Digital Investigation 10 (2013) 226–245

Contents lists available at SciVerse ScienceDirect

Digital Investigation

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

Digital image forgery detection using passive techniques: A survey

Gajanan K. Birajdar [a,*], Vijay H. Mankar [b]

[a] Department of Electronics & Communication, Priyadarshini Institute of Engineering & Technology, Nagpur 440019, Maharashtra, India
[b] Department of Electronics & Telecommunication, Government Polytechnic, Nagpur 440001, Maharashtra, India

ARTICLE INFO

Article history:
Received 11 December 2012
Received in revised form 7 April 2013
Accepted 29 April 2013

Keywords:
Passive/blind image forgery detection
Image forensic
Image manipulation detection
Image authentication
Image tampering detection

ABSTRACT

Today manipulation of digital images has become easy due to powerful computers, advanced photo-editing software packages and high resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. Blind or passive methods do not need any explicit priori information about the image. First, various image forgery detection techniques are classified and then its generalized structure is developed. An overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed. The present status of image forgery detection technique is discussed along with a recommendation for future research.

1. Introduction to image forgery

The rapid growth of image processing softwares and the advancement in digital cameras has given rise to large amounts of doctored images with no obvious traces, generating a great demand for automatic forgery detection algorithms in order to determine the trustworthiness of a candidate image. A forgery detection algorithm should be passive, requiring no prior information about the image content or any protecting methods like watermarks.

According to the Wall Street Journal, 10% of all color photographs published in United States were actually digitally altered and retouched (Amsberry, 1989). The scientific community has also been subject to forgeries (Farid, 2006a; Pearson, 2005). The authenticity of photographs has an essential role as these photos are popularly used as supporting evidences and historical records in growing number and wide range of applications from forensic investigation, journalistic photography, criminal investigation, law enforcement, insurance claims and medical imaging. Image forgery has a long history (Rocha et al., 2011). As shown in Fig. 1, in todays digital world it is possible to create, alter and modify the information represented by an image very easily without leaving any obvious traces of these operations.

In recent years blind digital image forgery detection field has found significant interest from the scientific community. This is evident from the Fig. 2 which shows the number of papers related to digital image tampering detection that have been published in IEEE and Elsevier conferences and journals over the last 13 years. Due to the technological advancement in the recent years, law enforcement has needed to stay abreast of emerging technological advances and use these in the investigation of crime. The Scientific Working Group on Imaging Technology (SWGIT) provide recommendations and guidelines to law enforcement agencies and others in the criminal justice system regarding the best practices for photography, videography, and video and image analysis (https://

* Corresponding author. Pillai HOC College of Engg. & Technology, Rasayani, Raigad 410207, India. Tel.: +91 9224445046.
E-mail addresses: gajanan123@gmail.com, gajanan123@rediffmail.com (G.K. Birajdar), vhmankar@gmail.com (V.H. Mankar).

1742-2876/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2013.04.007

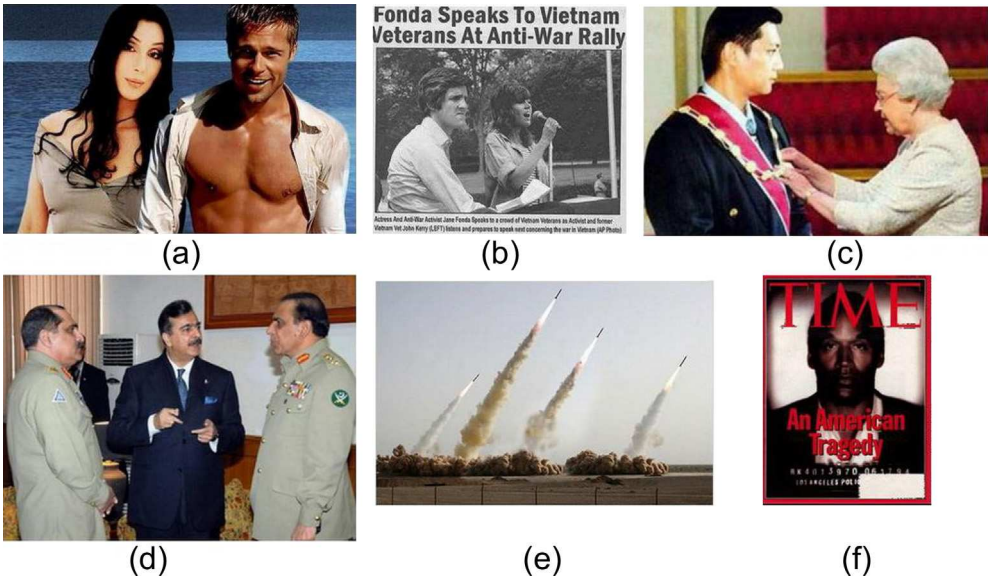

Fig. 1. Recent image forgeries reported (a) Composite of Cher and Brad Pitt (Johnson and Farid, 2005) (b) Photomontage of John Kerry and Jane Fonda (Johnson and Farid, 2005) (c) Jeffrey Wong Su En receiving the award from Queen Elizabeth II (Redi et al., 2011) (d) Pakistan prime minister Yousaf Gilani (www.fourandsix.com, 2012) (e) Iranian montage of missiles (Irene et al., 2011) (f) Time covers reporting on the O.J. Simpson case (Redi et al., 2011).

www.swgit.org/documents, 2012). SWGIT provides information on the appropriate use of various imaging technologies for use by personnel in the criminal justice system through the release of documents such as the SWGIT best practices documents.

Different image forgery detection techniques are classified in 1.1 and then generalized structure of image forgery detection is presented in 1.2. We then compared the performance of some typical image forgery detection algorithms. An overview of passive digital image authentication method is presented and the existing blind forgery detection techniques are reviewed. This papers focus is to classify various image forgery detection methods emphasizing on passive or blind techniques. We hope that this article will serve as a guide and help the researchers from the image forgery detection area to find new research problems.

1.1. Image forgery classification

Image forgery detection aims to verify the authenticity of a digital image. Image authentication solution is classified into two types. (1) Active and (2) Blind or passive. An active forgery detection techniques, such as digital watermarking or digital signatures uses a known authentication code embedded into the image content before the images are sent through an unreliable public channel. By verifying the presence of such authentication code authentication

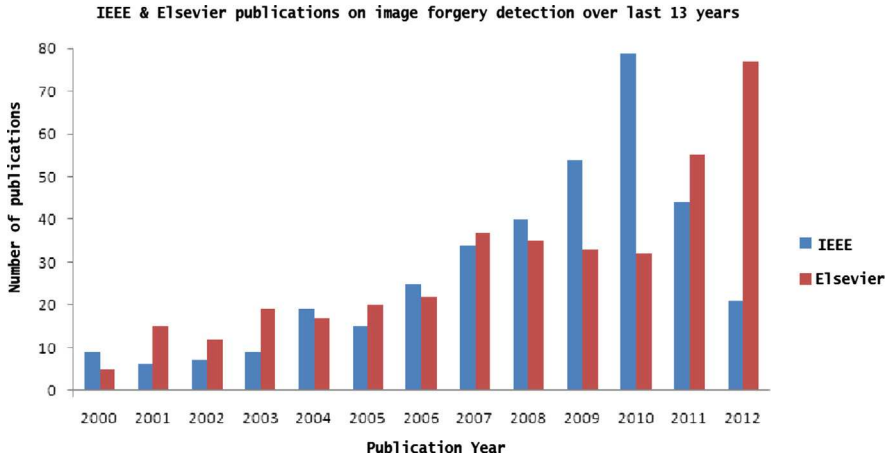

Fig. 2. Number of publications over last 13 years. Results obtained by submitting query "Image tampering detection" from IEEE (http://ieeexplore.ieee.org) and Elsevier (http://www.sciencedirect.com) websites.

may be proved by comparing with the original inserted code. However, this method requires special hardware or software to insert the authentication code inside the image before the image is being distributed.

Passive or blind forgery detection technique uses the received image only for assessing its authenticity or integrity, without any signature or watermark of the original image from the sender. It is based on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may highly likely disturb the underlying statistics property or image consistency of a natural scene image which introduces new artifacts resulting in various forms of inconsistencies. These inconsistencies can be used to detect the forgery. This technique is popular as it does not need any prior information about the image. Existing techniques identify various traces of tampering and detect them separately with localization of tampered region. Fig. 3 shows classification of image forgery detection techniques.

Several surveys have been published on image forgery detection: Rocha et al. (2011), Farid (2009a), Mahdian and Saic (2010), Lanh et al. (2007a), Luo et al. (2007a), Mahdian and Saic (2008a), Ng et al. (2006), Sencar and Memon (2008), Zhang et al. (2008a), Bayram et al. (2008a) and Redi et al. (2011). Still most of the image forgery techniques are remained unidentified and this articles objective is to explore all the existing blind forgery techniques and recent updates in this field.

1.2. Generalized structure of image forgery detection

Image forgery detection techniques are two-class classification techniques. Objective of blind or passive detection is to classify given images into two classes: original (or authentic) and forged images. Mostly existing blind image forgery detection approaches extract features from images first, then select a classifier and train the classifier using the features extracted from training image sets, and finally classify the features. Few such approaches are proposed in Luo et al. (2006), Mahdian and Saic (2007), Myna et al. (2007), Kirchner and Fridrich (2010), Cao et al. (2010a), Mahalakshmi et al. (2012) and Gul et al. (2010). Here, we describe a generalized framework of blind image forgery detection approach tentatively, which consists of the following major steps:

(1) *Image preprocessing*: Before feature extraction process some operations are performed over the images under consideration, such as cropping, transforming RGB image into grayscale, DCT or DWT transformation to improve the classification performance. (2) *Feature extraction*: A set of features are extracted for each class that helps distinguish it from other classes, while remaining invariant to characteristic differences within the class from the input forged data. In particular, extract informative features and select feature that must be sensitive to image manipulation. One of the desirable characteristic of selected features and constructed feature vector should be with low dimension, which will reduce the computational complexity of training and classification. (3) *Classifier selection and feature preprocessing*: Based on the extracted set of features select or design appropriate classifiers and choose a large set of images to train classifiers. Obtain some important parameters of classifiers, which can be utilized for the classification. Feature preprocessing is used to reduce the dimensionality of features without decreasing the machine learning based classification performance at the same time reduction in computational complexity (Sutthiwan et al., 2009b). (4) *Classification*: The purpose of classifier is to discriminate the given images and classify them into two categories: original and forged images. Various classifiers are used such as SVM in Lint et al. (2005), Fu et al. (2006), Chen et al. (2007), Shi et al. (2007a), Hsu and Chang (2006), Wang et al. (2009), Zhenhua et al. (2009), Dirik et al. (2007), Chen et al. (2008a) and Khanna et al. (2008) and LDA in Fang et al. (2009a). (5) *Postprocessing*: In some of the forgeries like copy move and splicing, postprocessing operation involves localization of forged region as investigated in Fridrich et al. (2003), Sergio and Asoke (2011), Muhammad et al. (2011), Gopi et al. (2006) and Ghorbani et al. (2011). According to the steps described above, the structure of blind image forgery detection is presented in Fig. 4.

2. Copy-move or region duplication forgery

Copy move is the most common image tampering technique used due to its simplicity and effectiveness, in which parts of the original image is copied, moved to a desired location and pasted. This is usually done in order to hide certain details or to duplicate certain aspects of an image. Textured regions are used as ideal parts for copy-move forgery, since textured areas have similar color and noise variation properties to that of the image which are unperceivable for human eye looking for inconsistencies in image statistical properties. Blurring is usually used along the border of the modified region to lessen the effect of irregularities between the original and pasted region.

