Signal Processing: *Image Communication* 25 (2010) 389–399

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

A bibliography on blind methods for identifying image forgery ☆

Babak Mahdian *, Stanislav Saic

Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod Vodárenskou věží 4, 182 08 Prague 8, Czech Republic

ARTICLE INFO

Article history:
Received 2 June 2009
Accepted 6 May 2010

Keywords:
Image forensics
Digital forgery
Image tampering
Blind forgery detection
Multimedia security

ABSTRACT

Verifying the integrity of digital images and detecting the traces of tampering without using any protecting pre-extracted or pre-embedded information have become an important and hot research field. The popularity of this field and the rapid growth in papers published during the last years have put considerable need on creating a complete bibliography addressing published papers in this area. In this paper, an extensive list of blind methods for detecting image forgery is presented. By the word blind we refer to those methods that use only the image function. An attempt has been made to make this paper complete by listing most of the existing references and by providing a detailed classification group.

1. Introduction

Verifying the integrity of digital images and detecting the traces of tampering without using any protecting pre-extracted or pre-embedded information have become an important and hot research field of image processing. The popularity of this field and the rapid growth in papers published in recent years have put considerable need on creation a complete paper showing existing methods. The present paper represents a comprehensive list of references on blind methods for detecting image forgery. By word blind we refer to those methods using only and only the image function to perform the forgery detection task. Though there are some other published surveys, many of existing blind methods for detecting image forgery are uncited and remain unidentified.

In this article we do not contemplate to go into details of particular methods or describe results of comparative experiments. This work also does not contain articles from popular press or papers only giving general information about image forensics. We will try to directly jump into the core topic of the paper. We hope that this work will help the researchers from the image processing community to find new research problems and solutions. An attempt has been made to make this paper complete by listing most of the existing references.

The authors have tried to design a detailed classification group and fit the presented references into this classification. To assist readers in "going to the source", seminal contributions are identified within the literature published in English. If identified sources are available only in another language (most likely Chinese), we always mention this. To the best knowledge of the authors, this bibliography appears to be the most complete published source of references on blind methods for detecting image forgery.

1.1. Motivation

The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. The art of making image fakery has a long history. But, in today's digital age, it is possible to very easily change the information represented by an image without leaving any obvious traces of tampering (see Fig. 1).

☆ This work has been supported by the Czech Science Foundation under the projects no. GACR 102/08/0470 and GACR P202/10/P509.

* Corresponding author.
E-mail addresses: mahdian@utia.cas.cz (B. Mahdian), ssaic@utia.cas.cz (S. Saic).

0923-5965/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.image.2010.05.003

Fig. 1. Some examples of recent image forgeries.

The digital information revolution and issues concerned with multimedia security have also generated several approaches to tampering detection. Generally, these approaches could be divided into active and passive-blind approaches. The area of active methods simply can be divided into the data hiding approach [121,139,140] and the digital signature approach [119,135,78,72].

By data hiding we refer to methods embedding secondary data into the image. The most popular group of this area belongs to digital watermarks [1,106,94,115]. Digital watermarking assumes an inserting of a digital watermark at the source side (e.g., camera) and verifying the mark integrity at the detection side. Watermarks mostly are inseparable from the digital image they are embedded in, and they undergo the same transformations as the image itself. A major drawback of watermarks is that they must be inserted either at the time of recording the image, or later by a person authorized to do so. This limitation requires specially equipped cameras or subsequent processing of the original image. Furthermore, some watermarks may degrade the image quality.

The digital signature approach consists mainly of extracting unique features from the image at the source side and encoding these features to form digital signatures. Afterwards signatures are used to verify the image integrity. Signatures have similar disadvantages as the data hiding group.

In this work, we focus on blind methods, as they are regarded as a new direction and in contrast to active methods they do not need any prior information about the image. Blind methods are mostly based on the fact that forgeries can bring into the image specific detectable changes (e.g., statistical changes). In high quality forgeries, these changes cannot be found by visual inspection. Existing methods mostly try to identify various traces of tampering and detect them separately. The final decision about the forgery can be carried out by fusion of results of separate detectors.

2. Blind methods for detecting image forgery

Citations are classified into several categories and listed, for each category, in alphabetical order according to the first author.

2.1. Existing surveys

There have been published several surveys on image forensics: [30] by Hany Farid, [64] by Tran Van Lanh et al., [83] by Weiqi Luo et al., [87] by Babak Mahdian and Stanislav Saic, [102] by Tian-Tsong Ng and Shih-Fu Chang, [120] by Taha Sencar and Nasir Memon and [141] by Qiong Wu (in Chinese).

Despite these existing surveys, most of the existing blind methods for detecting forgeries are uncited and remain unidentified. Our huge effort in this paper was to include all the existing references that directly deal with blind image forensics.

2.2. Near-duplicated image regions

Detection of near-duplicated image regions may signify copy–move (copy-paste) forgery. In this type of forgery, a part of the image is copied and pasted into another part of the same image typically with the intention to hide an object or a region.

In [8], Sevinc Bayram et al. proposed a clone detector based on Fourier–Mellin transform of the image's blocks. The Fourier–Mellin transform is invariant with respect to scale and rotation. This allows a better behavior of the method when dealing with slightly resized and rotated cloned regions. In [23], Brandon Dybala et al. proposed a cloning detection method based on a filtering operation and nearest neighbor search. Jessica Fridrich et al. [37] proposed a method detecting copy–move forgery using discrete cosine transform of overlapping blocks and their lexicographical representation. Hailing Huang et al. [50] used the SIFT algorithm to detect the cloned regions in the image. SIFT features are stable with respect to changes in illumination, rotation and scaling. Aaron Langille and Minglun Gong [63] proposed a method searching for blocks with similar intensity patterns based on a kd-tree. Guohui Li et al. [69] proposed a duplicated regions detection method based on wavelet transform and singular value decomposition. Weihai Li et al. [70] using a copy–move detector for JPEG images based on blocking artifacts. Hwei J. Lin et al. [73] proposed a method using radix sort. In [80], Weiqi Luo et al. proposed a copy–move forgery detection method based on seven intensity-based characteristics features. Babak Mahdian and Stanislav Saic [85] proposed a method for detecting near-duplicated regions based on moment invariants, principal component analysis and kd-tree. A.N. Myna [95] proposed a method using the idea of log-polar coordinates and wavelet transforms. Alin C. Popescu and Hany Farid [108] proposed a method based on representing image blocks using principal components analysis. In [9] Bravo S. Sergio and Asoke K. Nandi proposed a near-duplication detection method based on log-polar coordinates. The method is invariant with respect to reflection, rotation or scaling. Jing Zhang et al. [146] proposed a copy–move detection method based on wavelet transform and phase correlation.

Although these methods are capable of detecting near-duplicates parts of the image, their computational time is very high and typically they produce a high number of false positives. Furthermore, a human interpretation of the results is necessary.

2.3. Interpolation and geometric transformations

When two or more images are spliced together to create high quality and consistent image forgeries, geometric transformations are almost always needed. These transformations, typically, are based on the resampling of a portion of an image onto a new sampling lattice. This requires an interpolation step, which typically brings into the signal statistical changes. Detecting these specific statistical changes may signify tampering.

