www.ietdl.org

Published in IET Image Processing
Received on 16th July 2012
Revised on 22nd January 2013
Accepted on 19th February 2013
doi: 10.1049/iet-ipr.2012.0388

ISSN 1751-9659

Survey on blind image forgery detection

Tanzeela Qazi[1], Khizar Hayat[1], Samee U. Khan[2], Sajjad A. Madani[1], Imran A. Khan[1], Joanna Kołodziej[3], Hongxiang Li[4], Weiyao Lin[5], Kin Choong Yow[6], Cheng-Zhong Xu[7]

[1]*Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, Pakistan*
[2]*Electrical and Computer Engineering, North Dakota State University, Fargo, ND, USA*
[3]*Institute of Computer Science, Cracow University of Technology, Cracow, Poland*
[4]*Department of Electrical and Computer Engineering, University of Louisville, Louisville, KY, USA*
[5]*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, People's Republic of China*
[6]*Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, People's Republic of China*
[7]*Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI, USA*
E-mail: samee.khan@ndsu.edu

Abstract: With the mushroom growth of state-of-the-art digital image and video manipulations tools, establishing the authenticity of multimedia content has become a challenging issue. Digital image forensics is an increasingly growing research field that symbolises a never ending struggle against forgery and tampering. This survey attempts to cover the blind techniques that have been proposed for exposing forgeries. This work dwells on the detection techniques for three of the most common forgery types, namely copy/move, splicing and retouching.

1 Introduction

A picture may worth a thousand words but, alongside, it may have scores of interpretations. One wonders whether the proverbs, like 'seeing is believing', are relevant in today's life. Images and videos can be altered on the fly with a variety of common editing tools. Some of the manipulated images 'have even' received awards for their 'originality'. Owing to such sophisticated digital image/video editing software tools, the establishment of the authenticity of an image has become a challenging task, encompassing a variety of issues. In this age of illusions, there is a huge question mark over the use of multimedia data as an evidence in the courts of law.

Digital image forensics is a field that analyses images of a particular scenario to establish (or otherwise) credibility and authenticity through a variety of means. It is fast becoming a popular field because of its potential applications in many domains, such as intelligence, sports, legal services, news reporting, medical imaging and insurance claim investigations [1, 2]. A very interesting area within this context is the sports' video tampering. The increasing reliance on the technology – in popular sports, such as football, tennis and cricket – has the risk of tampering outcomes in the favour of one of the competitors because of the amounts of the monetary investments, legally (telecasting and betting) or illegally (match fixing and spot fixing). This survey deals with the state-of-the-art digital image forensics in the context of three predominant types of forgeries: (a) copy or move forgery, (b) image splicing and (c) image retouching. There are already some attempts to review blind forensics techniques, such as those reported in [1, 3–7]. However, the authors of these surveys focus only on the characteristics of one selected class of forgery methodologies. We attempt to exhaustively survey the recent literature on the subject to complement those efforts.

The rest of the survey is organised as follows. A concise account of the background concepts, needed for the understanding of this survey, is given in Section 2. Sections 3–5 are dedicated to the survey of image forensics in the context of the three considered types of forgeries. The concluding remarks are provided in Section 6.

2 Background

The driving force behind the digital image forensics is image forgery. Image forgery can be traced back to as early as 1840s when Hippolyte Bayrad created the very first fake image (Fig. 1), in which he was shown committing a suicide [8]. In 1860s another fake image appeared in which the head of Abraham Lincoln (the then US President) was fixed over the body of an adversary politician, John Calhoun [9]. Many other instances could be found in the history of the period spanning over the late 19th century and the early 20th century. With the advent of the Hollywood factor, motion films with synthesised scenes have become a norm. Various tampered war photographs then appeared and the use of such photographs was considered part and parcel of a successful war propaganda. Computers revolutionised the art with early 'super examples' of the work as Terminator, Jurassic Park and Forest Gump, in the early 1990s. The 21st century dawned with the tragedy of 9/11, when many innocent civilians lost their lives. Different videos of Osama bin Laden emerged, of which many were, later on,

Fig. 1 *First fake image*

determined to be fake through forensics analyses [10]. With the passage of time, many advanced software editing tools have been made available to the end users who can now easily alter an image with little or no effort. With such a long history of forgeries, photography, especially digital photography has lost its innocence. Over the past few years, many techniques have been introduced to tamper images or videos. These techniques can be classified into following three general categories [2, 8]:

1. copy/move forgery,
2. image splicing and
3. image retouching.