First attempt in identifying tampered areas was investigated by Fridrich et al. (2003). The authors proposed a method of detecting copy-move forgery using discrete cosine transform (DCT) of overlapping blocks and their lexicographical representation to avoid the computational burden. Best balance between performance and complexity was obtained using block matching algorithm. Popescu and Farid (2004) presented a method using principal component analysis (PCA) for the representation of image segments i.e. overlapping square blocks. PCA-based detection results in reduction of the computational cost and the number of computations required are $O(N_t N \log N)$, where N_t is the dimensionality of the truncated PCA representation and N the number of image pixels. Average detection accuracies obtained was 50% when JPEG quality = 95 with block size of 32×32 and 100% when JPEG quality = 95 with block size of 160×160. Accuracy degrades for small block sizes and low JPEG qualities. To deal with computational complexity the use of k-dimensional tree was proposed by Langille and Gong (2006) in which a method searching for blocks with similar intensity patterns using matching techniques was used. The resulting algorithm has a complexity of $O(N_b N_s)$, where N_s = neighborhood search size and N_b = the number of blocks (which is a function of input image with resolution MN). Zero-normalized cross

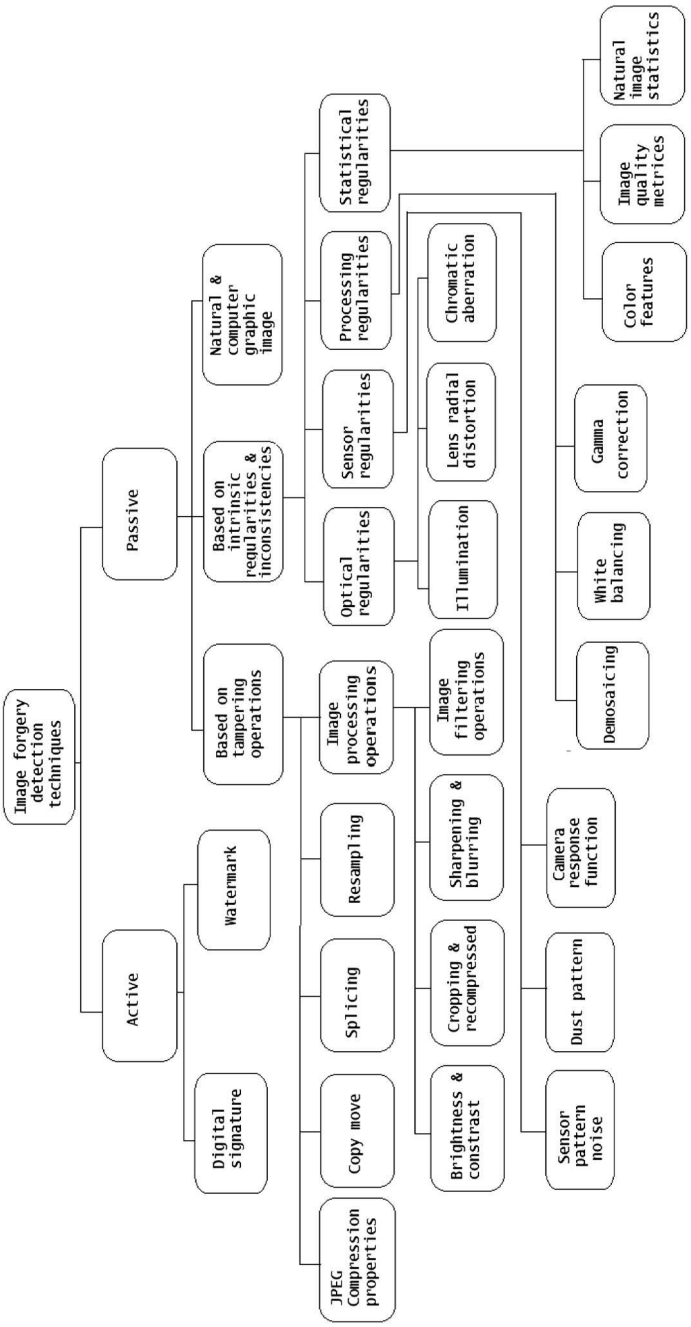

Fig. 3. Digital image forgery detection techniques classification.

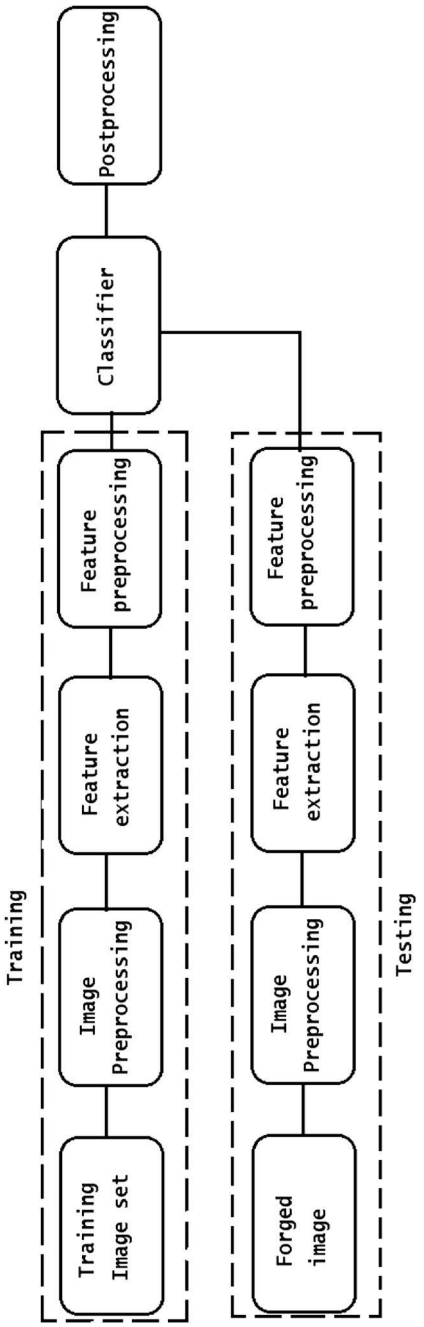

Fig. 4. Generalized structure of image forgery detection.

correlation (ZNCC) was used as a similarity measure and accurate detection results obtained through searching within at most 100 neighboring blocks in the sorted block array.

A copy-move forgery detection and localization method based on dividing an image into small overlapped blocks, then comparing the similarity of these blocks and finally identifying possible duplicated regions using intensity-based characteristics features was introduced by Luo et al. (2006). Illustrated algorithm has lower computational complexity and is more robust against stronger attacks and various types of after-copying manipulations, such as lossy compression, noise contamination, blurring and a combination of these operations resulting in accuracy of 0.9631 and false negative of 0.0966 in case of mixed operations. A method for detecting near-duplicated regions based on blur moment invariants, PCA and kd-tree was described by Mahdian and Saic (2007). To create the feature vector, algorithm uses 24 blur invariants up to the seventh order resulting in correct region duplication detection but major disadvantage of the method is its large computational time (Average run time is 30 min for 640×480 RGB image when block size of 24 and similarity threshold of 0.98).

Myna et al. (2007) developed a method using a log-polar coordinates and wavelet transforms to detect and localize copy-move forgery. Dimensionality reduction is obtained by applying wavelet transform to the input image and exhaustive search is performed to identify the similar blocks in the image by mapping them to log-polar coordinates and using phase correlation as the similarity criterion. Qiumin et al. (2011) employed log-polar fast Fourier transform (LPFFT) which is rotation and scale invariant with lower computational complexity of $O(n^2 \log n)$ where n is blocksize. A cloning detection method based on a filtering operation and nearest neighbor search was explored in Dybala et al. (2007). Li et al. (2007) used singular value decomposition (SVD) for feature vector dimensionality reduction and wavelet transform for duplicated regions detection. Duplicated regions were localized by lexicographically sorting and neighborhood detecting for all blocks even when the image was highly compressed or edge processed.

JPEG image forensics approach is implemented to detect copy-paste forgery based on the check of block artifact grid (BAG) mismatch by Li et al. (2008b) even when a JPEG image is truncated or multi-compressed. Scale invariant features transform (SIFT) features which are stable with respect to changes in illumination, rotation and scaling applied by Huang et al. (2008) to detect the cloned regions in the image. A method has good accuracy on different kind of post image processing like JPEG compression, rotation, noise, scaling and is also robust to compound image processing. A novel methodology based on SIFT is evaluated to estimate the geometric transformation parameters (horizontal and vertical translation, scaling factors and rotation angle) with high reliability in addition to detect forged image by Irene et al. (2011). The proposed method achieves true positive rate (TPR) of around 100%. The technique also utilized for splicing detection.

A copy-move detection approach based on wavelet transforms and phase correlation was created to estimate

the spatial offset between the copied region and the pasted region by Zhang et al. (2008a). But the performance relies on the location of copy-move regions. The Fourier-Mellin transform (FMT) features, which are invariant to scale and rotation was extracted and lexicographic sorting is used to detect copy move forgery by Bayram et al. (2009). The method is robust against various manipulation types (JPEG compression, rotation and scaling) in addition to this authors also presented a detection scheme that make use of counting bloom filters. Use of radix sort method was suggested by Lin et al. (2009a) to reduce the computational complexity in forged area detection. The radix sort method is used for sorting the feature vectors of the divided sub-blocks instead of lexicographic sorting, which improves time efficiency significantly at a slight decrease in the robustness. Detection rates obtained were in the range of 94–98% in presence of various manipulations.

Liu et al. (2011a) designed an efficient and robust passive authentication method that uses the circle block and the Hu moments to detect and locate the duplicate regions with rotation. Features are extracted from the first four Hu moments of the circle blocks in low frequency part of Gaussian pyramid decomposition to reduce the computational complexity. To perform an efficient search, overlapping blocks of pixels are mapped to 1-D descriptors derived from log-polar map for automated detection and localization of duplicated regions affected by reflection, rotation and scaling in images is focused in Sergio and Asoke (2011). Out of total 20 non-tampered test images algorithm detected 3 false matches (The number of images mistakenly classified as forgeries). A blind copy move image forgery detection method obtained in Muhammad et al. (2011) using dyadic wavelet transform (DyWT) which is shift invariant utilizing both the LL1 and HH1 subbands to find similarities and dissimilarities between the blocks of an image. Accuracy claimed is 95.9% with false positive of 4.54%.

Gopi et al. (2006) exploited auto regressive coefficients as the feature vector and artificial neural network (ANN) classifier to detect digital image forgery. 300 feature vectors from different images are used to train an ANN and the ANN is tested with another 300 feature vectors. Percentage of hit in identifying the digital forgery is 77.67% in experiment 1 in which manipulated images were used to train ANN and 94.83% in experiment 2 in which a database of forged images was used. An algorithm based on discrete wavelet transform (DWT) to reduce the dimension the image and DCT-quantization coefficients decomposition (DCT-QCD) to reduce the dimension of feature vector is illustrated by Ghorbani et al. (2011) to detect copy-move forgery.

Bashar et al. (2010) proposed a duplication detection approach that adopts two robust features based on DWT and kernel principal component analysis (KPCA). Multi-resolution wavelet coefficients and KPCA-based projected vectors corresponding to image-blocks are arranged into a matrix for lexicographic sorting. 'Translation – Flip' and 'Translation – Rotation' duplications are also detected using global geometric transformation and the labeling technique to identify the forgeries. XiaoBing and ShengMin (2008) identified the location of copy-move image tampering by applying SVD which served to produce algebraic and geometric invariant feature vectors. The proposed method has lower computational complexity, robust against retouching details and noise. Sutthiwan et al. (2010) presented a method for passive-blind color image forgery detection which is a combination of image features extracted from image luminance by applying a rake – transform and from image chroma by using edge statistics. The technique extracts multi-size block discrete cosine transform – Markov process (MBDCT-MP) features from Y-channel and support vector machine (SVM) with degree 2 polynomial kernel is employed for classification purpose resulting in almost 99% of accuracy.

Xunyu and Siwei (2011) developed a region duplication method by estimating the transform between matched SIFT keypoints that is robust to distortions based on image feature matching. The algorithm results in average detection accuracy of 99.08% but one of the limitation of the method is smaller region duplication is hard to detect as it has fewer keypoints. Kakar and Sudha (2012) described a novel technique based on transform-invariant features for detecting copy-paste forgeries with possible post-processing based on the MPEG-7 image signature tools. A feature matching process that utilizes the inherent constraints in matched feature pairs to improve the detection of cloned regions is used resulting in a feature matching accuracy in excess of 90% across postprocessing operations.

All the methods discussed above that are able to detect and locate detecting copy move forgery and near duplicates regions of the image, these are computationally expensive and a human interpretation of the results is necessary. Also, they introduce high false positives. Further, few techniques often fails to detect the forgery when the size of the forged area is much smaller than image dimensions.

3. Image splicing or image composites

Image splicing involves replacing of image fragments from one or more different images on to another image. Image splicing is one of the simple and commonly used image tampering schemes. Image splicing detection is of the fundamental task in image forgery detection.

The method based on bispectral analysis was introduced by Farid (1999) to detect un-natural higher-order correlations introduced into the signal by the tampering process and is successfully used for detecting human-speech splicing. Bicoherence is a normalized bispectrum. Ng and Chang (2004) developed an image-splicing detection model based on the use of bicoherence magnitude and phase features. The results of detection accuracy was about 70%. Later same authors proposed a method for detecting the abrupt splicing discontinuity using bicoherence features (Ng et al., 2004). Inverse camera response functions were computed by analyzing the edges in different patches of the image and verifying their consistency by Lint et al. (2005). Fu et al. (2006) used Hilbert-Huang transform (HHT) to generate features for classification and statistical natural image model based on moments of characteristic functions with wavelet decomposition was employed to distinguish the spliced images from the authentic images. Chen et al. (2007) investigated a scheme that extracts image features from moments of wavelet characteristic

functions and 2-D phase congruency which is a sensitive measure of sharp transitions for image splicing detection.

Natural image model was constructed by Shi et al. (2007a) to detect splicing which consists of statistical features extracted from the test image as well as 2-D arrays generated by applying to the test images multi-size block discrete cosine transform (MBDCT). Hsu and Chang (2006) proposed a method in which for a given image, first suspicious splicing areas identified, and then computing the geometry invariants from the pixels within each region and the camera response function (CRF) is estimated from these geometry invariants. The cross-fitting errors are fed into an SVM classifier. Johnson and Farid (2007c) presented a method to detect compositing of two or more people into a single image based on estimating a cameras intrinsic parameters from the image of a persons eyes. Inconsistencies in the estimated principal point was used as evidence of tampering. The discontinuity of image pixel correlation and coherency caused by splicing in terms of image run-length representation and image edge statistics were used for image splicing detection in which SVM is used as the classifier by Dong et al. (2008).