Claude S. Fillion and Gaurav Sharma [33] analyzed the detection of content adaptive resizing. They proposed a technique capable of detecting the presence of seam-carving. In [41], Andrew Gallagher proposed a method for detecting digitally zoomed images. The method is based on the periodicity in the second derivative signal of interpolated images. In [61], Matthias Kirchner proposed a resampling detection method based on linear filtering and cumulative periodograms. In [93], Matthias Kirchner and Thomas Gloe analyzed resampling detection in re-compressed JPEG images. Qingzhong Liu and Andrew H. Sung [77] proposed a method for detecting resized JPEG images. Their work is based on neighboring joint density features of the DCT coefficients and classification relying on support vector machines. The paper shows blocking artifacts can help to increase the resampling detection performance in JPEG compressed images. Babak Mahdian and Stanislav Saic [86,91] proposed a method for detecting the traces of interpolation based on a derivative operator and radon transformation. The same authors, in another work [89] analyzed the usefulness of cyclostationarity theory in image forensics and proposed a local cyclostationarity detector to find the traces of scaling and rotation. Methods dealing with detection of interpolation have weak results when dealing with JPEG images. Therefore, Lakshmanan Nataraj et al. [96] proposed a method for detecting JPEG resized images. The method is based on addition of a suitable amount of Gaussian noise to the image so that the periodicity due to JPEG compression is suppressed while that due to the resizing is retained. In order to detect the traces of resampling, Alin C. Popescu and Hany Farid [109] analyzed the imperceptible specific correlations brought into the resampled signal by the interpolation step and proposed a resampling detector based on an expectation/maximization algorithm. S. Prasad and K.R. Ramakrishnan [112] analyzed several spatial and frequency domain techniques to detect the traces of resampling. Their most promising method is based on zero-crossings of the second difference signal. Anindya Sarkar et al. [118] proposed a machine learning based framework for detection of seam carving. The framework is based on the Markov features, consisting of 2-D difference histograms in the block-based DCT domain. In [138], Weimin Wei et al. proposed a method for estimation of the rescaling factor. The method is based on periodic artifacts brought into the signal by the interpolation process. In [143] (in Chinese), Zhu Xiu Ming et al. proposed a resampling detector based on expectation/maximization algorithm.

The mentioned methods mostly are efficient when the image being analyzed is in a non-compressed format. Artifacts of JPEG compression typically conceal the traces of interpolation.

2.4. Image splicing

When dealing with the photomontage detection problem, one of the fundamental tasks is the detection of image splicing. Image splicing assumes cut and paste of image regions from one image onto the another image.

To detect image splicing, Dong et al. [22] proposed a support vector machine based method. Their features are gained by analyzing the discontinuity of image pixel correlation and coherency caused by splicing. In [26], Hany Farid proposed how to detect un-natural higher-order correlations introduced into the signal by the tampering process. The method is based on bispectral analysis. In [49,48], Yu-Feng Hsu and Shih-Fu Chang proposed a method based on camera response function estimated from geometry invariants. E.S. Gopi et al. [44,45] proposed how to detect forgeries using an artificial neural network, independent component analysis and auto-regressive coefficients. Wang Jing and Zhang Hongbin [52] proposed a method for detecting image splicing based on a Sobel edge detector, a derivative operation and a Hough transform. Micah K. Johnson and Hany Farid [55] proposed how to detect compositing of two or more people into a single image based on estimating the camera's principal point from the image of a person's eyes. Zhouchen Lin et al. [76] proposed a method based on computing the inverse camera response functions by analyzing the edges in different patches of the image and verifying their consistency. Tian-Tsong Ng and Shih-Fu Chang [99] proposed and studied an image-splicing model based on the idea of bipolar signal perturbation. The same authors in [103] proposed a method for detecting the abrupt splicing discontinuity using bicoherence features. In [105,98], Tian-Tsong Ng and Mao-Pei Tsui proposed an edge-profile-based method for extracting CRF signature from a single image. Yun Q. Shi et al. analyzed image splicing in [38,16,122,123]. The proposed methods are based on Hilbert–Huang transform [38], statistics of 2-D phase congruency [16] and a natural image model to classify spliced images from authentic images [122]. Wei Wang et al. [136] proposed an image splicing detection method based on gray level co-occurrence matrix (GLCM) of thresholded edge image of image chroma. Zhen Zhang et al. [150] proposed a splicing detection scheme based on moment features extracted from the discrete cosine transform and image quality features.

Many of the mentioned methods work well when the image being analyzed is compressed by a high quality factor. Otherwise, the compression artifacts make the localization of the forgery very difficult.

2.5. Computer graphics and paintings

In today's digital age, high quality computer graphics look so photorealistic that it is difficult to visually differentiate them from real images. Since this technique can also be used to create convincing image forgeries, there is a need to have sophisticated methods distinguishing between computer graphics and photographic images.

To detect computer graphics, in [117], Dongmei Chen et al. used the wavelet decomposition coefficients of natural images. In particular, the fractional lower order moments in the image wavelet domain are extracted and evaluated with the support vector machines. In [18], Sintayehu Dehnie et al. presented an approach by focusing on the imaging sensor's pattern noise. Shih-Fu Chang et al. [101] proposed a geometry-based image model motivated by the physical image generation process for classifying photographic images and photorealistic computer graphics. Authors also deployed an online system for distinguishing photographic and computer graphic images [100,104]. In [19], Emir Dirik et al. investigated the problem of identifying photo-realistic computer generated and real images by introducing features to detect the presence of color filter array demosaicking and chromatic aberration. In [59], Nitin Khanna et al. proposed a method based on residual pattern noise. Alex Leykin et al. [66] offer to use edge properties features for effectively differentiate paintings from photographs. In [67], Alex Leykin et al. found that photographs differ from paintings in their color, edge, and texture properties. Based on these features, they trained and tested a classifier for distinguishing paintings from photographs. Siwei Lyu and Hany Farid [84] proposed a statistical model for photographic images consisting of first and higher-order wavelet statistics. Anderson Rocha et al. [116] proposed a method identifying computer generated images using progressive randomization. Gopinath Sankar et al. [117] proposed a framework for differentiating between computer graphics and real images based on an aggregate of other existing features and a feature selection procedure. Yun Q. Shi et al. [124] proposed a method using features formed by using statistical moments of characteristic function of wavelet subbands and their prediction errors. Patchara Sutthiwan et al. [128] used statistical moments of 1-D and 2-D characteristic functions to derive image features that can distinguish between computer graphics and photographic images. In [142], Qiong Wu et al. proposed a method based on zero-connectivity and fuzzy membership to detect forged regions in inpainted images.

Methods pointed out in this section work well for non-compressed images or JPEG images with a high quality factor. Otherwise, they typically fail.

2.6. JPEG and compression properties

In order to alter an image, typically the image must be loaded onto a photo-editing software and after the changes are done, the digital image is re-saved. Sophisticated methods capable of finding the image's compression history can be helpful in forgery detection.

