 1–10, 2005.

[132] M. K. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in *Proceedings of the 9th International Conference on Information Hiding*, T. Furon, F. Cayre, G. J. Doërr, and P. Bas, Eds., vol. 4567 of *Lecture Notes in Computer Science*, pp. 311–325, Springer, 2007.

[133] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 450–461, 2007.

[134] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," in *Proceedings of the International Conference on Information Hiding*, pp. 66–80, 2010.

[135] W. Zhang, X. Cao, J. Zhang, J. Zhu, and P. Wang, "Detecting photographic composites using shadows," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 1042–1045, IEEE, 2009.

[136] Q. Liu, X. Cao, C. Deng, and X. Guo, "Identifying image composites through shadow matte consistency," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1111–1122, 2011.

[137] H. Farid and J. Kosecka, "Estimating planar surface orientation using bispectral analysis," *IEEE Transactions on Image Processing*, vol. 16, no. 8, pp. 2154–2160, 2007.

[138] M. K. Johnson and H. Farid, "Detecting photographic composites of people," in *Proceedings of the International Workshop on Digital Watermarking*, pp. 19–33, 2007.

[139] V. Conotter and G. Boato, "Detecting photo manipulation on signs and billboards," in *Proceedings of the International Conference on Image Processing (ICIP '10)*, pp. 1741–1744, IEEE, Hong Kong, China, September 2010.

[140] P. Kakar, N. Sudha, and W. Ser, "Exposing digital image forgeries by detecting discrepancies in motion blur," *IEEE Transactions on Multimedia*, vol. 13, no. 3, pp. 443–452, 2011.

[141] H. Yao, S. Wang, Y. Zhao, and X. Zhang, "Detecting image forgery using perspective constraints," *IEEE Signal Processing Letters*, vol. 19, pp. 123–1126, 2012.

[142] M. Kirchner and R. Böhme, "Tamper hiding: defeating image forensics," in *Proceedings of the 9th International Conference on Information Hiding*, T. Furon, F. Cayre, G. Doerr, and P. Bas, Eds., pp. 326–341, 2007.

[143] M. Kirchner and R. Böhme, "Hiding traces of resampling in digital images," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 582–592, 2008.

[144] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?" in *Proceedings of the 15th international Conference on Multimedia*, pp. 78–86, 2007.

[145] M. Goljan, J. Fridrich, and M. Chen, "Defending against fingerprint-copy attack in sensor-based camera identification," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 227–236, 2011.

[146] R. Caldelli, I. Amerini, and A. Novi, "An analysis on attacker actions in fingerprint-copy attack in source camera identification," in *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS '11)*, pp. 1–6, November-December 2011.

[147] M. Kirchner and R. Böhme, "Synthesis of color filter array pattern in digital images," in *Media Forensics and Security*, E. J. Delp, J. Dittmann, N. Memon, and P. W. Wong, Eds., vol. 7254 of *Proceedings of SPIE*, 2009.

[148] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 1694–1697, March 2010.

[149] M. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1050–1065, 2011.

[150] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "The cost of jpeg compression anti-forensics," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '11)*, pp. 1884–1887, May 2011.

[151] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, "Countering jpeg anti-forensics," in *Proceedings of the 18th IEEE International Conference on Image Processing (ICIP '11)*, pp. 1949–1952, September 2011.

[152] S. Lai and R. Böhme, "Countering counter-forensics: the case of jpeg compression," in *Proceedings of the 13th International Conference on Information Hiding (IH '11)*, pp. 285–298, Springer, Berlin, Heidelberg, 2011.

[153] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *Proceedings of the 17th IEEE International Conference on Image Processing (ICIP '10)*, pp. 2109–2112, September 2010.

[154] M. Barni, M. Fontani, and B. Tondi, "A universal technique to hide traces of histogram-based image manipulations," in *Proceedings of the 14th ACM Workshop on Multimedia and Security (MM&SEC '12)*, September 2012.

[155] M. Barni, "A game theoretic approach to source identification with known statistics," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '12)*, pp. 1745–1748, March 2012.

[156] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensics versus anti-forensics: a decision and game theoretic framework," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '12)*, pp. 1749–1752, March 2012.

[157] O. Celiktutan, B. Sankur, and I. Avcibas, "Blind identification of source cell-phone model," *IEEE Transactions on Information Foren- Sics and Security*, vol. 3, no. 3, pp. 553–566, 2008.

[158] M. Kharrazi, H. T. Sencar, and N. D. Memon, "Improving steganalysis by fusion techniques: a case study with image steganography," *Transactions on Data Hiding and Multimedia Security*, vol. 4300, pp. 123–137, 2006.

[159] S. Bayram, I. Avcibaş, B. Sankur, and N. Memon, "Image manipulation detection," *Journal of Electronic Imaging*, vol. 15, no. 4, Article ID 041102, 2006.

[160] M. Fontani, T. Bianchi, A. de Rosa, A. Piva, and M. Barni, "A dempster-shafer framework for decision fusion in image

forensics," in *Proceedings of the IEEE International Workshop on Forensics and Security (WIFS '11)*, pp. 1–6, November-December 2011.

[161] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, NJ, USA, 1976.

[162] M. Barni and A. Costanzo, "A fuzzy approach to deal with uncertainty in image forensics," *Signal Processing: Image Communication*, vol. 27, no. 9, pp. 998–1010, 2012.