Zhang et al. (2008b) obtained a splicing detection method based on moment features extracted from the MBDCT and image quality metrics (IQMs) extracted from the given test image, which are sensitive to spliced image. Ng and Tsui (2009) and Ng T.T. (2009) described an idea of extracting the CRF signature from surfaces linear in image irradiance using linear geometric invariants from the single image. In second paper authors explored an edge-profile-based method for extracting CRF signature from a single image. The proposed method requires straight edges and edges should be wide enough so that edge profiles can be reliably extracted. QingZhong and Andrew (2009) suggested a method based on extraction of neighboring joint density features of the DCT coefficients and then SVM is applied to the features for image splicing detection. Wang et al. (2009) implemented a color image splicing detection method based on gray level co-occurrence matrix (GLCM) of thresholded edge image of image chroma. Zhenhua et al. (2009) illustrated splicing detection system consisting of an order statistic filters (OSF) based edge sharpness measure and a visual saliency guided feature extraction mechanism. Zhang et al. (2009c) constructed a method for detecting image composites based on estimated shadow geometry and photometry.

Fang et al. (2009b), evaluated consistency check of camera characteristics among different areas in an image for image splicing detection. Color sharpness and singular value difference are used for image authentication. CRF was used to detect splicing regions by (Yu-Feng and Shih-Fu, 2010). In this a test image was first automatically segmented into distinct arbitrarily shaped regions. One CRF estimated from each region using geometric invariants from locally planar irradiance points (LPIPs).

Zhang et al. (2010) introduced a method based on the planar homography constraint to locate the fake region roughly and an automatic extraction method using graph cut with online feature/parameter selection to segment the fake object. Zhao et al. (2010) proposed a method based on chroma spaces. Four gray level run-length run-number (RLRN) vectors with different directions extracted from decorrelated chroma channels were employed as distinguishing features for image splicing detection and SVM as a classifier. Liu et al. (2011b) investigated a technique based on photometric consistency of illumination in shadows by formulating color characteristics of shadows measured by the shadow matte value.

Table 1 shows comparison of various algorithms for image splicing. However all the above proposed techniques

Table 1
Comparison of image splicing or image composite detection algorithms.

Algorithm	Extracted features	Dimension of feature vector	Classifier	Detection accuracy
Ng et al. (2004)	Bicoherence features	768 segments	SVM	71%
Lint et al. (2005)	Inverse camera response function	–	SVM	100% (Using two test images)
Fu et al. (2006)	Hilbert-Huang transform (HHT) & Moments of characteristics function using wavelet decomposition based features	110	SVM	80.15%
Chen et al. (2007)	Statistical moments of wavelet characteristic function and 2D phase congruency	120	SVM	82.32%
Shi et al. (2007a,b)	Moments of characteristic functions of wavelet subbands and Markov transition probabilities of difference 2-D arrays	266	SVM	91.87%
Hsu and Chang (2006)	Camera response function using geometry invariants	6	SVM	87%
Dong et al. (2008)	Run length (RL) and edge detection (SP) based statistical moments	12 (RL) + 49 (SP) = 61	SVM	76.52%
Zhang et al. (2008a,b,c)	Moment features extracted from multi-size block discrete cosine transform (MBDCT) and some image quality metrics (IQMs)	72 (IQMs) + 168 (MBDCT) = 240	SVM	87.10%
QingZhong and Andrew (2009)	Neighboring joint density of DCT coefficients	169	SVM	89.2%
Wang et al. (2009)	Gray level co-occurrence matrix (GLCM) of chroma components	324	SVM	90.5%
Zhenhua et al. (2009)	Edge sharpness measure order statistic filter (OSF)	10/9	SVM	96.33%
Fang et al. (2009a,b)	Color sharpness, inter-channel singular value difference, and the difference between an estimate of the demosaiced and tested image	20	LDA	90%
Yu-Feng and Shih-Fu (2010)	CRF estimation using geometry invariants	20	SVM	70%
Zhao et al. (2010)	Four gray level run-length run-number (RLRN) vectors extracted from chroma channels	60	SVM	94.7%

have few limitations. Image splicing detection fails when concealing measures, such as blur is applied after splicing when the edge sharpness cues are used for detection purpose. Also it requires straight edges and edges should be wide enough so that edge profiles can be reliably extracted. Sometimes manual labeling of image regions makes a particular approach a semiautomatic one. Further, highly localized and minor tampering will most likely go unnoticed and difficult to detect. The compression artifacts make the localization of the forgery difficult when the image being analyzed is compressed by a low quality factor.

4. Image forgery detection using JPEG compression properties

JPEG is most popular and commonly used compression standard which has been found in variety of applications. Most digital cameras export JPEG file format. To identify whether an image in bitmap format has been previously JPEG compressed or not is an important issue for some image processing applications and plays very important role in image tampering detection.

Fan and Queiroz (2003) constructed a method determining whether an image has been previously JPEG compressed and to estimate compression parameters. A method for the maximum likelihood estimation was devised to estimate what quantization table was used. However, the original intention of the paper was not for tampering detection. A method for estimation of primary quantization matrix from a double compressed JPEG image presented in Fridrich and Lukas (2003). Three different approaches were presented from which the neural network classifier based one is the most effective reliable yielding less than 1% of errors. One of the limitation of proposed method is, sufficiently large images are required to obtain accurate results and is not possible to reliably estimate quantization steps for high-frequency coefficients due to insufficient statistics.

Popescu (2004) developed a technique for detecting if a JPEG image has been double compressed by examining the histograms of the DCT coefficients, as double JPEG compression amounts to double quantization of the block DCT coefficients which introduces specific artifacts visible in the histograms of these coefficients. But images that are compressed first with a high quality, then with a significantly lower quality are generally harder to detect. Neelamani et al. (2003) implemented a method to estimate image JPEG compression history components including the color transformation, subsampling, and the quantization table employed during the previous JPEG operations based on DCT coefficient structure created by previous JPEG operation as JPEG-compressed images exhibit near-periodic behavior due to quantization. A statistical model based on Benford's law for the probability distributions of the first digits of the block-DCT and quantized JPEG coefficients was obtained by Fu et al. (2007). The generalized Benford's law can be used in the detection of JPEG compression for images in bitmap format, the estimation of JPEG compression Q factor for JPEG compressed bitmap image, and the detection of double compressed JPEG image.

Tjoa et al. (2007a) explored a method to determine which transform was used during compression. The method is based on analyzing the histograms of coefficient subbands to determine the nature of the transform method. The three block transforms – DCT, Hadamard, and Slant and three wavelet transforms – 5/3, 9/7, and 17/11 were correctly determined using proposed method. Tjoa et al. (2007b) evaluated a method to estimate the block size in digital images in a blind manner without making any assumptions on the block size or the nature of any previous processing with a detection accuracy which correctly classifies an image as block-processed with a probability of 95.0% and the probability of false alarm at 7.4%. A passive approach to detect digital forgeries by checking image quality inconsistencies based on blocking artifact caused by JPEG compression was suggested by Ye et al. (2007). The blocking artifacts introduced during JPEG compression could be used as a "natural authentication code". A blocking artifact measure is proposed based on the estimated quantization table using the power spectrum of the DCT coefficient histogram.

Zhang et al. (2009a) illustrated a method to detect and locate for the tampered areas in tampered images based on double JPEG2000 compression. The technique exploits the fact that double JPEG2000 compression amounts to particular double quantization of the sub-band DWT coefficients, which introduces specific artifacts visible in the Fourier transforms of DWT coefficient histograms. Luo et al. (2008) implemented a method for block size estimation based on morphological operation. The method is based on maximum-likelihood estimation resulted in 40% accuracy improvement compared with existing gradient-based method reported in Tjoa et al. (2007b). Fridrich and Penvy (2008) introduced a reliable method for detection of double compressed JPEG images and a maximum likelihood estimator of the primary quality factor with the accuracy better than 90%. It is based on classification using support vector machines with features derived from the first order statistics of individual DCT modes of low-frequency DCT coefficients. The algorithm not only detects cover images but also images processed using steganographic algorithms.

Qu et al. (2008) formulated the shifted double JPEG compression (SD-JPEG) as a noisy convolutive mixing model for identifying if a given JPEG image has ever been compressed twice with inconsistent block segmentation. A total of 13 features which represent the asymmetric characteristic of the independent value map then feed to an SVM classifier resulting in detection accuracy of above 90% at QF of 95. Chunhua et al. (2008) created a machine learning based scheme to distinguish between double and single JPEG compressed images with detection rate of 95%. This scheme relies on the Markov process and transition probability matrix (TPM) applied to the difference JPEG 2-D arrays, which are of the second order statistics which detects the artifacts left with double JPEG compression.

Li et al. (2008a) utilized the probabilities of the first digits of quantized DCT coefficients from individual AC (alternate current) modes called as mode based first digit features (MBFDF) to reveal the double JPEG compression history of a given JPEG image. Using the approach primary

QF identified correctly in most of the cases using fisher linear discriminant (FLD) classifier. Weihai et al. (2008) tested a blind approach to detect copy-paste forgery in a JPEG image to check whether a copied area came from the same image or not. The approach utilizes the mismatch information of BAG as a clue of copy-paste forgery. The complexity of this algorithm is quite high. Junfeng et al. (2006) developed an approach by examining the double quantization effect hidden among the DCT coefficients that can detect doctored JPEG images and locate the doctored parts. The approach has several advantages like the ability to detect doctored images by different kinds of synthesizing methods (such as alpha matting and inpainting, besides simple image cut/paste), the ability to work without fully decompressing the JPEG images and the fast speed. However, the method fails when the original image to contribute the undoctored part is not a JPEG image and in case of heavy compression after image forgery.

The artifacts introduced by lossy JPEG compression was employed as an inherent signature for compressed images by Chen and Hsu (2008). The method first estimates the blockiness for each pixel, model the linear dependency of the blockiness measure, and finally analyze the different peak energy distributions to discriminate single compressed images from tampered images. However, detection of cropped-and-recompressed is feasible only when the original quality factor is smaller than the recompression quality factor. Farid (2009b) proposed a method for detecting image composites created by different JPEG compression quality on low quality images and can detect relatively small regions that have been altered. The technique detects if part of an image was initially compressed at a lower quality than the rest of the image. This technique is effective only when the tampered region is of lower quality than the image into which it was inserted.

Lin et al. (2009b) constructed a fast, fully automatic method for detecting tampered images by examining the double quantization effect hidden among the DCT coefficients using SVM classifier. The technique was insensitive to different kinds of forgery methods such as alpha matting and inpainting, in addition to simple image cut/paste. The method fails when the whole image is resized, rotated, or cropped. Detection method of double JPEG compressed image was proposed based on histograms of DCT coefficients and SVM by Mahdian and Saic (2009a). The method exploits the fact that altering a JPEG image brings into the image specific artifacts like periodic zeros and double peaks. However, the method produces high false positive to natural images with "nonperfect histograms".

Huang et al. (2010) presented a method which can detect double JPEG compression with the same quantization matrix. First a "proper" randomly perturbed ratio is obtained from the JPEG coefficients of the recompressed test image and then this universal "proper" ratio generate a dynamically changed threshold, which can be utilized to distinguish between the singly and doubly compressed images. If the QF is no less than 90, the final detection accuracy rates are constantly higher than 90% for UCID, NRCS, and OurLab image dataset. The method can also be extended to detect the triple JPEG compression, four times JPEG compression, and so on. Luo et al. (2010) evaluated a method for image tamper detection including identifying whether a bitmap image has previously been JPEG compressed, quantization steps estimation and detecting the quantization table of a JPEG image by analyzing the effects of quantization, rounding and truncation errors. The method achieves accuracy of around 90% even the image size decreases to 8×8 and the quality factor is as high as 95 while identifying JPEG images, average accuracy is 81.97% for the images with size of 128×128 and with the quality factor 85 while estimating quantization steps, and the accuracy can achieve over 94.52% when the image size becomes larger than 64×64 while detecting quantization table.

Wang et al. (2010) implemented an algorithm which can locate the tampered region in a lossless compressed tampered image when its unchanged region is output of JPEG decompressor. PCA is employed to separate different spatial frequencies quantization noises, i.e. low, medium and high frequency quantization noise and extract high frequency quantization noise for tampered region localization. However, this methods fails to detect forgery if the tampered region of a forged image has little high frequency information or the source image is saved in JPEG format with higher quality than the quality tampered image. Bianchi and Piva (2011) illustrated a reliable method to detect the presence of non-aligned double JPEG compression (NA-JPEG) based on a single feature which depends on the integer periodicity of the DCT coefficients when the DCT is computed according to the grid of the previous JPEG compression. Additionally the method accurately estimates both the quantization step and the grid shift of the primary JPEG compression.

Chen and Hsu (2011) presented a technique to detect either block-aligned or misaligned recompression by formulating the periodic characteristics of JPEG images both in spatial and transform domains. The approach is limited if a global operation such as additive white Gaussian noise or blurring are applied with a large distortion level before recompression. Kee et al. (2011) described a technique which extracts camera signature (9163 camera configurations) from a JPEG image consisting of information about quantization tables, Huffman codes, thumbnails, and EXIF format to determine if an image has been modified in any way. Bianchi et al. (2011) applied a statistical test to differentiate between original and forged regions in JPEG images by computing probability models for the DCT coefficients of singly and doubly compressed regions along with an estimation of the primary quantization factor in the case of double compression. Bianchi and Piva (2012) proposed a method to detect into a digital image the presence of non-aligned double JPEG compression based on the observation that the DCT coefficients exhibit an integer periodicity when the blockwise DCT is computed according to the grid of the primary JPEG compression.