In [3], Sebastiano Battiato and Giuseppe Messina experimentally analyzed some of weakness and strength points of the current solutions based on DCT and JPEG properties. Yi L. Chen and Chiou T. Hsu [17] proposed a quantization noise model to characterize single and doubly compressed images. In [25], Zhigang Fan and Ricardo Queiroz proposed a method determining whether an image has been previously JPEG compressed. If so, compression parameters are estimated. Specifically, a method for the maximum likelihood estimation of JPEG quantization steps was developed. In [29] Hany Farid proposed a method for detecting composites created by JPEG images of different qualities. The method detects whether a part of an image was initially compressed at a lower quality than the rest of the image. Xiaoying Feng and Gwenael Doerr [32] detect double JPEG images by using periodic artifacts of re-quantization and discontinuities in the signal histogram. Jan Lukáš and Jessica Fridrich [35] presented a method for estimation of primary quantization matrix from a double compressed JPEG image. The paper presents three different approaches from which the Neural Network classifier based one is the most effective. Tomáš Pevný and Jessica Fridrich [36] proposed a method based on support vector machine classifiers with feature vectors formed by histograms of low-frequency DCT coefficients. Dongdong Fu et al. [39] proposed a statistical model based on Benford's law for the probability distributions of the first digits of the block-DCT and quantized JPEG coefficients. Based on the assumption that block operation create disparities across block boundaries, Chang-Tsun Li [68] proposed a method for analyzing the properties of image's blocks. In [75] Zhouchen Lin et al. examined the double quantization effect hidden among the DCT coefficients and proposed a method insensitive to different kinds of forgery methods such as alpha matting or inpainting. Sabrina Lin et al. [74] proposed a method allowing estimating which kind of source encoder has been applied on the input image. Weiqi Luo et al. [82] proposed a method for detecting recompressed image blocks based on JPEG blocking artifact characteristics. The same authors also proposed a detection method [81] for identifying the blocking artifacts. The method is based on cross-differential filter and maximum-likelihood estimation. Babak Mahdian and Stanislav Saic [90] proposed a method for detection double compressed JPEG images based on histograms properties of DCT coefficients and support vector machines. Ramesh Neelamani et al. [97] proposed a method to estimate the JPEG compression history. Alin C. Popescu [111] proposed a double JPEG Compression technique by examining the histograms of the DCT coefficients. In [113], Zhenhua Qu et al. formulated the shifted double JPEG compression as a noisy convolutive mixing model to identify whether a given JPEG image has been compressed twice with inconsistent block segmentation. Matthew Sorell [125] has explored the conditions under which primary quantization coefficients can be identified. Steven Tjoa et al. [133] proposed a method for determining which transform was used during compression. The method is

based on analyzing the histograms of coefficient sub-bands. Steven Tjoa et al. [134] proposed a block size estimation scheme making on the nature of prior image compression or processing. Shuiming Ye et al. [144] proposed a forgery detection method checking image quality inconsistencies based on blocking artifacts caused by JPEG compression. Jing Zhang et al. [147] proposed a method for detecting JPEG 2000. The method is based on the statistical difference in the sub-band discrete wavelet transform coefficient histograms between single and double JPEG 2000 compression.

A typical advantage of the methods in this group is their good response for detecting re-saved images. The problem is that often images only are rotated, resized, enhanced (e.g. contrast), re-saved, etc. So, only the knowledge that image has been re-saved often is not enough.

2.7. Color filter array and inter pixel correlation

Many digital cameras are equipped with a single charge-coupled device (CCD) or complementary metal oxide semiconductor (CMOS) sensor. The color images are typically obtained in conjunction with a color filter array. At each pixel location only a single color sample is captured. Missing colors are computed by an interpolating process, called Color Filter Array (CFA) Interpolation. The tampering process can destroy the specific correlations brought into images pixels by CFA interpolation.

In [13,12], Hong Cao and Alex C. Kot proposed a demosaicing regularity detection method based on partial second-order derivative correlation models which detect both the intrachannel and the cross-channel demosaicing correlation. In [20], Ahmet E. Dirik and Nasir Memon proposed two features analyzing traces of CFA. The paper shows the successful application of features for tamper detection and for distinguishing between computer graphics and real images. In [24], Na Fan et al. proposed a neural network based method for analyzing the traces of CFA. In [40], Andrew Gallagher and Tsuhan Chen proposed a method based on detection of the presence of demosaicing to detect forgeries. In [51], Yizhen Huang and Yangjing Long proposed a decision mechanism using BP neural networks and a majority-voting scheme for demosaicking correlation recognition and digital photo authentication. The method also distinguishes the digital camera photographs from computer graphics. Marie-Charlotte Poilpré et al. [107] described a method for detecting the traces of Bayer CFA interpolation. The method searches for CFA related peaks in the Fourier domain. Alin C. Popescu and Hany Farid [110] described the specific correlations brought by the CFA interpolation into the image and proposed a method capable of their automatic detection. The method is based on an expectation/maximization (EM) algorithm and uses a linear model. Ashwin Swaminathan et al. [130,132] technique to find the camera's color array pattern and the color interpolation methods. The estimated interpolation coefficients allow to determine the brand and model of the camera from which an image was captured.

One of the most important drawbacks of methods pointed out in this section is their weak results for stronger JPEG compression. Otherwise, they are able to localize the doctored parts of the image with a good precision.

2.8. Lighting

Different photographs are taken under different lighting conditions. Thus, when two or more images are spliced together to create an image forgery, it is often difficult to match the lighting conditions from the individual photographs. Therefore detecting lighting inconsistencies can propose an another proper way to find traces of tampering.

Under certain simplifying assumptions, arbitrary lighting environments can be modeled with a nine-dimensional model based on a linear combination of spherical harmonics. In [56], Micah K. Johnson and Hany Farid have shown how to approximate a lower-order five-dimensional version of this model and how to estimate the model's parameters from a single image. Another work from same authors focuses on image forgeries created by splicing photographs of different people [57]. Authors suggest how the direction to a light source can be estimated from specular highlights that appear on the eye. In [31], Hany Farid and Mary J. Bravo described several computational methods for detecting inconsistencies in shadows and reflections. Sandeep Gholap and P.K. Bora [42] proposed a method to find the forgery in digital images by estimation of the illuminant color. In [149], Wei Zhang et al. described how image composites can be detected by enforcing the geometric and photometric constraints from shadows. In particular, they explored shadow relations that are modeled by the planar homology and the color characteristics of the shadows measured by the shadow matte.

A very important advantage of this group is that it is not easy to conceal the traces of inconsistencies in lighting conditions. The disadvantage of the group is the necessary human interpretation of the results.

2.9. Local noise

Additive noise is a commonly used tool to conceal the traces of tampering and is the main cause of failure of many active or passive forgery detection methods. Often by creating digital image forgeries, noise becomes inconsistent. Therefore, the detection of various noise levels in an image may signify tampering.

In [46], Hongmei Gou et al. proposed a method based on three sets of statistical noise features. Their features are based on an image denoising algorithm, wavelet analysis and a neighborhood prediction. Babak Mahdian and Stanislav Saic [92,88] proposed a method for detecting local image noise inconsistencies based on estimating local noise variance using wavelet transform and a segmentation step. In [111], Alin C. Popescu proposed a method based on measuring the local noise variance using the second and fourth moments.

Typically, these methods work well when the level of noise is noticeably different in various parts of the image. Their common problem is their high rate of false positives.

2.10. Chromatic aberration

Optical imaging systems are not ideal and often bring different types of aberrations into the captured images. Chromatic aberration is caused by the failure of the optical system to perfectly focus light of all wavelengths. By the tampering process, the aberration can become inconsistent across the image. This can be used as another way to detect image forgeries.

Ahmat E. Dirik et al. [19] proposed a simple method for detecting the presence of chromatic aberration. The method is based on an upscaling operation and mutual information. In [43], Thomas Gloe et al. analyzed the lateral chromatic aberration and proposed a low-cost estimator of this abberation. Furthermore, test results based on an image database are provided. In [53], Micah K. Johnson and Hany Farid proposed a model describing the relative positions at which light of varying wavelength strikes the sensor. The model parameters are estimated using an automatic technique based on maximizing the mutual information between color channels.

Methods dealing with chromatic aberration work well for non-compressed non-uniform parts of the image. For the uniform regions of the image or typical JPEG images we can expect weak results.