The techniques from each of these categories can be implemented additionally as (a) active or (b) passive approaches [7]. The active approaches are mostly concerned with the data hiding techniques, such as digital watermarks and digital signatures, wherein prior information is considered essential and integral to the process. Data hiding approaches embed some secondary data into the cover images. Usually, the watermarks are either embedded at the time of the image acquisition through specially equipped devices or later after further processing of the actual image. However, the latter approach may degrade the quality of the original image [4]. As opposed to their active counterparts, the passive approaches do not require any prior explicit information about the original image [7, 11, 12]. The passive blind techniques, where the analyser has just the final product at disposal, provide a solution to identify image alterations without relying on the insertion of an extrinsic data or digital signatures for the image authentication. These blind techniques are the main category of the forensic method surveyed in this paper.

Blind passive forgery detection methods are broadly categorised as being (a) visual and (b) statistical. Visual methods are based on visual clues that may not require no hardware or software tools. For example, inconsistencies in images and light deformation on an object within an image. In contrast, the statistical methods are considered more robust and convincing as they analyse the pixel values of the image.

The operations that are performed in blind image forensics have three main aspects:

1. source identification,
2. forgery detection and
3. detection of computer generated images.

Source identification [13] specifies the source device that had been used to capture the image, whereas forgery detection traces the tampering evidence [http://www.csc.fsksm.utm.my/syed/research/image-forensics/10-image-forensics.html]. The availability of traces or clues would indicate that the image in question is tampered with or otherwise [7]. Owing to the availability of sophisticated software and hardware tools, it is possible to create computer generated images and illusions. The film industry has been actively using such tools to routinely turn fiction into reality with real-life accuracy.

3 Detection of copy/move forgery

Copy/move forgery is one of the most popular forms of tampering in which some region is copied from a particular location in an image and thereafter pasted at one or more locations within the same image or a different image of preferably the same scene [2]. Two examples are given in Fig. 2 to demonstrate the copy/move forgery.

The original image, as reported in [14] in the form of Fig. 2*a*, is depicting two army vehicles. The image is forged to obtain the image in Fig. 2*b*. The truck has been camouflaged from the image by copying a region that is roughly of a circumference as indicated by the circle and moved to the location of the truck (in the original image). The second example (Fig. 2*c*), which is cropped from an original birth certificate, offers an instance of a very serious crime in the form of document forgery. The tampered version is shown in Fig. 2*d*, in which, one can see how the birth date has been changed by copying digits from the registration number field.

Recent surveys and feature analysis studies dwelling on the copy/move forgery detection can be found in [2, 15–18]. A simple taxonomy of such methods presented in most of these publications follow the classification, graphically described in Fig. 3. Broadly speaking, the detection methods may either be brute force, involving exhaustive search or block based. These techniques usually rely on the correlation between the original patch and the suspected pasted version.

The 'brute force' approach involves an exhaustive search that overlays a given image with circularly shifted versions to examine matching segments [14]. 'Exhaustive search' is not that effective when some post-processing is applied to the copied area. Moreover, the computational complexity is too high to make such a comparison with an attractive proposition. With very large copy/move patches, autocorrelation may also be an effective strategy to reduce the complexity. However, normally the patch sizes cannot be made to conform to about a quarter of the forged image [14]. 'Block-based matching' techniques give better results in comparison with the exhaustive search- and autocorrelation-based methodologies. Exact matching of blocks may have limited value in the face of the fact that

Fig. 2 *Example of copy-move forgery*
a Original image 1
b Forged image 1

usually the forged areas are post-processed and may not retain the original values. 'Approximate block matching' can be a better option as one can impose some threshold on the (mis)matching or extract robust features (RFs) from the suspect area for comparison. A typical approximate block matching strategy splits the image into overlapping blocks and apply a suitable technique to extract features on the basis of which the blocks are compared to determine similarity. The block-based matching techniques may be classified as follows.