5. Photographic images and photorealistic computer graphic (PRCG) images classification

As computer graphics (CG) technologies rapidly develop, sophisticated computer graphics rendering

software can generate remarkably photorealistic images. Photorealistic images can be created that are difficult to distinguish visually from photographic images. As the rendering technology evolves, photorealistic images can be modeled and rendered easily. One of the challenging and immediate problem is to distinguish between photorealistic computer generated (PRCG) images from real (photographic) images.

Leykin and Cutzu (2003) investigated a technique based on properties of intensity and color edges to differentiate paintings from photographs of real scenes. Ng and Chang (2004b) constructed a detector which classifies photographic images (PIM) from PRCG using natural image statistics (NIS). Three types of NIS with different statistical order, i.e. NIS derived from the power spectrum, wavelet transform and local patch of images were studied. Lyu and Farid (2005) created a statistical model for photographic images consisting of first and higher-order wavelet statistics using LDA and a non-linear SVM. However, the model don't necessarily give any insight into how one might render more photorealistic images. Cutzu et al. (2005) computed the image classification system that discriminates paintings from photographs based on the evidence that that photographs differ from paintings in their color, edge, and texture properties.

Ng et al. (2005) proposed a method for classifying photographic images and photorealistic computer graphics based on a geometry-based image model motivated by the physical image generation process. The classification was based on the SVM classifier. Further Ng and Chang (2006) deployed an online system for distinguishing photographic and computer graphic images in which users are able to submit any image from a local or an online source to the system and get classification results with confidence scores. Dehnie et al. (2006) developed a digital image forensics technique to distinguish images captured by a digital camera from computer generated images based on the properties of the residual image (pattern noise in case of digital camera images) extracted by a wavelet based denoising filter.

Rocha and Goldenstein (2006) described a new methodology to separate photographs and computer generated images using the progressive randomization (PR) technique that extracts the statistical properties of each one of photographs and computer generated image classes. Wang and Moulin (2006) implemented a method for differentiating digital photorealistic images from digital photographs using a wavelet based statistical model to extract features from the characteristic functions of wavelet coefficient histograms.

Dirik et al. (2007) proposed the use of features based on the differences in the acquisition process of images to distinguish computer generated images from real images. Traces of demosaicking and chromatic aberration are used to differentiate computer generated images from digital camera images. Shi et al. (2007b) introduced a novel approach to distinguish computer graphics from photographic images based on the statistical moments of characteristic function of the image wavelet subbands and their prediction-error features. Same authors explored the use of genetic algorithm to select an optimal feature set for distinguishing computer graphics from digital photographic images using the same feature set but with reduced dimensions (Chen et al., 2008b).

Khanna et al. (2008) presented method for distinguishing between an image captured using a digital camera, a computer generated image and an image captured using a scanner based on sensor pattern noise features extracted from digital cameras and scanners. Sankar et al. (2009) developed a technique for differentiating between computer graphics and real images based on an aggregate of existing features. In addition to this, filters were proposed to effectively detect attacks like creation of hybrid images and histogram manipulations. Sutthiwan et al. (2009a), employed statistical moments of 1-D and 2-D characteristic functions to derive image features which captures the statistical differences that can distinguish between computer graphics and photographic images.

Sutthiwan et al. (2009b) evaluated a method to differentiate between computer graphics and photographic images by applying Markov process (MP) to model difference JPEG 2-D arrays along horizontal and vertical directions to derive TPM which characterize the MP. Li et al. (2010) proposed a method for the discrimination between natural images and photorealistic computer graphics using second-order difference statistics and the Fisher linear discrimination analysis to construct a classifier. Wu et al. (2011) developed a method for discriminating computer generated graphics from photographic images based on several highest histogram bins of the difference images as features for the classification.

Table 2 describes comparison of various photographic images and computer graphics images algorithm. The techniques discussed above works well for uncompressed images or JPEG images with a high quality factor. Performance of various methods decreases with higher degrees of JPEG compression and down-sampling operation. Also from a rendering point of view, few methods don't necessarily give any insight into how one might render more photorealistic images.

6. Lighting inconsistency

Different photographs are captured under different lighting conditions. When combining image fragments from different images, it is difficult to match the lighting conditions from the individual photographs. Therefore, lighting inconsistency detection for different parts in an image can be employed to identify tampering.

Johnson and Farid (2005) described a technique for estimating the direction within one degree of freedom of an illuminating light source from only a single image to detect forgery. First the direction of the illuminated source is estimated for different objects/people in an image, inconsistencies in lighting can be used as evidence of digital tampering. Same authors illustrated a model based on inconsistencies in the lighting due to multiple light sources, diffuse lighting, directional lighting from a single image which is then used as evidence of tampering. It is illustrated by Johnson and Farid (2007a) that any arbitrary lighting environments can be modeled with a 9-dimensional model. Johnson and Farid (2007b)

Table 2
Comparison of various photographic image and photo-realistic computer generated (PRCG) image classification algorithms.

Algorithm	Extracted features	Dimension of feature vector	Classifier	Classification accuracy
Ng and Chang (2004b)	Natural image statistics (NIS) derived from the power spectrum, wavelet transform and local patch of images	129 (NIS) & 102 (CG)	SVM	83%
Lyu and Farid (2005)	First- and higher-order wavelet statistics	216	LDA & non-linear SVM	67%
Ng et al. (2005)	Geometry-based features by means of the fractal geometry at the finest scale and the differential geometry at the intermediate scale	192	SVM	83.5%
Rocha and Goldenstein (2006)	Statistical descriptors of the least significant bit (LSB) occurrences using Progressive Randomization (PR) technique	96	SVM	90%
Wang and Moulin (2006)	The characteristic functions of wavelet-coefficient histograms (High pass filtering and band pass filtering)	144	FLD	100%
Dirik et al. (2007)	Color filter array demosaicking and chromatic aberration based features	72	SVM	90%
Shi et al. (2007a,b)	Moments of wavelet subbands & prediction error image	234	SVM	82.1%
Khanna et al. (2008)	Residual pattern noise (sensor pattern noise)	15	SVM	85.9%
Chen et al. (2008a,b)	Moments of wavelet subbands & prediction error image	100	SVM	82.3%
Sankar et al. (2009)	Moment-based method, texture interpolation method, color histogram and patch statistics based features	80	Two-class classifier	90%
Sutthiwan et al. (2009a)	Image pixel 2D array and image JPEG 2-D array, 2D histogram features	780 (450 using BFS)	SVM	87.6% (92.7% using BFS)
Sutthiwan et al. (2009b)	Second order statistics transition probability matrices (TPM) derived from Applying (Markov process) MP to model difference JPEG 2-D arrays	324 (150 using BFS)	SVM	94.0% (94.2% using BFS)
Li et al. (2010)	Features based on the variance and kurtosis of second-order difference signals and the first four order statistics of predicting error signals	144	FLDA	95.5%
Wu et al. (2011)	Histogram bins of first-order and second-order difference images	112	FLD	95%

constructed a technique to measure the 3-D direction to a light source from the position of the highlight on the eye. Specular highlights that appear on the eye are a powerful cue as to the shape, color and location of the light source(s). Inconsistencies in shape, color and location of the light source properties of the light can be used as evidence of forgery.

Zhang et al. (2009c) investigated a method to detect image composites by enforcing the geometric and photometric constraints from shadows. In particular, authors explored (i) the imaged shadow relations that are modeled by the planar homology and (ii) the color characteristics of the shadows measured by the shadow matte. Farid and Bravo (2010) described three computational methods that can be applied to detect the inconsistencies in shadows, reflections, and planar perspective distortions that seem to elude the human visual system. Yingda et al. (2011) proposed an improved blind image identification algorithm based on inconsistency in light source direction which is defined as "neighborhood method" as inconsistency in the light source direction can be considered as strong evidence of the image tampering. The neighborhood method was used to calculate surface normal matrix of image in the blind identification algorithm with detection rate of 87.33%. Farid (2010) studied a 3-D photo forensic analysis of the historic and controversial Zapruder film on JFK. The analysis shows that the shadow is consistent with the 3-D geometry of the scene and position of the sun proving that the 8 mm original film has not been altered.

Major advantage of these methods is that it is difficult to hide the traces of inconsistencies in lighting conditions which is present due to digital tampering.

7. Projective geometry

Photographs with composited regions, it is often difficult to keep the appearance of the image correct perspective. Hence, traces of tampering can be detected by applying the principles from projective geometry.

Johnson and Farid (2006b) proposed three techniques for estimating the transformation H of a plane imaged under perspective projection. With this transformation, a planar surface can be rectified to be fronto-parallel where each technique requires only a single image and exploits different geometric principles. Conotter et al. (2010) presented a technique for detecting text manipulation on sign or billboard using the evidence that text in an image follows the expected perspective projection, deviations from which are used as evidence of tampering. It is difficult to identify forgery if the inserted text is applied with correct homography.

An important advantage of this approach is that it is difficult to conceal the traces of tampering. However, few techniques are semiautomatic.

8. Chromatic aberration

The imperfections in optical imaging systems results in different types of aberrations into the captured images. Chromatic aberration is caused from imperfection in the lens to perfectly focus light different wavelengths in a digital camera which provokes a discrepancy in the location in which the sensor receives light of different wavelengths. There are two types of chromatic aberration: longitudinal and lateral. Longitudinal aberration causes

different wavelengths to focus at different distances from the lens while lateral aberration is attributed to different wavelengths focusing at different positions on the sensor. Tampering of image causes the aberration across the image inconsistent. This reveals the presence of forgery.

Johnson and Farid (2006a) implemented a model for lateral chromatic aberration and automatic technique for estimating these model parameters that is based on maximizing the mutual information between color channel was derived. This approach for detecting tampering is effective when the manipulated region is relatively small. Lanh et al. (2007b) estimated the parameters of lateral chromatic aberration by maximizing the mutual information between the corrected R and B channels with the G channel. The parameters extracted are then used as input features to an SVM classifier for identifying source cell phone of images resulted in average accuracy rate of 92.22%. Gloe et al. (2010) obtained a new approach to estimate lateral chromatic aberration with low computational complexity and, for the first time, provide results on using lateral chromatic aberration in real-world scenarios based on the 'Dresden' image database. Memon et al. (2011) employed a technique which is able to obtain a stable enough CA pattern distinguishing different copies of the same lens.

Most of the methods discussed above suffer heavily from image modification attack and it is observed that the detection performs poorly on low quality images.

9. Color filter array (CFA) and inter pixel correlation

Many digital cameras are equipped with a single charge-coupled device (CCD) or complementary metal oxide semiconductor (CMOS) sensor which capture color images using CFA. The CFA consists of an array of color sensors, each of which captures the corresponding color scene at an appropriate pixel location where it is located and remaining colors are obtained by interpolating process. Image forgery can be detected by identifying correlation introduced by the interpolation process.

Popescu and Farid (2005a) introduced a method to detect and locate image tampering based on an expectation/maximization (EM) algorithm and uses a linear model in lossless and lossy compressed images. The detection accuracies for eight different CFA interpolation algorithms are close to 100% for quality factors greater than 96, and that they decrease with decreasing quality factors. Swaminathan et al. (2006a) investigated a technique for identifying the CFA pattern and the interpolation algorithm. The interpolation coefficients corresponding to the three color planes were estimated and an SVM was used for identifying the interpolation method. 100% classification accuracy in identifying the correct CFA interpolation algorithm with no false alarms was obtained. Cao and Kot (2009) presented a detection framework of image demosaicing regularity using partial derivative correlation models which detects both the cross and the intra-channel correlation caused by demosaicing. The test identification accuracies of 97.5% for 14 commercial DSCs of different models and 99.1% for 10 RAW-tools was obtained using the probabilistic SVM classifier.

Huang and Long (2008) proposed a decision mechanism using 3-layer feedforward back propagation neural networks (BPN) and a majority-voting scheme is designed for demosaicking correlation recognition and digital photo authentication based on a quadratic pixel correlation model, in which such correlation is expressed in a quadratic form. Gallagher and Chen (2008) developed a technique which detects the presence of demosaicing in a digital image to detect and localizing tampering. Also an approach is described to distinguish between PIM and PRCG images. Swaminathan et al. (2009) focused on the problem of component forensics and examined how the intrinsic fingerprint traces left behind in the final digital image by the different components of the imaging device can be used as evidence to estimate the component parameters.

Dirik and Memon (2009) constructed a tamper detection techniques based on artifacts created by CFA by computing features like CFA pattern number estimation and CFA based noise analysis and finally classification is done by using a simple threshold based classifier. The technique is sensitive to strong JPEG re-compression and resizing and may also not work well if the tampered region area is too small. Fan et al. (2009) proposed a framework which is effective in recognizing the demosaicking algorithms for raw CFA images based on a generalized neural network framework to simulate the stylized computational rules in demosaicking through bias and weight value adjustment. Kirchner (2010) formulated an efficient method to determine the configuration of the CFA pattern in demosaiced digital images using only one linear filtering operation per image which is used to assess the authenticity of digital images. However, JPEG compression severely reduces correct recognition rate of the CFA pattern configuration.

Takamatsu et al. (2010) described a method for estimating demosaicing algorithms from image noise variance based on the observation that the noise variance in interpolated pixels becomes smaller than that of directly observed pixels without interpolation. Estimation of the CFA pattern accuracy is 95.8% for multiple image and 98.4% for single image when JPEG quality is set to 100. One limitation of the proposed method is that the accuracy decreases when the image is processed (e.g., image compression and other image filtering) after demosaicing.