2.11. Image processing operations

When altering an image, very often a combination of basic image processing operations is applied to the images. Detecting traces of these operations can be very helpful in identifying forgeries.

Ismail Avcibas et al. [2] proposed a method that discriminates between original and processed images. Here, the work is based on training a classifier with image quality features called generalized moments. In [5,4], Ismail Avcibas et al. used several sets of features for detecting various common image processing operations by constructing classifiers using features based on binary similarity measures, image quality metrics, higher-order wavelet statistics and a feature selection approach. In [28], Hany Farid proposed three techniques for detecting traces of image processing operations in scientific images. Specifically, image segmentation techniques are employed to detect image deletion, healing, and duplication. In [62], Matthias Kirchner and Jessica Fridrich analyzed the detection of median filtering in digital images. Jan Lukáš [79] analyzed usefulness of basic filtering techniques for detection of tampering. Some tampering operations can be approximated as a combination of linear and non-linear components. Ashwin Swaminathan et al. [129,131] modeled the linear part of the tampering process as a filter, and obtained its coefficients using blind deconvolution. These estimated coefficients are then used to identify possible manipulations.

Probably the most common problem of the methods in this section is their weak results for stronger JPEG compression.

2.12. Blur and sharpening

Often forgeries are created by combination of two or more source images. So, finding in an image various regions with different blur characteristics (blur inconsistencies) can be helpful in detection image forgeries. Furthermore, blur operation is one of the commonly used methods to conceal the traces of tampering.

Gang Cao et al. [11] proposed a local blur estimator for measuring the blurriness of pixels along image's edges. In [10], the same authors proposed a method for detecting sharpened images. The method is based on histogram gradient aberration and ringing artifacts metric. In [47], Dun-Yu Hsiao et al. proposed a tampering detection method based on blur estimation (using images DCT coefficients). In [71] Zhe Li and Jiang-bin Zheng proposed a method based on the local entropy of the gradient. In [114], Zhenhua Qu et al. proposed an image splicing detector based on the sharp splicing boundaries. In [126], Matthew Stamm and K.J. Ray Liu proposed a method detecting global contrast enhancement operations. The method uses artifacts introduced into an image's histogram during the enhancement operations. Yagiz Sutcu et al. [127] proposed a forgery detection method based on regularity properties of wavelet coefficients used for estimating sharpness and blurriness of edges. Xin Wang et al. [137] proposed an image forgery detection based on the consistency of defocus blur. The method uses local blur estimation at edge pixels. In [151], Jiangbin Zheng and Miao Liu proposed a method for detecting a traces of artificial blur. Their work is based on a wavelet homomorphic filtering and a mathematical morphology procedure. Chi Zhang and Hongbin Zhang proposed in [145] a forgery detection method based on analyzing the presence of traces of feather operation used to create a smooth transition between the forged region and its surroundings. Linna Zhou et al. [152] proposed a method for detection of blurred edges. The method is based on edge preserving smoothing filtering and mathematical morphology.

Unfortunately, most of the methods pointed out in this section need a human interpretation of the output.

2.13. Projective geometry

When two or more images are spliced together it can often be difficult to keep the appearance of the image's correct perspective. Thus, applying the principles from projective geometry to problems in image forgery detection can be also a proper way to detect traces of tampering.

Micah K. Johnson and Hany Farid [54] proposed three techniques for estimating the transformation of a plane imaged under perspective projection. Using this transformation, a planar surface can be rectified to be frontoparallel, providing a useful forensic tool. In [148], Wei Zhang

et al. described a technique for detecting image composites by analyzing two-view geometrical constrains.

A very important advantage of this approach is that it is hard to conceal the traces of inconsistencies in projective geometry. Difficulties for automation create one of the main drawbacks of this approach.

2.14. Semantic content of image

Analyzing the semantic content of the image can have a crucial role in image forgery detection.

Sangwon Lee et al. [65] suggest to find perceptually meaningful regions using an image segmentation technique and by using a common-sense reasoning techniques to find ambiguities and anomalies within an image.

A disadvantage of this approach is the need of human interpretation of the results.

2.15. Acquisition device analysis and identification

It is important to note that there also are other groups of forensic methods effective in forgery detection. For example, methods analyzing the image acquisition device have been shown to be very helpful. These methods mostly are based on sensor noise (for instance, Jessica Fridrich et al. [34,15] analyzed how photo-response nonuniformity (PRNU) of imaging sensors can be used for a variety of image forensic tasks including forgery localization), demosaicking artifacts (for example, Sevinc Bayram et al. [6], Mehdi Kharrazi et al. [60], Sevinc Bayram et al. [7], Ashwin Swaminathan et al. [132] used the traces of demosaicing to analyze the camera), sensor dust characteristics (e.g., Ahmet Emir Dirik et al. [21] showed that the location and shape of dust specks in front of the imaging sensor and their persistence make dust spots a useful fingerprint for digital single lens reflex cameras), JPEG properties (for instance, Hany Farid [27,58] proposed to use the quantization tables to distinguish between original and modified photos), etc. Furthermore, there also are methods dealing with identification of source cell-phones (for instance, Oya Celiktutan et al. [14] used binary similarity measures, image quality measures and higher order wavelet statistics to achieve this goal). Typically, a common drawback of these methods is that when the origin (acquisition device) of the image being analyzed is unknown, they cannot be applied. If the acquisition device is known, mostly they need have available a set of other images from the same particular device or at least from the same device model.

3. Discussion

To our best knowledge, this paper is the most complete published source of references on blind methods for detecting image forgery. We believe that it can help researches dealing with image forensics to find new promising ideas and to help the image processing community to find new research challenges.

Without any doubt, recent years have brought a significant improvement to the field of blind image forgery detection. But, in spite of this improvement and higher number of methods, we still can see a lot of drawbacks and imperfections of the existing methods.

When leaving the "ideal" lab conditions and applying the existing methods to real-life applications, the variety of image contents and characteristics cause considerably higher false positive rates (true images denoted as forgeries) than which are reported in the existing papers. Generally, the problem of false positives exists in all research fields and applications. But, image forensics mostly deals with the trustworthiness of photographs having an essential value (for instance, the trustworthiness of photographs as evidence in courtrooms). Therefore, in real-life applications, the problem of false positives can have catastrophical consequences.

Another drawback of existing methods is the problem of automation. Many of the method outputs need a human interpretation. For instance, when copy–move forgery (duplicated regions) detection methods are applied to real-life photos, we easily recognize that almost all real-photos contain some near-duplicated regions (sky, clouds, reads, walls, etc.).

Generally, we can state that the state-of-the-art of image forensics allows for detecting the presence of image modification in a considerably higher accuracy than the localization of the forgery in the image. Unfortunately, often the information whether the image has been altered or not is not enough. Images are typically rotated, resized, enhanced, re-saved, etc. So, the knowledge what operations the image being analyzed have undergone is often very desirable. To be able to localize the forgery, existing methods mostly need to have an "big enough" modified region containing some inconsistencies.

Still it is relatively easy to create undetectable image forgeries using existing methods. Many of existing methods deal with JPEG and compression properties. But, for instance, when analyzing images in media, almost all professional photographers (photographers who contribute to news agencies and journals) take photos using the raw file format. Typically, they enhance (and modify) the image in the raw format and then convert the photo to the JPEG file format. So, in such cases all methods dealing with JPEG artifacts are meaningless. Typically, localization of forgery in JPEG images is possible when the image content is regular and the modified region previously had a lower JPEG quality factor than the current JPEG quality factor.