Major limitation of the methods discussed above is that strong post-processing and JPEG compression hamper a reliable accurate detection of tampering.

10. Image processing operations

When altering an image, to conceal traces of tampering often various image processing operations are applied to the images. Detection of these operations results in identification of forgeries.

Lukas (2000) implemented a technique to detect manipulation in digital images using the convolutional filtering and spectral filtering operations. Avcibas et al. (2004) illustrated a method that discriminates between tampered image and its originals based on content-independent distortion measurements called as image quality measures used as features in the design of a linear regression classifiers. Bayram et al. (2005a) method based

on the neighbor bit planes of the image based on the basic idea that, the correlation between the bit planes as well the binary texture characteristics within the bit planes will differ between an original and a doctored image. These binary similarity measures are used as features in classifier design.

Bayram et al. (2006) explored a technique to detect doctored and manipulated images using three features, the binary similarity measures between the bit planes, the image quality metrics applied to denoised image residuals, and the statistical features obtained from the wavelet decomposition of an image. Stamm and Liu (2008, 2010) presented a method to detect globally and locally applied contrast enhancement and the use of histogram equalization by searching for the identifying features of each operations intrinsic fingerprint. Swaminathan et al. (2006b) exploited blind deconvolution to detect image tampering. The linear part of the tampering process is modeled as a filter and obtained its coefficients using blind deconvolution. Possible manipulations such as filtering, compression, rotation etc. are indentified using these estimated coefficients.

Luo et al. (2007b) described a method based on the property of the blocking artifact characteristics matrix (BACM) for effectively detecting cropping and recompression operations in JPEG images. BACM exhibits a symmetrical shape for the original JPEG images and this symmetrical property will be altered by cropping and recompression operations. Kirchner and Bohme (2008) developed different form of image transformation operations which are undetectable by resampling detectors based on periodic variations in the residual signal of local linear predictors in the spatial domain. The detectability and the resulting image quality is benchmarked against conventional linear and bicubic interpolation and interpolation with a sinc kernel. Kirchner and Fridrich (2010) proposed a method which investigates the detection of median filtering in digital image using streaking artifacts (for uncompressed images) and subtractive pixel adjacency matrix (SPAM for Compressed images) features and SVM classifier.

Cao et al. (2010b) presented an algorithm to detect the median filtering manipulation. Statistical characteristics of the median-filtered signal is analyzed and measured by the probability of zero value on the difference map of textured pixels. Mahalakshmi et al. (2012) obtained a technique for image authentication that detects the basic image operations such as re-sampling (rotation, rescaling), contrast enhancement and histogram equalization in the digital images. The interpolation related spectral signature method is used for detecting rotation and rescaling and for estimating parameters such as rotation angle and rescale factors. Gul et al. (2010) employed SVD based features to model the correlation among the rows and columns using relative linear dependency to detect image manipulations such as rotation, scaling, brightness adjustment, etc. Table 3 shows comparison of various image processing operation detection algorithms.

11. Local noise

Authentic image contains an amount of noise that is uniformly distributed across an entire image. It is common to add localized random noise to the forged image regions in order to conceal traces of tampering while creating forgeries. Detection of inconsistent local noise levels across the image resulted due to tampering can be utilized to perform forgery detection analysis.

Gou et al. (2007) introduced a novel approach for image tampering detection and steganalysis, using three sets of statistical noise features (60 features) based on denoising operations, wavelet analysis, and neighborhood prediction. SVM is used for classifying the authentic images and the tampered images resulting detection probability 90% and above.

Mahdian and Saic (2008b) investigated a method to detect image forgeries which divides the investigated image into various segments of different noise levels and the local noise is estimated based on tiling the high pass diagonal wavelet coefficients. The proposed method is not able to find the corrupted regions, when the noise degradation is very small. Also the detection performance radically decreases to images corrupted by noise. Lee and Choi (2010) described a color laser printer identification method by estimating the invisible noises with the wiener-filter and then a GLCM is calculated to analyze the texture of the noise. These 60 GLCM statistical features are used as input to a support vector machine classifier for identifying the color laser printers. Nataraj et al. (2010) proposed a re-sampling detectors which reliably detect re-sampling in JPEG images at lower QFs (75–90) by adding a controlled amount of noise to the image before the re-sampling detection step.

Typically, in all the methods it is difficult to find the corrupted regions, when the noise degradation is very small.

12. Interpolation and geometric transformations

When creating image composites, to give the image a more uniform aspect geometric transformations are needed. These geometric transformations typically involve re-sampling (e.g., scaling or rotating) which in turn calls for interpolation (e.g., nearest neighbor, bilinear, bicubic). Detecting the specific statistical changes due to interpolation step can be identified as possible image forgery.

Popescu and Farid (2005b) applied a technique to detect specific correlations into the image introduced by re-sampling operation using EM algorithm to estimate probability maps. The presence of these correlations can be used as evidence of digital tampering. This method performs well only on uncompressed TIFF, JPEG and GIF images with minimal compression. Gallagher (2005) presented an algorithm to detect the presence of interpolation in images by exploiting the property that the second derivative signal of the interpolated images contains a periodicity. The performance of the algorithm degrades for high order interpolation filters such as a windowed sinc interpolation filter and the interpolation detection algorithm fails in case of interpolation by a factor of 2.0.

Prasad and Ramakrishnan (2006) developed four techniques to detect the traces of re-sampling, two of the techniques are in pixel domain and two others in frequency domain. Spatial domain techniques are based on properties

Table 3
Various image processing operation detection algorithms.

Algorithm	Problem domain	Extracted features	Classifier	Detection accuracy
Avcibas et al. (2004)	Scaling, rotation, brightness adjustment and contrast enhancement detection	Two first-order moments of the angular correlation and two first-order moments of the Czenakowski measure	Linear regression classifier	Brightness adjustment = 69.2%, Contrast adjustment = 74.2%, Mixed processing = 80.0% (Results for tampered images with manipulations)
Bayram et al. (2005a,b)	Scaling-up, rotation, brightness adjustment, blurring and sharpening	Binary similarity measures	Linear regression classifier	Image scaling-up (@50%) = 99%, Rotation (@500) = 99%, Brightness adjustment (@40) = 78%, Gaussian blur (0.5) = 99%, Sharpening = 93.5%
Bayram et al. (2006)	Scaling-up/down, rotation, brightness adjustment, blurring and sharpening	Image quality Measures (IQM), Higher order wavelet statistics (HOWS), Binary similarity measures (BSM)	Clairvoyant classifier, Semiblind classifier, Blind classifier	Scaling up (10%) = 100%, Scaling down (10%) = 99%, Rotation (@150) = 100%, Blurring (0.3) = 72%, Brightness adjustment (15) = 76%, sharpening = 98%
Stamm and Liu (2010)	Contrast enhancement, histogram equalization, additive noise	Image pixel value histogram	Threshold classifier	Globally applied contrast enhancement = 99%, Locally applied contrast enhancement = 98.5%, Histogram equalization = 99%, Additive noise detection in images = 99%
Luo et al. (2007a,b)	Cropping and recompression operations in JPEG images	Blocking artifact characteristics matrix (BACM)	SVM	63.9% (@ QF1 is 80–89 & QF2 is 65), 99.2% (@ QF1 is 60–69 & QF2 is 85)
Kirchner and Fridrich (2010)	Detect median filtering operation used for denoising and smoothing	Streaking artifacts (Uncompressed), Subtractive pixel adjacency matrix (SPAM) (Compressed)	Soft-margin SVM	For uncompressed images, false positive rate of <1.8%
Cao et al. (2010a,b)	Detection of median filtering	The probability of zero values on the first order difference map in texture regions is used as MF statistical fingerprint	Thresholding classification	MF detection with true positive rate >0.85, Distinguish MF from other manipulations with true positive rate >0.95
Mahalakshmi et al. (2012)	Rotation, rescaling, contrast enhancement and histogram equalization	DA (DFT + Averaging) and AD (Averaging + DFT) methods		Rotation = 98.3% (Global) & 96.3% (Local), Rescaling = 99% (Global) & 97.6% (Local), Contrast enhancement = 100% (Global) & 98.3% (Local), Histogram equalization = 100% (Global) & 99.3% (Local)
Gul et al. (2010)	Scaling-up/down, rotation, brightness adjustment, contrast, rotation and blurring	SVD based features	Clairvoyant classifier, Semiblind classifier, Blind classifier	Scaling up = 100%, Scaling down = 100%, Rotation = 100%, Blurring = 90.5%, Brightness = 79%, Contrast = 81%

of the second difference and properties of the zero-crossings of the second difference. Frequency domain techniques include DCT high pass filtering and bi-orthogonal wavelets. Kirchner (2008) implemented a re-sampling detection method based on cumulative periodograms. Variance of prediction residuals of a resampled signal can be used to describe periodic artifacts in the corresponding p-map. Mahdian and Saic (2008c) proposed a blind, efficient and automatic method capable of finding traces of resampling and interpolation using specific periodic properties present in the covariance structure of interpolated signals and their derivatives using Radon transform with the detection accuracy near 100%.

Gloe and Kirchner (2009) investigated re-sampling detection in re-compressed JPEG images and shown that the blocking artifacts of the previous compression step can help to increase detection performance in JPEG compressed images. However, a detection of downscaling requires a lower JPEG quality in the first compression step. Mahdian and Saic (2009b) proposed a cyclostationarity detection method to detect the traces of geometrical transformations in an image and the specific parameters of the transformation are estimated. The method is based on the fact that a cyclostationary signal has a frequency spectrum correlated with a shifted version of itself. The detection is nearly perfect for scaling rates greater than 0.90.

Sarkar et al. (2009) developed a machine learning based framework to distinguish between seam-carved (or seam-inserted) and normal images using 324-dimensional Markov feature and consisting of 2D difference histograms in the block-based DCT domain with a detection accuracy of 94%. Fillion and Sharma (2010) constructed a method of detecting content-adaptive scaling of images using seam-carving using four sets of features and SVM which provides a classification accuracy of 91%. Wei et al. (2010) illustrated an image rotation angle estimator based on the relations between the rotation angle and the frequencies at which peaks due to interpolation occur in the spectrum of

the image edge map. Further, rescaling/rotation detection and parameter estimation to detect fake objects inserted into images also estimated.

Dalgaard et al. (2010) proposed a method to detect resampling traces for image authentication using differentiation prefilters. As derivative of the interpolated signal is used for covariance computation, it results in improvement of resampling manipulations detection significantly. Vazquez-Padin and Perez-Gonzalez (2011) investigated the design of prefilters to improve the estimation accuracy of the resampling factor of spatially transformed images. A framework which allows the definition of a cost function that measures the degree of detectability of the spectral peaks is proposed based on cyclostationarity theory with an estimation accuracy close to 90%.

The methods discussed above are performs well when the image being analyzed is in uncompressed format. The detection accuracy lowers in JPEG images compressed using lower QF as the artifacts of JPEG compression conceal the traces of interpolation.

13. Blur and sharpening

Blurring is a common process in digital image manipulation which is used to reduce the degree of discontinuity or to remove unwanted defects. Furthermore, blur operation is one of the commonly used methods to hide the presence of forgery. So identifying blur inconsistencies in various image regions can be helpful in detection image forgeries.

Hsiao and Pei (2005) implemented a tampering detection scheme based on blur region detection using image DCT coefficients and optional morphological operations. Sutcu et al. (2007) applied a method to detect image tampering operations that involve sharpness/blurriness adjustment based on the regularity properties of wavelet transform coefficients which involves measuring the decay of wavelet transform coefficients across scales. Zhang and Zhang (2007) described an image forgery detection method based on detecting the presence of feather operation, which is particularly useful to create a smooth transition between the selected region and its surroundings. The forged region can be determined by the value of weighted local entropy at a 17% false positive rate. A blur edge detection scheme is employed in Zhou et al. (2007) based on the edge processing and analysis using edge preserving smoothing filtering and mathematical morphology with average accuracy of 90%.

A passive blind digital image forgery detection method was introduced by Wang et al. (2008) based on consistency of defocus blur which uses local blur estimation at each edge pixels to exposes the defocus blur inconsistency. Elder-Zucker method is used to estimate the blurriness of chosen image patches and judge if their blurriness is consistent using threshold. Suwendi and Allebach (2008) proposed a nearest-neighbor and bilinear interpolation detection algorithms are designed to estimate rational resampling factors (above 1) in both the vertical and horizontal dimensions. A blind image forgery detection algorithm is designed by Cao et al. (2009) to detect sharpening operation in digital images based on histogram gradient aberration and ringing artifacts metric. Overall accuracy is found to be 93% using combination of both the features.

Cao et al. (2010a) proposed a blur operation detection approach which is based on assessing consistency of the estimated blur radius along an edge segment. Kakar et al. (2011) presented a method of detecting splicing in images, using discrepancies in motion blur. The approach is based on the gradients of the matting components of the image to estimate the motion blur present in the image. Further, a blur estimate measure (BEM) is developed to provide robust segmentation in the case of little perceptible blur. Cao et al. (2011) proposed a detection method of unsharp masking (USM) sharpening manipulation, which is commonly applied as a retouching tool. Overshoot artifacts measured by a sharpening detector can be used as a unique feature for identifying the history of sharpening operation.

Major drawback is most of the proposed techniques requires a human interpretation of the output.

14. Acquisition device analysis and identification

Digital image may come from various imaging devices, e.g., various cameras, scanners, computer graphics technology. In order to determine integrity and authenticity of a given image, identifying the device used for its acquisition is of major interest. Different image forgery detection techniques detect the traces left by the different processing steps in the image acquisition and storage phases. These traces mark the image with some kind of inherent “fingerprints” of the imaging devices, which can be used to identify the source of the image.

Kharrazi et al. (2004) developed a method of identifying the source camera of a digital image using the color processing/transformation and a set of IQM. Bayram et al. (2005b) applied a technique to identify the source camera of an image based on traces of the color interpolation in the RGB color channels. Measures are generated by using EM algorithm and SVM is used to classify the image origin. Farid, (2006b) proposed use of the quantization tables that controls the amount of compression achieved to distinguish between original and modified photos. Different cameras employ different quantization tables. A comparison of an image quantization scheme to a database of known cameras can be a simple technique for confirming or denying an image source. The traces of demosaicing are used to identify the camera by Bayram et al. (2008b) and Cao and Kot (2010).

Imaging sensors used in capturing devices tends to introduce various defects and to create noise in the pixel values. The sensor noise is the result of three main components, i.e. pixel defects, fixed pattern noise (FPN), and photo response non uniformity (PRNU). FPN and PNRU are the two components of the so-called pattern noise as illustrated in Fig. 5 and depend on dark currents in the sensor and pixel non-uniformities respectively. Chen et al. (2008b) investigated a technique to identify the source digital camera from its images and for revealing digitally altered images using PRNU using the maximum-likelihood principle. The method is robust against common image processing, such as JPEG compression, gamma correction, resizing, and denoising. Khanna et al. (2009) presented a

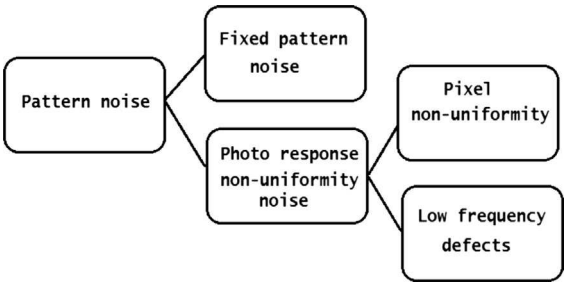

Fig. 5. Pattern noise in CCD.

method to identify the source camera of an unknown image, in which the imaging sensor pattern noise extracted from the image is correlated with all the reference camera patterns obtained from training images which is called as unique fingerprint of that camera. This correlation based approach is classification accuracy close to 100% when it is tested on 10 digital cameras. Li (2009) effectively used sensor pattern noises (SPN) extracted from digital images as device fingerprints for digital device identification with an identification rate greater than 99%. But one of the limitation is misclassification rate is high in case of small image size. In the approach an enhanced fingerprint can be obtained by assigning weighting factors inversely proportional to the magnitude of the signal components.

Li and Li (2010) proposed method of extracting PRNU called colour-decoupled PRNU (CD-PRNU), by exploiting the difference between the physical and artificial colour components of the photos taken by digital cameras that use a colour filter array for interpolating artificial colour components from the physical ones for digital camera identification. Typical identification rate for 768 $\times$ 1024 image size is 94.33% and 192 $\times$ 256 image size is 60.67%. Liu et al. (2010a) employed the binary hypothesis testing scheme to detect the presence of PRNU in the image and proposed a method to extract from the noise residual the significant regions with higher signal quality and discard those regions heavily deteriorated by irrelevant noises for identification of a specific digital camera.

Kang et al. (2012) proposed a source camera identification method that can remove the interference and raise the correlation to circular correlation norm (CCN) value and further a use of CCN as the test statistic, which can lower the false positive rate to be a half of that with statistic peak to correlation energy (PCE). True positive rate (TPR) of the proposed method is 99.9% on an image with size of 512 $\times$ 512 pixels at zero false positives (FP). Celiktutan et al. (2008) proposed a method to identify the originating camera based on three sets of features, binary similarity measures, image quality measures and higher order wavelet statistics in conjunction with SVM classifier. The method resulted in accuracy of 97.5% using decision fusion method when 16 camera models are used. Dirik et al. (2008) proposed a source camera identification method based on detection and matching of the sensor dust characteristics with average 99% identification accuracy. Sensor dust problem is due to interchangeable lenses that the digital single lens reflex cameras deploy.

Techniques to detect digital forgeries based on PRNU which can be used as fingerprint (which is a stochastic, spread-spectrum signal and thus robust to distortion) of imaging sensors are proposed by Fridrich (2009). Author evaluated how fingerprint can be estimated from images taken by the camera and later detected in a given image to establish image origin and integrity. Xu et al. (2009) proposed a model for detecting the brands and models of digital cameras from given digital images based on the transition probability matrices derived from four different directional Markov processes applied to the image difference JPEG 2-D arrays. The average classification accuracy for camera models is higher than 97% and the average brand classification rate is 96.3%. Bateman et al. (2009) proposed a method for identifying anomalies in digital cameras by analysing image variations using statistical process control (SPC). Authors presented use of SPC as an image authentication technique to highlight inconsistencies in the image data, which can help to make such an identification.

Liu et al. (2010b) investigated source camera classification based on a graph based approach that requires no extra auxiliary images nor a prior knowledge about the constitution of the image set. Performance with average classification accuracies over 95% is achieved while classifying 6 camera models. Alles et al. (2009) proposed a method to identify the source camera of heavily JPEG compressed digital photographs of resolution 640 $\times$ 480 pixels using PRNU. Classification accuracy of 83% for single images and 100% for around 20 simultaneously identified questioned images for 38 cameras of four different model is achieved. Micro and macro statistical features based on SVD is proposed for source cell-phone identification by Gul and Avcibas (2009) with the classification accuracy achieved by using 18 features is 92.4% for 9 different camera.

Fang et al. (2009b) developed a classifier to distinguish between digital images taken from digital single lens reflex (DSLR) and compact cameras based on wavelet coefficients and pixel noise statistics. Average classification accuracy of above 93% is achieved for 20 different cameras models. Goljan and Fridrich (2012) evaluated a method based on sensor fingerprint (PRNU) camera identification to images corrected for lens distortion. A detection reliability of 91% for a Panasonic camera and 99.8% for Canon with camera fingerprints estimated from 10 images is obtained.

15. Conclusion

Passive or blind techniques and methodologies for validating the integrity and authenticity of digital images is one of the rapidly growing areas of research. Passive methods require no extra prior knowledge of the image content or any embedded watermarks or signature. We have presented overview of digital image tampering detection and the existing references on blind methods for image forgery detection. Different image forgery detection techniques are classified and then generalized structure of image forgery detection is presented in this paper. We then compared the performance of some typical image forgery detection algorithms. Most of the techniques are developed to detect image tampering and some of also are able to

localize the forged areas. We hope it will contribute to find new promising methods and ideas to researchers working in the field of digital image forgery detection.

First drawback of existing methods is the problem of automation i.e. outputs need a human interpretation. Second, to localize the forgery, existing methods mostly need to have a larger modified region containing inconsistencies. Also, camera source identification is still limited to 9–15 cameras and in mobile camera model identification; the result can be adversely affected by increasing the number of cameras. It is observed that the identification methods based on intrinsic features of camera hardware like the lens and CCD sensor characteristics produce reliable and better results than those based on camera software parts (e.g., CFA interpolation algorithms). The compression artifacts make the localization of the forgery difficult when the image being analyzed is compressed by a low quality factor in most of the techniques.

In case of copy-move forgery detection, these methods are computationally expensive and they introduce high false positives. Image forgery localization methods based on JPEG works fine when the image content is consistent and the modified region previously had a lower JPEG quality factor than the current JPEG quality factor. In CFA and inter pixel relation based methods, tampering detection accuracy affects strong post-processing and JPEG compression. In case of image-splicing, detection accuracy lowers post-processing operations such as edge blurring, adding noise, and lossy compression.

Current research in passive-blind forgery detection is mainly limited to the image tampering detection techniques and can be extended to audio and video. Understanding the perception of visual semantics could be important also to identify the maliciousness of a forgery. The work suggested by Lee et al. (2006) finds perceptually meaningful regions using an image segmentation technique and by using a common-sense reasoning techniques. The validation of performance measures, such as accuracy, robustness, security is a major concern. This is because of the lack of established benchmarks and of public testing databases which evaluates the actual accuracy of digital image forgery methods. One of the major limitation of current image forgery detection methods is that there is no way to the distinction between malicious tampering and "innocent" retouching, such as red-eye correction or artistic manipulation. Also one of the challenging tasks is to find more robust statistical features to resist the various post-processing operations.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable and insightful comments on the earlier version of this manuscript.

References

Alles EJ, Geradts ZJ, Veenman CR. Source camera identification for heavily JPEG compressed low resolution still images. J Forensic Sci 2009; 54(3):628–38.

Amsberry C. Alterations of photos raise host of legal, ethical issues. Wall Street J Jan 1989.

Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In: Proc. International conference on image processing (ICIP) 2004. p. 2645–8.

Bashar M, Noda K, Ohnishi N, Mori K. Exploring duplicated regions in natural images. IEEE Trans Image Process 2010;99:1–40.

Bateman P, Ho AT, Woodward A. Image forensics of digital cameras by analysing image variations using statistical process control. In: Proc. International conference on information, communications and signal processing 2009. p. 1–5.

Bayram S, Avcibas I, Sankur B, Memon N. Image manipulation detection with binary similarity measures. In: Proc. of 13th European signal processing conference, vol. 1. 2005a. p. 752–5.

Bayram S, Avcibas I, Sankur B, Memon N. Image manipulation detection. J Electron Imaging 2006;15(4). 041102-1–041102-17.

Bayram S, Sencar HT, Memon NA. Survey of copy-move forgery detection techniques. In: Proc. of IEEE Western New York image processing workshop 2008.

Bayram S, Sencar HT, Memon ND. Classification of digital camera-models based on demosaicing artifacts. Digital Invest 2008b;5(1–2):49–59.

Bayram S, Sencar HT, Memon ND, Avcibas I. Source camera identification based on CFA interpolation. In: Proc. International conference on image processing (ICIP) 2005b. p. 69–72.

Bayram S, Taha H, Memon N. An efficient and robust method for detecting copy-move forgery. In: Proc. of the 2009 IEEE International conference on acoustics, speech and signal processing 2009. p. 1053–6.

Bianchi T, Piva A. Detection of non-aligned double JPEG compression with estimation of primary compression parameters. In: Proc. International conference on image processing 2011. p. 1929–32.

Bianchi T, Piva P. Detection of non-aligned double JPEG compression based on integer periodicity maps. IEEE Trans Inf Forensics Security 2012;7(2):842–8.

Bianchi T, Rosa A, Piva P. Improved DCT coefficient analysis for forgery localization in JPEG images. In: Proc. International conference on acoustics, speech and signal processing 2011. p. 2444–7.

Cao H, Kot AC. Accurate detection of demosaicing regularity for digital image forensics. IEEE Trans Inf Forensics Security 2009;4(4):899–910.

Cao H, Kot AC. Mobile camera identification using demosaicing features. In: Proc. International symposium on circuits and systems 2010. p. 1683–6.

Cao G, Zhao Y, Ni R. Detection of image sharpening based on histogram aberration and ringing artifacts. In: Proc. IEEE International conference on multimedia and Expo 2009. p. 1026–9.

Cao G, Zhao Y, Ni R. Edge-based blur metric for tamper detection. J Inf Hiding Multimed Signal Process 2010a;1(1):20–7.

Cao G, Zhao Y, Ni R, Kot AC. Unsharp masking sharpening detection via overshoot artifacts analysis. IEEE Signal Process Lett 2011;18(10): 603–6.

Cao G, Zhao Y, Ni R, Yu L, Tian H. Forensic detection of median filtering in digital images. In: Proc. IEEE International conference on multimedia and Expo 2010b. p. 89–94.

Celiktutan O, Avcibas I, Sankur B. Blind identification of source cell-phone model. IEEE Trans Inf Forensics Security 2008;3(3):553–66.

Chen M, Fridrich J, Goljan M, Lukas J. Determining image origin and integrity using sensor noise. IEEE Trans Inf Forensics Security 2008a; 3(1):74–90.

Chen Y, Hsu C. Image tampering detection by blocking periodicity analysis in JPEG compressed images. In: Proc. IEEE workshop on multimedia signal processing 2008. p. 803–8.

Chen Y, Hsu C. Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. IEEE Trans Inf Forensics Security 2011;6(2):396–406.

Chen W, Shi Y, Su W. Image splicing detection using 2-d phase congruency and statistical moments of characteristic function. In: Proc. of SPIE electronic imaging: security, steganography, and watermarking of multimedia contents 2007.

Chen W, Shi YQ, Xuan GR, Su W. Computer graphics identification using genetic algorithm. In: Proc. IEEE International conference on pattern recognition 2008b. p. 1–4.

Chunhua C, Shi YQ, Wei S. A machine learning based scheme for double JPEG compression detection. In: Proc. International conference on pattern recognition 2008. p. 1–4.

Conotter V, Boato G, Farid H. Detecting photo manipulation on signs and billboards. In: Proc. International conference on image processing 2010. p. 1741–4.