When dealing with methods detecting geometric transformations and color filter array Interpolation, they lose their effectiveness when the analyzed image is saved using a lower JPEG quality factor. When dealing with methods analyzing additional noise, blurriness or computer graphics, they often produce many false positives when they are used locally.

Image forensics is a burgeoning research field and despite the limitations of existing methods, it promises a significant improvement in forgery detection in the never-ending competition between image forgery creators and image forgery detectors.

As a suggestion for the potential future work, it can be mentioned here that there is a need to generate a common test images database. This will enable researchers to train,

test, and evaluate their methods much easier. Furthermore, there is a need to develop further novel and sophisticated analyzing methods allowing for detection of forgery from different points of view. Another challenging task will be improving the reliability and robustness issues of methods.

References

[1] M. Arnold, M. Schmucker, S.D. Wolthusen, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, Inc., Norwood, MA, USA, 2003.

[2] I. Avcibas, S. Bayram, N.D. Memon, M. Ramkumar, B. Sankur, A classifier design for detecting image manipulations, in: ICIP, 2004, pp. 2645–2648.

[3] S. Battiato, G. Messina, Digital forgery estimation into dct domain: a critical analysis, in: MiFor '09: Proceedings of the First ACM Workshop on Multimedia in Forensics, ACM, New York, NY, USA, 2009, pp. 37–42.

[4] S. Bayram, I. Avcibas, B. Sankur, N. Memon, Image manipulation detection with binary similarity measures, in: Proceedings of 13th European Signal Processing Conference, vol. 1, Antalya, Turkey, 2005, pp. 752–755.

[5] S. Bayram, I. Avcibas, B. Sankur, N. Memon, Image manipulation detection, Journal of Electronic Imaging 15 (4) (December 2006) 041102-1–041102-17.

[6] S. Bayram, H.T. Sencar, N.D. Memon, Classification of digital camera-models based on demosaicing artifacts, Digital Investigation 5 (1–2) (2008) 49–59.

[7] S. Bayram, H.T. Sencar, N.D. Memon, I. Avcibas, Source camera identification based on cfa interpolation, in: ICIP (3), 2005, pp. 69–72.

[8] S. Bayram, H. Taha Sencar, N. Memon, An efficient and robust method for detecting copy–move forgery, in: ICASSP '09: Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Computer Society, Washington, DC, USA, 2009, pp. 1053–1056.

[9] S. Bravo-Solorio, A.K. Nandi, Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling, in: European Signal Processing Conference, 2009, pp. 824–828.

[10] G. Cao, Y. Zhao, R. Ni, Detection of image sharpening based on histogram aberration and ringing artifacts, in: IEEE International Conference on Multimedia and Expo, 2009, pp. 1026–1029.

[11] G. Cao, Y. Zhao, R. Ni, Edge-based blur metric for tamper detection, Journal of Information Hiding and Multimedia Signal Processing 1 (1) (2010) 20–27.

[12] H. Cao, A.C. Kot, A generalized model for detection of demosaicing characteristics, in: ICME, 2008, pp. 1513–1516.

[13] H. Cao, A.C. Kot, Accurate detection of demosaicing regularity for digital image forensics, IEEE Transactions on Information Forensics and Security 4 (4) (2009) 899–910.

[14] O. Celiktutan, I. Avcibas, B. Sankur, Blind identification of source cell-phone model, IEEE Transactions on Information Forensics and Security 3 (3) (September 2008) 553–566.

[15] M. Chen, M. Goljan, J. Lukas, Determining image origin and integrity using sensor noise, IEEE Transactions on Information Forensics and Security 3 (1) (March 2008) 74–90.

[16] W. Chen, Y.Q. Shi, W. Su, Image splicing detection using 2-d phase congruency and statistical moments of characteristic function, in: SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, USA, January 2007.

[17] Y.-L. Chen, C.-T. Hsu, Detecting doubly compressed images based on quantization noise model and image restoration, in: IEEE Workshop on Multimedia Signal Processing, 2009.

[18] S. Dehnie, H.T. Sencar, N.D. Memon, Digital image forensics for identifying computer generated and digital camera images, in: ICIP, IEEE, Atlanta, USA, 2006, pp. 2313–2316.

[19] A.E. Dirik, S. Bayram, H.T. Sencar, N. Memon, New features to identify computer generated images, in: IEEE International Conference on Image Processing, ICIP '07, vol. 4, 2007, pp. 433–436.

[20] A.E. Dirik, N. Memon, Image tamper detection based on demosaicing artifacts, in: ICIP (09), Cairo, Egypt, November 2009, pp. 429–432.

[21] A.E. Dirik, H.T. Sencar, N. Memon, Digital single lens reflex camera identification from traces of sensor dust, IEEE Transactions on Information Forensics and Security 3 (3) (September 2008) 539–552.

[22] J. Dong, W. Wang, T. Tan, Y. Shi, Run-length and edge statistics based approach for image splicing detection, in: Digital Watermarking, 7th International Workshop, IWDW 2008, Busan, Korea, November 10-12, 2008, pp. 76–87.

[23] B. Dybala, B. Jennings, D. Letscher, Detecting filtered cloning in digital images, MM&Sec '07: Proceedings of the 9th Workshop on Multimedia & Security, ACM, New York, NY, USA, 2007, pp. 43–50.

[24] N. Fan, C. Jin, Y. Huang, A pixel-based digital photo authentication framework via demosaicking inter-pixel correlation, in: MM& Sec '09: Proceedings of the 11th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2009, pp. 125–130.

[25] Z. Fan, R.L. de Queiroz, Identification of bitmap compression history: jpeg detection and quantizer estimation, IEEE Transactions on Image Processing 12 (2) (2003) 230–235.

[26] H. Farid, Detecting digital forgeries using bispectral analysis, Technical Report AIM-1657, AI Lab, Massachusetts Institute of Technology, 1999.

[27] H. Farid, Digital image ballistics from JPEG quantization, Technical Report TR2006-583, Department of Computer Science, Dartmouth College, 2006.

[28] H. Farid, Exposing digital forgeries in scientific images, in: ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.

[29] H. Farid, Exposing digital forgeries from jpeg ghosts, IEEE Transactions on Information Forensics and Security 1 (4) (2009) 154–160.

[30] H. Farid, A survey of image forgery detection, IEEE Signal Processing Magazine 2 (26) (2009) 16–25.

[31] H. Farid, M. Bravo, Image forensic analyses that elude the human visual system, in: SPIE Symposium on Electronic Imaging, San Jose, CA, 2010.

[32] X. Feng, G. Doerr, Jpeg recompression detection, in: SPIE Conference on Media Forensics and Security, 2010.

[33] C.S. Fillion, G. Sharma, Detecting content adaptive scaling of images for forensic applications, in: Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security XII, 2010.

[34] J. Fridrich, Digital image forensics, IEEE Signal Processing Magazine 2 (26) (2009) 26–37.

[35] J. Fridrich, J. Lukas, Estimation of primary quantization matrix in double compressed jpeg images, in: Proceedings of DFRWS, vol. 2, Cleveland, OH, USA, August 2003.

[36] J. Fridrich, T. Pevny, Detection of double-compression for applications in steganography, IEEE Transactions on Information Security and Forensics 3 (2) (June 2008) 247–258.

[37] J. Fridrich, D. Soukal, J. Lukas, Detection of copy–move forgery in digital images, in: Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, Cleveland, OH, USA, August 2003, pp. 55–61.