Cutzu F, Leykin A, Riad H. Distinguishing paintings from photographs. Comput Vis Image Und 2005;100(3):249–73.

Dalgaard N, Mosquera C, Perez-Gonzalez F. On the role of differentiation for resampling detection. In: Proc. International conference on image processing 2010. p. 1753–6.
Dehnie S, Sencar HT, Memon ND. Digital image forensics for identifying computer generated and digital camera images. In: Proc. International conference on image processing (ICIP) 2006. p. 2313–6.
Dirik AE, Bayram S, Sencar HT, Memon N. New features to identify computer generated images. In: Proc. IEEE International conference on image processing, vol. 4. 2007. p. 433–6.
Dirik AE, Memon N. Image tamper detection based on demosaicing artifact. In: Proc. International conference on image processing (ICIP) 2009. p. 429–32.
Dirik AE, Sencar HT, Memon N. Digital single lens reflex camera identification from traces of sensor dust. IEEE Trans Inf Forensics Security 2008;3(3):539–52.
Dong J, Wang W, Tan T, Shi Y. Run-length and edge statistics based approach for image splicing detection. In: Proc. digital water marking. 7th International workshop (IWDW) 2008. p. 76–87.
Dybala B, Jennings B, Letscher D. Detecting filtered cloning in digital images. In: Proc. of the 9th workshop on multimedia & security. ACM; 2007. p. 43–50.
Fan N, Jin C, Huang Y. A pixel-based digital photo authentication framework via demosaicking inter-pixel correlation. In: Proc. of the 11th ACM workshop on multimedia and security 2009. p. 125–30.
Fan Z, Queiroz RL. Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Trans Image Process 2003; 12(2):230–5.
Fang Y, Dirik AE, Sun X, Memon N. Source class identification for DSLR and compact cameras. In: Proc. IEEE workshop on multimedia signal processing 2009b. p. 1–5.
Fang Z, Wang S, Zhang X. Image splicing detection using camera characteristic inconsistency. In: Proc. of International conference on multimedia information networking and security 2009a. p. 20–4.
Farid H. Detecting digital forgeries using bispectral analysis. Technical Report AIM-1657. AI Lab, Massachusetts Institute of Technology; 1999.
Farid H. Exposing digital forgeries in scientific images. In: Proc. ACM multimedia and security workshop 2006a. p. 29–36.
Farid H. Digital image ballistics from JPEG quantization. Technical Report TR2006–583. Department of Computer Science, Dartmouth College; 2006b.
Farid H. A survey of image forgery detection. IEEE Signal Proc Mag 2009a; 2(26):6–25.
Farid H. Exposing digital forgeries from JPEG ghosts. IEEE Trans Inf Forensics Security 2009b;1(4):154–60.
Farid HA. 3-D lighting and shadow analysis of the JFK Zapruder film (Frame 317). Department of Computer Science, Dartmouth College; 2010. TR2010-677.
Farid H, Bravo M. Image forensic analyses that elude the human visual system. In: Proc. SPIE symposium on electronic imaging, vol. 7541. 2010. p. 754106–754106-10.
Fillion CS, Sharma G. Detecting content adaptive scaling of images for forensic applications. In: Proc. of the SPIE, electronic imaging, media forensics and security XII, vol. 7541. 2010. p. 75410.
Fridrich J. Digital image forensics. IEEE Signal Process Mag 2009;2(26): 26–37.
Fridrich J, Lukas J. Estimation of primary quantization matrix in double compressed JPEG images. In: Proc. of the digital forensic research workshop (DFRWS), vol. 2. 2003.
Fridrich J, Pevny T. Detection of double-compression for applications in steganography. IEEE Trans Inf Forensics Security 2008;3(2):247–58.
Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. In: Proc. of digital forensic research workshop 2003. p. 55–61.
Fu D, Shi Y, Su W. Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition. In: Proc. of International workshop on digital watermarking 2006. p. 177–87.
Fu D, Shi Y, Su W. A generalized Benford's law for JPEG coefficients and its applications in image forensics. In: Proc. SPIE electronic imaging: security, steganography, and watermarking of multimedia contents, vol. 6505. 2007. p. 65051L.
Gallagher AC. Detection of linear and cubic interpolation in JPEG compressed images. In: Proceedings of the 2nd Canadian conference on computer and robot vision (CRV'05) 2005. p. 65–72.
Gallagher A, Chen T. Image authentication by detecting traces of demosaicing. In: Proc. Proceedings of the CVPR WVU workshop 2008. p. 1–8.
Ghorbani M, Firouzmand M, Faraahi A. DWT-DCT (QCD) based copy-move image forgery detection. In: Proc. of 18th International conference on systems, signals and image processing (IWSSIP) 2011. p. 1–4.
Gloe T, Kirchner M. On resampling detection in re-compressed images. In: Proc. IEEE workshop on information forensics and security 2009. p. 21–5.
Gloe T, Winkler A, Borowka K. Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics. In: Proc. SPIE conference on media forensics and security 2010. p. 754107.
Goljan M, Fridrich J. Identifying images corrected for lens distortion using sensor fingerprints. In: Proc. SPIE, electronic imaging, media watermarking, security, and forensics XIV 2012. p. OH 1–13.
Gopi E, Lakshmanan N, Gokul T, Ganesh S, Shah P. Digital image forgery detection using artificial neural network and auto regressive coefficients. In: Proc. Canadian conference on electrical and computer engineering 2006. p. 194–7.
Gou H, Swaminathan A, Wu M. Noise features for image tampering detection and steganalysis. In: Proc. International conference on image processing (ICIP) 2007. p. 97–100.
Gul G, Avcibas I. Source cell phone camera identification based on singular value decomposition. In: Proc. IEEE workshop on information forensics and security 2009. p. 171–5.
Gul G, Avcibas I, Kurugollu F. SVD based image manipulation detection. In: Proc. International conference on image processing (ICIP) 2010. p. 1765–8.
Hsiao DY, Pei SC. Detecting digital tampering by blur estimation. In: Proc. of first International workshop on systematic approaches to digital forensic engineering (SADFE'05) on systematic approaches to digital forensic engineering 2005. p. 264.
Hsu Y, Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. In: Proc. IEEE International conference on multimedia and Expo (ICME) 2006. p. 549–52.
http://www.fourandsix.com/photo-tampering-history/category/2012 [accessed 10.12.12].
https://www.swgit.org/documents.
Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. In: Proc. of the 2008 IEEE Pacific-Asia workshop on computational intelligence and industrial application 2008. p. 272–6.
Huang F, Huang J, Shi YQ. Detecting double JPEG compression with the same quantization matrix. IEEE Trans Inf Forensics Security 2010; 5(4):848–56.
Huang Y, Long Y. Demosaicking recognition with applications in digital photo authentication based on a quadratic pixel correlation model. In: Proc. IEEE conference on computer vision and pattern recognition 2008. p. 1–8.
Irene L, Caldelli R, Del A, Serra G. A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Security 2011;6(3):1099–110.
Johnson M, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: Proc. ACM multimedia and security workshop 2005. p. 1–10.
Johnson M, Farid H. Exposing digital forgeries through chromatic aberration. In: Proc. ACM multimedia and security workshop 2006b. p. 48–55.
Johnson M, Farid H. Metric measurements on a plane from a single image. Technical Report TR2006-579. Department of Computer Science, Dartmouth College; 2006a.
Johnson M, Farid H. Exposing digital forgeries in complex lighting environments. IEEE Trans Inf Forensics Security 2007a;3(2):450–61.
Johnson M, Farid H. Exposing digital forgeries through specular highlights on the eye. In: Proc. International workshop on information hiding 2007c. p. 311–25.
Johnson M, Farid H. Detecting photographic composites of people. In: Proc. of 6th International workshop on digital watermarking 2007. p. 19–33.
Junfeng H, Zhouchen L, Lifeng W, Xiaoou T. Detecting doctored JPEG images via DCT coefficient analysis. In: Proc. of the 9th European conference on computer vision, vol. Part III. 2006. p. 423–35.
Kakar P, Natarajan S, Ser W. Exposing digital image forgeries by detecting discrepancies in motion blur. IEEE Trans Multimed 2011;13(3):443–52.
Kakar P, Sudha N. Exposing postprocessed copy-paste forgeries through transform-invariant features. IEEE Trans Inf Forensics Security 2012; 7(3):1018–28.
Kang X, Li Y, Qu Z, Huang J. Enhancing source camera identification performance with a camera reference phase sensor pattern noise. IEEE Trans Inf Forensics Security 2012;7(2):393–402.
Kee E, Johnson M, Farid H. Digital image authentication from JPEG headers. IEEE Trans Inf Forensics Security 2011;6(3):1066–75.
Khanna N, Chiu GT-C, Allebach JP, Delp EJ. Forensic techniques for classifying scanner, computer generated and digital camera images. In: Proc. IEEE International conference on acoustics, speech and signal processing 2008. p. 1653–6.

Khanna N, Mikkilineni AK, Delp EJ. Forensic camera classification: verification of sensor pattern noise approach. Forensic Sci Commun Jan 2009;11(1).
Kharrazi M, Sencar HT, Memon ND. Blind source camera identification. In: Proc. International conference on image processing (ICIP) 2004. p. 709–12.
Kirchner M. Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue. In: Proc. of the 10th ACM workshop on multimedia and security 2008. p. 11–20.
Kirchner M. Efficient estimation of CFA pattern configuration in digital camera images. In: Proc. SPIE conference on media forensics and security, vol. 7541. 2010. p. 754111.
Kirchner M, Bohme R. Hiding traces of resampling in digital images. IEEE Trans Inf Forensics Security 2008;3(1):101–17.
Kirchner M, Fridrich J. On detection of median filtering in digital images. In: Proc. of the SPIE, electronic imaging, media forensics and security XII, vol. 7541. 2010. p. 754110–754110-12.
Langille A, Gong M. An efficient match-based duplication detection algorithm. In: Proc. of the 3rd Canadian conference on computer and robot vision 2006. p. 64.
Lanh T, Chong K, Emmanuel S, Kankanhalli MS. A survey on digital camera image forensic methods. In: Proc. IEEE International conference on multimedia and Expo (ICME) 2007a. p. 16–9.
Lanh T, Emmanuel S, Kankanhalli M. Identifying source cell phone using chromatic aberration. In: Proc. IEEE International conference on multimedia and Expo 2007b. p. 883–6.
Lee JY, Choi JH. Identifying color laser printer using noisy feature and support vector machine. In: Proc. 5th International conference on ubiquitous information technologies and applications (CUTE) 2010. p. 1–6.
Lee S, Shamma DA, Gooch B. Detecting false captioning using common-sense reasoning. Digital Invest 2006;3(1):65–70.
Leykin A, Cutzu F. Differences of edge properties in photographs and paintings. In: Proc. International conference on image processing (ICIP) 2003. p. 541–4.
Li CT. Source camera identification using enhanced sensor pattern noise. In: Proc. IEEE International conference on image processing 2009. p. 1509–12.
Li CT, Li Y. Digital camera identification using colour-decoupled photo response non-uniformity noise pattern. In: Proc. International symposium on circuits and systems 2010. p. 3052–5.
Li B, Shi YQ, Huang J. Detecting doubly compressed JPEG images by using mode based first digit features. In: Proc. IEEE workshop on multimedia signal processing 2008a. p. 730–5.
Li G, Wu Q, Tu D, Sun S. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: Proc. International conference on multimedia & Expo 2007. p. 1750–3.
Li W, Yuan Y, Yu N. Detecting copy-paste forgery of JPEG image via block artifact grid extraction. In: Proc. International workshop on local and non-local approximation in image processing 2008b. p. 121–6.
Li W, Zhang T, Ping XJ, Zheng E. Identifying photorealistic computer graphics using second-order difference statistics. In: Proc. International conference on fuzzy systems and knowledge discovery 2010. p. 2316–9.
Lin Z, He J, Tang X, Tang C. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognit 2009b;42(11):2492–501.
Liu G, Junwen W, Shiguo L, Zhiquan W. A passive image authentication scheme for detecting region-duplication forgery with rotation. J Netw Comput Appl 2011a;34(5):1557–65.
Lin H, Wang C, Kao Y. Fast copy-move forgery detection. WSEAS Trans Signal Process 2009a;5(5):188–97.
Lint Z, Wang R, Tang X, Shum H. Detecting doctored images using camera response normality and consistency. In: Proc. of IEEE Computer Society conference on computer vision and pattern recognition(CVPR'05), vol. 1. 2005. p. 1087–92.
Liu BB, Hu Y, Lee HK. Source camera identification from significant noise residual regions. In: Proc. International conference on image processing 2010. p. 1749–52.
Liu Q, Cao X, Deng C, Guo X. Identifying image composites through shadow matte consistency. IEEE Trans Inf Forensics Security 2011b; 6(3):1111–22.
Liu BB, Lee HK, Hu Y, Choi CH. On classification of source cameras: a graph based approach. In: Proc. Workshop on information forensics and security 2010a. p. 1–5.
Lukas J. Digital image authentication using image filtering techniques. In: Proceedings of ALGORITMY 2000, conference on scientific computing 2000. p. 236–44.
Luo W, Huang J, Qiu G. Robust detection of region-duplication forgery in digital image. In: Proc. of the 18th International conference on pattern recognition 2006. p. 746–9.
Luo W, Huang J, Qiu G. A novel method for block size forensics based on morphological operations. In: Proc. of International workshop on digital watermarking (IWDW) 2008. p. 229–39.
Luo W, Huang J, Qiu G. JPEG error analysis and its applications to digital image forensics. IEEE Trans Inf Forensics Security 2010;5(3):480–91.
Luo W, Qu Z, Pan F, Huang J. A survey of passive technology for digital image forensics. Front Comput Sci China 2007a;1(2):166–79.
Luo W, Qu Z, Huang J, Qiu G. A novel method for detecting cropped and recompressed image block. In: Proc. IEEE International conference on acoustics, speech and signal processing, vol. 2. 2007b. p. 217–20.
Lyu S, Farid H. How realistic is photorealistic? IEEE Trans Signal Process 2005;53(2):845–50.
Mahdian B, Saic S. Detection of near-duplicated image regions. In: Computer recognition systems 2Advances in soft computing, vol. 45. 2007. p. 187–95.
Mahdian B, Saic S. Blind methods for detecting image fakery. In: Proc. IEEE International Carnahan conference on security technology 2008. p. 280–6.
Mahdian B, Saic S. Detection of resampling supplemented with noise inconsistencies analysis for image forensics. In: Proc. International conference on computational sciences and its applications 2008. p. 546–56.
Mahdian B, Saic S. Blind authentication using periodic properties of interpolation. IEEE Trans Inf Forensics Security 2008c;3(3):529–38.
Mahdian B, Saic S. Detecting double compressed JPEG images. In: Proc. of 3rd International conference on imaging for crime detection and prevention (ICDP-09) 2009a. P12.
Mahdian B, Saic S. Detection and description of geometrically transformed digital images. In: Proc. Media forensics and security, proceedings of SPIE-IS & T electronic imaging, vol. 7254. 2009b. p. 72540.
Mahdian B, Saic S. A bibliography on blind methods for identifying image forgery. Signal Process Image Commun 2010;25:389–99.
Mahalakshmi DS, Vijayalakshmi K, Priyadharsini S. Digital image forgery detection and estimation by exploring basic image manipulations. Digital Invest 2012;8(3–4):215–25.
Memon N, Dittmann J, Alattar A, Delp III E. Toward the identification of DSLR lenses by chromatic aberration. In: Proc. SPIE conference on media watermarking, security, and forensics 2011. p. 788010.
Muhammad G, Hussain M, Khawaji K, Bebis G. Blind copy move image forgery detection using dyadic uncedimated wavelet transform. In: Proc. of 17th International conference on digital signal processing 2011. p. 1–6.
Myna A, Venkateshmurthy M, Patil C. Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: Proc. of the International conference on computational intelligence and multimedia applications (ICCIMA 2007) 2007. p. 371–7.
Nataraj L, Sarkar A, Manjunath S. Improving re-sampling detection by adding noise. In: Proc. SPIE conference on media forensics and security, vol. 7541. 2010. p. 75410.
Neelamani R, Queiroz R, Fan Z, Baraniuk R. JPEG compression history estimation for color images. In: Proc. International conference on image processing, vol. 2. 2003. p. III–245–248.
Ng T-T, Chang S-F, Lin C-Y, Sun Q. Passive-blind image forensics. In: Multimedia security technologies for digital rights. USA: Elsevier; 2006.
Ng T, Chang S. A model for image splicing. In: Proc. of IEEE International conference on image processing (ICIP) 2004. p. 1169–72.
Ng T, Chang S. Classifying photographic and photorealistic computer graphic images using natural image statistics. ADVENT Technical Report, #220-2006-6. Columbia University; 2004b.
Ng T, Chang S, Sun Q. Blind detection of photomontage using higher order statistics. In: Proc. IEEE International symposium on circuits and systems (ISCAS) 2004. p. 688–91.
Ng T, Tsui M. Camera response function signature for digital forensics - part I: theory and data selection. In: Proc. IEEE workshop on information forensics and security 2009p.156–160.
Ng T-T. Camera response function signature for digital forensics – part II: signature extraction. In: Proc. IEEE workshop on information forensics and security 2009. p. 161–5.
Ng T-T, Chang S-F, Hsu J, Xie L, Tsui M-P. Physics-motivated features for distinguishing photographic images and computer graphics. In: Proc. of the 13th annual ACM International conference on multimedia 2005. p. 239–48.
Ng T-T, Chang S-F. An online system for classifying computer graphics images from natural photographs. In: Proc. SPIE Electronic imaging 2006.
Pearson H. Image manipulation: CSI, cell biology. Nature 2005;434:952–3.
Popescu A, Farid H. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515. Department of Computer Science, Dartmouth College; 2004.

Popescu A, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Trans Signal Process 2005a;53(10):3948–59.
Popescu A, Farid H. Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process 2005b;53(2):758–67.
Popescu AC. Statistical tools for digital image forensics (Ph.D. thesis). Hanover: Department of Computer Science, Dartmouth College; 2004.
Prasad S, Ramakrishnan KR. On resampling detection and its application to image tampering. In: Proc. of the IEEE International conference on multimedia and exposition 2006. p. 1325–8.
Qiumin W, Shuozhong W, Xinpeng Z. Log-polar based scheme for revealing duplicated regions in digital images. IEEE Signal Process Lett 2011;18(10):559–62.
Qingzhong L, Andrew H. A new approach for JPEG resize and image splicing detection. In: Proc. ACM multimedia and security workshop 2009. p. 43–8.
Qu Z, Luo W, Huang J. A convolutive mixing model for shifted double JPEG compression with application to passive image authentication. In: Proc. IEEE International conference on acoustics, speech and signal processing 2008. p. 1661–4.
Redi JA, Taktak W, Dugelay J. Digital image forensics: a booklet for beginners. Multimed Tools Appl 2011;51(1):133–62.
Rocha A, Scheirer W, Boult T, Goldenstein S. Vision of the unseen: current trends and challenges in digital image and video forensics. ACM Comput Surv 2011;43(4):26:1–26:42.
Rocha A, Goldenstein S. Is it fake or real?. In: Proc. XIX Brazilian symposium on computer graphics and image processing 2006.
Sankar G, Zhao V, Yang Y-H. Feature based classification of computer graphics and real images. In: Proc. IEEE International conference on acoustics, speech and signal processing 2009. p. 1513–6.
Sarkar A, Nataraj L, Manjunath BS. Detection of seam carving and localization of seam insertions in digital images. In: Proc. of the 11th ACM workshop on multimedia and security 2009. p. 107–16.
Sencar HT, Memon N. Overview of state-of-the-art in digital image forensics. In: Proc. Indian Statistical Institute platinum jubilee monograph series titled statistical science and interdisciplinary research 2008. p. 1–20.
Sergio B, Asoke N. Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Process 2011;91:1759–70.
Shi Y, Chen C, Chen W. A natural image model approach to splicing detection. In: Proc. of ACM workshop on multimedia and security (ACM MMSEC07) 2007a. p. 51–62.
Shi YQ, Chen W, Xuan G. Identifying computer graphics using HSV color model and statistical moments of characteristic functions. In: Proc. IEEE International conference on multimedia and Expo 2007b. p. 1123–6.
Stamm M, Liu K. Blind forensics of contrast enhancement in digital images. In: Proc. IEEE International conference on image processing 2008. p. 3112–5.
Stamm M, Liu K. Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Trans Inf Forensics Security 2010;5(3):492–506.
Sutthiwan P, Ye J, Shi YQ. An enhanced statistical approach to identifying photorealistic images. In: Proc.8th International workshop on digital watermarking 2009a. p. 323–35.
Sutthiwan P, Shi YQ, Wei S, Tian-Tsong N. Rake transform and edge statistics for image forgery detection. In: Proc. IEEE International conference on multimedia and Expo (ICME) 2010. p. 1463–8.
Sutthiwan P, Cai X, Shi YQ, Zhang H. Computer graphics classification based on Markov process model and boosting feature selection technique. In: Proc. IEEE International conference on image processing 2009b. p. 2913–6.
Suwendi A, Allebach JP. Nearest-neighbor and bilinear resampling factor estimation to detect blockiness or blurriness of an image. J Electron Imaging 2008;17(2):94–101.
Sutcu Y, Coskun B, Sencar HT, Memon N. Tamper detection based on regularity of wavelet transform coefficients. In: Proc. IEEE International conference on image processing (ICIP) 2007. p. 397–400.
Swaminathan A, Wu M, Liu KJR. Image tampering identification using blind deconvolution. In: Proc. International conference on image processing (ICIP) 2006a. p. 2309–12.
Swaminathan A, Min W, Liu KJR. Non-intrusive forensic analysis of visual sensors using output images. In: Proc. IEEE International conference on acoustics, speech and signal processing, vol. 5. 2006b. p. V.
Swaminathan A, Min W, Liu KJR. Component forensics. IEEE Signal Process Mag 2009;26(2):38–48.
Takamatsu J, Matsushita Y, Ogasawara T, Ikeuchi K. Estimating demosaicing algorithms using image noise variance. In: Proc. IEEE conference on computer vision and pattern recognition 2010. p. 279–86.
Tjoa S, Lin W, Liu K. Transform coder classification for digital image forensics. In: Proc. International conference on image processing (ICIP) 2007a. p. 105–8.
Tjoa S, Lin W, Zhao H, Liu K. Block size forensic analysis in digital images. In: Proc. IEEE International conference on acoustics, speech and signal processing 2007b. p. I-633–6.
Vazquez-Padin D, Perez-Gonzalez F. Prefilter design for forensic resampling estimation. In: Proc. workshop on information forensics and security 2011. p. 1–6.
Wang W, Dong J, Tan T. Effective image splicing detection based on image chroma. In: Proc. IEEE International conference on image processing 2009. p. 1257–60.
Wang Y, Moulin P. On discrimination between photorealistic and photographic omages. In: Proc. IEEE International conference on acoustics, speech, and signal processing, vol. 2. 2006. p. II.
Wang W, Dong J, Tan T. Tampered region localization of digital color images based on JPEG compression noise. In: Proc. International workshop on digital watermarking 2010. p. 120–33.
Wang X, Xuan B, Long Peng S. Digital image forgery detection based on the consistency of defocus blur. In: Proc. International conference on intelligent information hiding and multimedia signal processing 2008. p. 192–5.
Weihai L, Nenghai Y, Yuan Y. Doctored JPEG image detection. In: Proc. IEEE International conference on multimedia and Expo 2008. p. 253–6.
Wei W, Wang S, Zhang X, Tang Z. Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery. IEEE Trans Inf Forensics Security 2010;5(3):507–17.
Wu R, Li X, Yang B. Identifying computer generated graphics via histogram features. In: Proc. International conference on image processing 2011. p. 1933–6.
XiaoBing K, ShengMin W. Identifying tampered regions using singular value decomposition in digital image forensics. In: Proc. of International conference on computer science and software engineering 2008. p. 926–30.
Xunyu P, Siwei L. Region duplication detection using image feature matching. IEEE Trans Inf Forensics Security 2011;5(4):857–67.
Xu G, Shi YQ, Su W. Camera brand and model identification using moments of 1-D and 2-D characteristic functions. In: Proc. 16th IEEE International conference on image processing 2009. p. 2917–20.
Yingda L, Xuanjing S, Haipeng C. An improved image blind identification based on inconsistency in light source direction. J Supercomput 2011;58(1):50–67.
Ye S, Sun Q, Chang E. Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In: Proc. IEEE International conference on multimedia and Expo (ICME) 2007. p. 12–5.
Yu-Feng H, Shih-Fu C. Camera response functions for image forensics: an automatic algorithm for splicing detection. IEEE Trans Inf Forensics Security 2010;5(4):816–25.
Zhang W, Cao X, Qu Y, Hou Y, Zhao H, Zhang C. Detecting and extracting the photo composites using planar homography and graph cut. IEEE Trans Inf Forensics Security 2010;5(3):544–55.
Zhang W, Cao X, Zhang J, Zhu J, Wang P. Detecting photographic composites using shadows. In: Proc. IEEE International conference on multimedia and Expo 2009c. p. 1042–5.
Zhang J, Feng Z, Su Y. A new approach for detecting copy-move forgery in digital images. In: Proc. of IEEE International conference on communication systems 2008. p. 362–6.
Zhang Z, Kang J, Ren Y. An effective algorithm of image splicing detection. In: Proc. International conference on computer science and software engineering 2008b. p. 1035–9.
Zhang J, Wang H, Su Y. Detection of double-compression in JPEG2000 images for application in image forensics. J Multimed 2009a;4(6):379–88.
Zhang Z, Yuan R, Jian P, Zhang H, Shan-Zhong. A survey on passive-blind image forgery by doctor method detection. In: Proc. of the seventh International conference on machine learning and cybernetics, vol. 6. 2008a. p. 3463–7.
Zhang C, Zhang H. Detecting digital image forgeries through weighted local entropy. In: Proc. IEEE International symposium on signal processing and information technology 2007. p. 62–7.
Zhao X, Li J, Li S, Wang S. Detecting digital image splicing in chroma spaces. In: Proc. International workshop on digital watermarking 2010. p. 12–22.
Zhenhua Q, Guoping Q, Jiwu H. Detect digital image splicing with visual cues. In: Proc. International workshop on information hiding 2009. p. 247–61.
Zhou L, Wang D, Guo Y, Zhang J. Blur detection of digital forgery using mathematical morphology. In: Proc. of the 1st KES International symposium on agent and multi-agent systems 2007. p. 990–8.