[38] D. Fu, Y.Q. Shi, W. Su, Detection of image splicing based on Hilbert–Huang transform and moments of characteristic functions with wavelet decomposition, in: International Workshop on Digital Watermarking, Jeju, Korea, November 2006, pp. 177–187.

[39] D. Fu, Y.Q. Shi, W. Su, A generalized Benford's law for jpeg coefficients and its applications in image forensics, in: SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, USA, January 2007.

[40] A. Gallagher, T. Chen, Image authentication by detecting traces of demosaicing, in: Proceedings of the CVPR WVU Workshop, Anchorage, AK, USA, June 2008, pp. 1–8.

[41] A.C. Gallagher, Detection of linear and cubic interpolation in jpeg compressed images, in: CRV '05: Proceedings of the 2nd Canadian Conference on Computer and Robot Vision (CRV'05), IEEE Computer Society, Washington, DC, USA, 2005, pp. 65–72.

[42] S. Gholap, P.K. Bora, Illuminant colour based image forensics, in: TENCON 2008—2008, TENCON 2008. IEEE Region 10 Conference, IEEE Computer Society, Hyderabad, India, November 2008, pp. 1–5.

[43] T. Gloe, A. Winkler, K. Borowka, Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics, in: SPIE Conference on Media Forensics and Security, 2010.

[44] E.S. Gopi, Digital image forgery detection using artificial neural network and independent component analysis, Applied Mathematics and Computation 194 (2) (2007) 540–543.

[45] E.S. Gopi, N. Lakshmanan, T. Gokul, S. KumaraGanesh, P.R. Shah, Digital image forgery detection using artificial neural network and auto regressive coefficients, in: CCECE, 2006, pp. 194–197.

[46] H. Gou, A. Swaminathan, M. Wu, Noise features for image tampering detection and steganalysis, in: ICIP (6), IEEE, San Antonio, USA, 2007, pp. 97–100.

[47] D.-Y. Hsiao, S.-C. Pei, Detecting digital tampering by blur estimation, in: SADFE '05: Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) on Systematic Approaches to Digital Forensic Engineering, IEEE Computer Society, Washington, DC, USA, 2005, p. 264.

[48] Y.-F. Hsu, S.-F. Chang, Detecting image splicing using geometry invariants and camera characteristics consistency, in: ICME, 2006, pp. 549–552.
[49] Y.-F. Hsu, S.-F. Chang, Image splicing detection using camera response function consistency and automatic segmentation, in: ICME, 2007, pp. 28–31.
[50] H. Huang, W. Guo, Y. Zhang, Detection of copy–move forgery in digital images using sift algorithm, in: PACIIA '08: Proceedings of the 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, IEEE Computer Society, Washington, DC, USA, 2008, pp. 272–276.
[51] Y. Huang, Y. Long, Demosaicking recognition with applications in digital photo authentication based on a quadratic pixel correlation model, in: IEEE Conference on Computer Vision and Pattern Recognition, Anchorage, AK, USA, 2008, pp. 1–8.
[52] W. Jing, Z. Hongbin, Exposing digital forgeries by detecting traces of image splicing, in: 8th International Conference on Signal Processing, Guilin, China, November 2006, pp. 16–20.
[53] M. Johnson, H. Farid, Exposing digital forgeries through chromatic aberration, in: ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.
[54] M. Johnson, H. Farid, Metric measurements on a plane from a single image, Technical Report TR2006-579, Department of Computer Science, Dartmouth College, 2006.
[55] M. Johnson, H. Farid, Detecting photographic composites of people, in: 6th International Workshop on Digital Watermarking, Guangzhou, China, 2007.
[56] M. Johnson, H. Farid, Exposing digital forgeries in complex lighting environments, IEEE Transactions on Information Forensics and Security 3 (2) (2007) 450–461.
[57] M. Johnson, H. Farid, Exposing digital forgeries through specular highlights on the eye, in: 9th International Workshop on Information Hiding, Saint Malo, France, 2007.
[58] E. Kee, H. Farid, Digital image authentication from thumbnails, in: Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security XII, 2010.
[59] N. Khanna, G.T.-C. Chiu, J.P. Allebach, E.J. Delp, Forensic techniques for classifying scanner, computer generated and digital camera images, in: IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, USA, April 2008, pp. 1653–1656.
[60] M. Kharrazi, H.T. Sencar, N.D. Memon, Blind source camera identification, in: ICIP, 2004, pp. 709–712.
[61] 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, ACM, New York, NY, USA, 2008, pp. 11–20.
[62] M. Kirchner, J. Fridrich, On detection of median filtering in digital images, in: Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA, USA, January 2010.
[63] A. Langille, M. Gong, An efficient match-based duplication detection algorithm, in: CRV '06: Proceedings of the 3rd Canadian Conference on Computer and Robot Vision (CRV'06), IEEE Computer Society, Washington, DC, USA, 2006, p. 64.
[64] T.V. Lanh, K.-S. Chong, S. Emmanuel, M.S. Kankanhalli, A survey on digital camera image forensic methods, in: ICME, 2007, pp. 16–19.
[65] S. Lee, D.A. Shamma, B. Gooch, Detecting false captioning using common-sense reasoning, Digital Investigation 3 (Suppl. 1) (2006) 65–70.
[66] A. Leykin, F. Cutzu, Differences of edge properties in photographs and paintings, in: ICIP (3), 2003, pp. 541–544.
[67] A. Leykin, F. Cutzu, H. Riad, Distinguishing paintings from photographs, Computer Vision and Image Understanding 100 (3) (2005) 249–273.
[68] C.-T. Li, Detection of block artifacts for digital forensic analysis, in: e-Forensics, 2009, pp. 173–178.
[69] G. Li, Q. Wu, D. Tu, S. Sun, A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd, in: ICME, 2007, pp. 1750–1753.
[70] W. Li, Y. Yuan, N. Yu, Detecting copy-paste forgery of jpeg image via block artifact grid extraction, in: International Workshop on Local and Non-Local Approximation in Image Processing, 2008.
[71] Z. Li, J. Bin Zheng, Blind detection of digital forgery image based on the local entropy of the gradient, in: IWDW, 2008, pp. 161–169.
[72] C.Y. Lin, S.F. Chang, Generating robust digital signature for image/video authentication, in: ACM Multimedia Workshop, 1998, pp. 115–118.
[73] H.-J. Lin, C.-W. Wang, Y.-T. Kao, Fast copy–move forgery detection, WSEAS Transactions on Signal Processing 5 (5) (2009) 188–197.
[74] W.-Y. Lin, S. Tjoa, H.V. Zhao, K.J.R. Liu, Image source coding forensics via intrinsic fingerprints, in: ICME, 2007, pp. 1127–1130.
[75] Z. Lin, J. He, X. Tang, C.-K. Tang, Fast, automatic and fine-grained tampered jpeg image detection via dct coefficient analysis, Pattern Recognition 42 (11) (2009) 2492–2501.
[76] Z. Lint, R. Wang, X. Tang, H.-Y. Shum, Detecting doctored images using camera response normality and consistency, in: CVPR '05: Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)—Volume 1, IEEE Computer Society, Washington, DC, USA, 2005, pp. 1087–1092.
[77] Q. Liu, A.H. Sung, A new approach for jpeg resize and image splicing detection, in: MiFor '09: Proceedings of the First ACM workshop on Multimedia in Forensics, ACM, New York, NY, USA, 2009, pp. 43–48.
[78] C.S. Lu, H.M. Liao, Structural digital signature for image authentication: an incidental distortion resistant scheme, in: MULTIMEDIA '00: Proceedings of the 2000 ACM workshops on Multimedia, ACM Press, New York, NY, USA, 2000, pp. 115–118.
[79] J. Lukas, Digital image authentication using image filtering techniques, in: Proceedings of ALGORITMY 2000, Conference on Scientific Computing, Podbanske, Slovakia, September 2000, pp. 236–244.
[80] W. Luo, J. Huang, G. Qiu, Robust detection of region-duplication forgery in digital image, in: ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition, IEEE Computer Society, Washington, DC, USA, 2006, pp. 746–749.
[81] W. Luo, J. Huang, G. Qiu, A novel method for block size forensics based on morphological operations, in: IWDW, 2008, pp. 229–239.
[82] W. Luo, Z. Qu, J. Huang, G. Qiu, A novel method for detecting cropped and recompressed image block, in: IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 2, Honolulu, HI, USA, April 2007, pp. 217–220.
[83] W. Luo, Z. Qu, F. Pan, J. Huang, A survey of passive technology for digital image forensics, Frontiers of Computer Science in China 1 (2) (2007) 166–179.
[84] S. Lyu, H. Farid, How realistic is photorealistic? IEEE Transactions on Signal Processing 53 (2) (2005) 845–850.
[85] B. Mahdian, S. Saic, Detection of copy–move forgery using a method based on blur moment invariants, Forensic Science International 171 (2–3) (2007) 180–189.
[86] B. Mahdian, S. Saic, Blind authentication using periodic properties of interpolation, IEEE Transactions on Information Forensics and Security 3 (3) (September 2008) 529–538.
[87] B. Mahdian, S. Saic, Blind methods for detecting image fakery, in: IEEE International Carnahan Conference on Security Technology, IEEE Computer Society, Prague, Czech Republic, October 2008, pp. 280–286.
[88] B. Mahdian, S. Saic, Detection of resampling supplemented with noise inconsistencies analysis for image forensics, in: International Conference on Computational Sciences and its Applications, IEEE Computer Society, Perugia, Italy, July 2008, pp. 546–556.
[89] B. Mahdian, S. Saic, A cyclostationarity analysis applied to image forensics, in: IEEE Workshop on Applications of Computer Vision (IEEE WACV), December 2009.
[90] B. Mahdian, S. Saic, Detecting double compressed jpeg images, in: The 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP-09), London, UK, December 2009.
[91] B. Mahdian, S. Saic, Detection and description of geometrically transformed digital images, in: Media Forensics and Security, Proceedings of SPIE-IS&T Electronic Imaging, vol. 7254, San Jose, CA, USA, January 2009.
[92] B. Mahdian, S. Saic, Using noise inconsistencies for blind image forensics, Image Vision Computing 27 (10) (2009) 1497–1503.
[93] T.G. Matthias Kirchner, On resampling detection in re-compressed images, in: IEEE Workshop on Information Forensics and Security, December 2009, pp. 21–25.
[94] P. Moulin, The role of information theory in watermarking and its application to image watermarking, Signal Processing 81 (6) (2001) 1121–1139.
[95] A.N. Myna, M.G. Venkateshmurthy, C.G. Patil, Detection of region duplication forgery in digital images using wavelets and log-polar mapping, in: ICCIMA '07: Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), IEEE Computer Society, Washington, DC, USA, 2007, pp. 371–377.
[96] L. Nataraj, A. Sarkar, B.S. Manjunath, Adding gaussian noise to denoise jpeg for detecting image resizing, in: International Conference on Image Processing, 2009, November 2009.

[97] R. Neelamani, R.L. de Queiroz, Z. Fan, S. Dash, R.G. Baraniuk, Jpeg compression history estimation for color images, IEEE Transactions on Image Processing 15 (6) (2006) 1365–1378.
[98] T.-T. Ng, Camera response function signature for digital forensics—part II: signature extraction, in: IEEE Workshop on Information Forensics and Security, December 2009, pp. 161–165.
[99] T.-T. Ng, S.-F. Chang, A model for image splicing, in: IEEE International Conference on Image Processing (ICIP), Singapore, October 2004.
[100] T.-T. Ng, S.-F. Chang, An online system for classifying computer graphics images from natural photographs, in: SPIE Electronic Imaging, San Jose, CA, January 2006.
[101] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, M.-P. Tsui, Physics-motivated features for distinguishing photographic images and computer graphics, in: MULTIMEDIA '05: Proceedings of the 13th Annual ACM International Conference on Multimedia, ACM, New York, NY, USA, 2005, pp. 239–248.
[102] T.-T. Ng, S.-F. Chang, C.-Y. Lin, Q. Sun, Passive-blind image forensics, in: W. Zeng, H. Yu, C.Y. Lin (Eds.), Multimedia Security Technologies for Digital Rights, Elsevier, Hawthorne, NY, USA, 2006.
[103] T.-T. Ng, S.-F. Chang, Q. Sun, Blind detection of photomontage using higher order statistics, in: IEEE International Symposium on Circuits and Systems (ISCAS), Vancouver, Canada, 2004.
[104] T.-T. Ng, S.-F. Chang, M.-P. Tsui, Lessons learned from online classification of photo-realistic computer graphics and photographs, in: IEEE Workshop on Signal Processing Applications for Public Security and Forensics (SAFE), April 2007.
[105] T.-T. Ng, M.-P. Tsui, Camera response function signature for digital forensics—part I: theory and data selection, in: IEEE Workshop on Information Forensics and Security, December 2009, pp. 156–160.
[106] N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain, Signal Processing 66 (3) (May 1998) 385–403.
[107] M.-C. Poilpré, P. Perrot, H. Talbot, Image tampering detection using Bayer interpolation and jpeg compression, in: e-Forensics '08: Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop, ICST, Brussels, Belgium, Belgium, 2008, pp. 1–5. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[108] A. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions, Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.
[109] A. Popescu, H. Farid, Exposing digital forgeries by detecting traces of re-sampling, IEEE Transactions on Signal Processing 53 (2) (2005) 758–767.
[110] A. Popescu, H. Farid, Exposing digital forgeries in color filter array interpolated images, IEEE Transactions on Signal Processing 53 (10) (2005) 3948–3959.
[111] A.C. Popescu, Statistical tools for digital image forensics, Ph.D. Thesis, Department of Computer Science, Dartmouth College, Hanover, NH, 2005.
[112] S. Prasad, K.R. Ramakrishnan, On resampling detection and its application to image tampering, in: Proceedings of the IEEE International Conference on Multimedia and Exposition, Toronto, Canada, 2006, pp. 1325–1328.
[113] Z. Qu, W. Luo, J. Huang, A convolutive mixing model for shifted double jpeg compression with application to passive image authentication, in: IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, USA, April 2008, pp. 4244–1483.
[114] Z. Qu, G. Qiu, J. Huang, Detect digital image splicing with visual cues, in: Information Hiding, 11th International Workshop, IH 2009, Darmstadt, Germany, June 8-10, 2009, pp. 247–261.
[115] C. Rey, J.-L. Dugelay, A survey of watermarking algorithms for image authentication, EURASIP Journal on applied Signal Processing 2002 (June 2002) 613–621 (special issue on image analysis for multimedia interactive services 2002).
[116] A. Rocha, S. Goldenstein, Is it fake or real? in: XIX Brazilian Symposium on Computer Graphics and Image Processing, Manaus, Brazil, April 2006.
[117] G. Sankar, V. Zhao, Y.-H. Yang, Feature based classification of computer graphics and real images, in: ICASSP '09: Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Computer Society, Washington, DC, USA, 2009, pp. 1513–1516.
[118] A. Sarkar, L. Nataraj, B.S. Manjunath, Detection of seam carving and localization of seam insertions in digital images, in: MM&Sec '09: Proceedings of the 11th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2009, pp. 107–116.
[119] M. Schneider, S.F. Chang, A robust content based digital signature for image authentication, in: IEEE International Conference on Image Processing (ICIP'96), 1996.
[120] H.T. Sencar, N. Memon, Overview of state-of-the-art in digital image forensics, Indian Statistical Institute Platinum Jubilee Monograph series titled Statistical Science and Interdisciplinary Research, December 2008, pp. 1–20.
[121] H.T. Sencar, M. Ramkumar, A.N. Akansu, Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia, Academic Press, Inc., Orlando, FL, USA, 2004.
[122] Y.Q. Shi, C. Chen, W. Chen, A natural image model approach to splicing detection, in: ACM Workshop on Multimedia and Security (ACM MMSEC07), ACM, New York, NY, USA, September 2007, pp. 51–62.
[123] Y.Q. Shi, C. Chen, G. Xuan, W. Su, Steganalysis versus splicing detection, in: International Workshop on Digital Watermarking (IWDW07), Guangzhou, China, December 2007.
[124] Y.Q. Shi, W. Chen, G. Xuan, Identifying computer graphics using hsv color model and statistical moments of characteristic functions, in: ICME, 2007, pp. 1123–1126.
[125] M. Sorell, Conditions for effective detection and identification of primary quantization of re-quantized jpeg images, in: e-Forensics '08: Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop, ICST, Brussels, Belgium, Belgium, 2008, pp. 1–6. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[126] M. Stamm, K. Liu, Blind forensics of contrast enhancement in digital images, in: IEEE International Conference on Image Processing, San Diego, CA, USA, 2008, pp.3112–3115.
[127] Y. Sutcu, B. Coskun, H.T. Sencar, N. Memon, Tamper detection based on regularity of wavelet transform coefficients, in: ICIP: IEEE International Conference on image Processing, IEEE, San Antonio, USA, 2007, pp. 397–400.
[128] P. Sutthiwan, J. Ye, Y.Q. Shi, An enhanced statistical approach to identifying photorealistic images, in: IWDW '09: Proceedings of the 8th International Workshop on Digital Watermarking, Springer-Verlag, Berlin, Heidelberg, 2009, pp. 323–335.
[129] A. Swaminathan, M. Wu, K.J.R. Liu, Image tampering identification using blind deconvolution, in: ICIP, 2006, pp. 2309–2312.
[130] A. Swaminathan, M. Wu, K.J.R. Liu, Nonintrusive component forensics of visual sensors using output images, IEEE Transactions on Information Forensics and Security 2 (1) (2007) 91–106.
[131] A. Swaminathan, M. Wu, K.J.R. Liu, Hiding traces of resampling in digital images, IEEE Transactions on Information Forensics and Security 3 (1) (March 2008) 101–117.
[132] A. Swaminathan, M. Wu, K.J.R. Liu, Component forensics, IEEE Signal Processing Magazine 26 (2) (March 2009) 38–48.
[133] S. Tjoa, W.-Y.S. Lin, K.J.R. Liu, Transform coder classification for digital image forensics, in: ICIP (6), 2007, pp. 105–108.
[134] S. Tjoa, W.-Y.S. Lin, H.V. Zhao, K.J.R. Liu, Block size forensic analysis in digital images, in: IEEE International Conference on Acoustics, Speech and Signal Processing, Honolulu, HI, USA, April 2007.
[135] C.-H. Tzeng, W.-H. Tsai, A new technique for authentication of image/video for multimedia applications, in: Proceedings of the 2001 Workshop on Multimedia and Security, ACM Press, New York, NY, USA, 2001, pp. 23–26.
[136] W. Wang, J. Dong, T. Tan, Effective image splicing detection based on image chroma, in: IEEE International Conference on Image Processing, 2009.
[137] X. Wang, B. Xuan, S. Long Peng, Digital image forgery detection based on the consistency of defocus blur, International Conference on Intelligent Information Hiding and Multimedia Signal ProcessingIEEE Computer Society, Los Alamitos, CA, USA, 2008, pp. 192–195.
[138] W. Weimin, W. Shuozhong, T. Zhenjun, Estimation of rescaling factor and detection of image splicing, in: 11th IEEE International Conference on Communication Technology, IEEE Computer Society, Hangzhou, China, 2008, pp. 676–679.
[139] M. Wu, Multimedia data hiding, Ph.D. Thesis, A dissertation presented to the faculty of Princeton university in candidacy for the degree of doctor of philosophy, June 2001.
[140] M. Wu, B. Liu, Multimedia Data Hiding, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.
[141] Q. Wu, G.-H. Li, D. Tu, S.-J. Sun, State of the art and prospects on blind digital image forensics technology based on authenticity detection, Acta Automatica Sinica (2008) ISSN=0254-4156.

[142] Q. Wu, S.-J. Sun, W. Zhu, G.-H. Li, D. Tu, Detection of digital doctoring in exemplar-based inpainted images, in: Seventh International Conference on Machine Learning and Cybernetics, Kunming, China, July 2008, pp. 1222–1226.
[143] Z. Xiu-ming, X. Guo-rong, Y. Qiu-ming, T. Xue-feng, S. Yung-qing, Re-sampling detection in information forensics, International Journal of Automation and Computing 26 (11) (2007) 2596–2597.
[144] S. Ye, Q. Sun, E.C. Chang, Detecting digital image forgeries by measuring inconsistencies of blocking artifact, in: ICME, 2007, pp. 12–15.
[145] C. Zhang, H. Zhang, Detecting digital image forgeries through weighted local entropy, in: IEEE International Symposium on Signal Processing and Information Technology, Giza, Egypt, December 2007, pp. 62–67.
[146] J. Zhang, Z. Feng, Y. Su, A new approach for detecting copy–move forgery in digital images, in: IEEE Singapore International Conference on Communication Systems, 2008, pp. 362–366.
[147] J. Zhang, H. Wang, Y. Su, Detection of double-compression in jpeg2000 images, in: IITA '08: Proceedings of the 2008 Second International Symposium on Intelligent Information Technology Application, IEEE Computer Society, Washington, DC, USA, 2008, pp. 418–421.
[148] W. Zhang, X. Cao, Z. Feng, J. Zhang, P. Wang, Detecting photographic composites using two-view geometrical constraints, in: IEEE International Conference on Multimedia and Expo, 2009, pp. 1078–1081.
[149] W. Zhang, X. Cao, J. Zhang, J. Zhu, P. Wang, Detecting photographic composites using shadows, in: IEEE International Conference on Multimedia and Expo, 2009, pp. 1042–1045.
[150] Z. Zhang, J. Kang, Y. Ren, An effective algorithm of image splicing detection, in: CSSE '08: Proceedings of the 2008 International Conference on Computer Science and Software Engineering, IEEE Computer Society, Washington, DC, USA, 2008, pp. 1035–1039.
[151] J. Zheng, M. Liu, A digital forgery image detection algorithm based on wavelet homomorphic filtering, in: IWDW, 2008, pp. 152–160.
[152] L. Zhou, D. Wang, Y. Guo, J. Zhang, Blur detection of digital forgery using mathematical morphology, in: KES-AMSTA '07: Proceedings of the 1st KES International Symposium on Agent and Multi-Agent Systems, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 990–998.