3.1 Spatial domain matching

Most of the known block matching techniques concentrate on the transform domain rather than the spatial domain. Of the few spatial domain algorithms, one is proposed in [19] to detect region duplication. The algorithm splits the image into overlapping blocks and for comparison, extracts a vector of seven features from each of the blocks. The first three features are the respective averages of red, blue and green colour components. The other four features are obtained after transforming the image to the ***YCbCr*** space – as the ***Y***-component – on the basis of horizontal, vertical and the two diagonal directions. An array consisting of the vector of each block is then lexicographically sorted to carry out the matching. Note that the ***RGB*** to ***YCrCb*** transform involves a relationship of the form

$$\begin{bmatrix} \boldsymbol{Y} \\ \boldsymbol{Cb} \\ \boldsymbol{Cr} \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.16875 & -0.33126 & 0.5 \\ 0.5 & -0.41869 & -0.08131 \end{bmatrix} \times \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{G} \\ \boldsymbol{B} \end{bmatrix}$$

The inverse would then be

$$\begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{G} \\ \boldsymbol{B} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1.402 \\ 1 & -0.34413 & -0.71414 \\ 1 & -1.772 & 0 \end{bmatrix} \times \begin{bmatrix} \boldsymbol{Y} \\ \boldsymbol{Cb} \\ \boldsymbol{Cr} \end{bmatrix}$$

Another spatial domain method [20] is based on the decomposition of the bit-plane slices of the investigated image followed by the encoding of these bit blocks with respective ASCII values, and then looking for the duplicated regions. This process produces high accuracy in reasonable time, but does not work for the JPEG images and in cases of rotation and scaling of the copied region.

There are many spatial domain techniques showing robustness against some post-processing. Liu *et al.* [21] use circle block and Hu moments to detect the rotated regions in a forged image. The method is claimed to have a good accuracy and low computational complexity because of its reliance on fewer selected features. To reduce the time complexity, Sekeh *et al.* [22] propose a technique based on

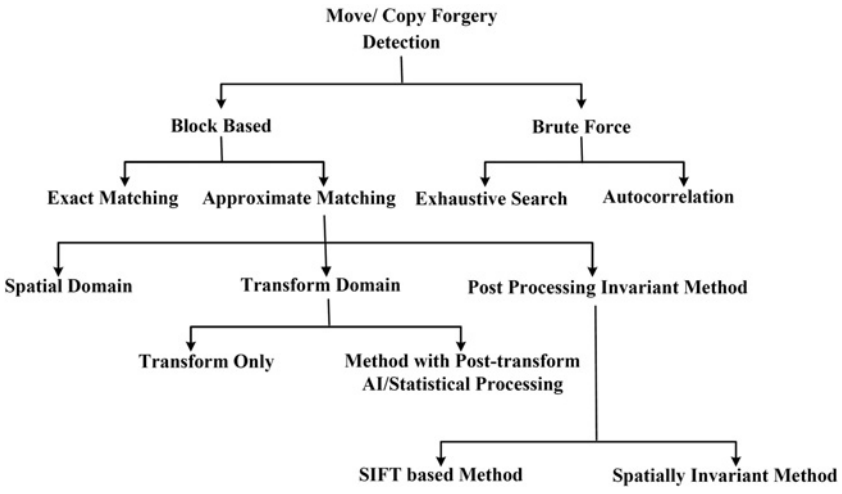

Fig. 3 *Methodology classification*

doi: 10.1049/iet-ipr.2012.0388

the block clustering that is implemented by using the local block matching algorithm. The technique reported in [23] applies radix sort to the overlapping blocks followed by the median filtering and connected component analysis for forgery detection. The method is claimed to be simple, efficient and localises detection without image degradation.

3.2 Transform domain matching

The approximate block matching techniques are usually based on the use of some intra component transformations, such as the discrete cosine transform (DCT) [24] or the discrete wavelet transform (DWT) [25]; and some artificial intelligence (AI), or statistical techniques, such as the principal component analysis (PCA) [26]. The general equation for a two-dimensional (2D) ($M \times N$ image) DCT is of the following form

$$\hat{a}_{k,l} = u_k v_l \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} a_{r,s} \cos\left(\frac{\pi k}{m}\frac{(2r+1)}{2}\right) \times \cos\left(\frac{\pi l}{n}\frac{(2s+1)}{2}\right) \quad (1)$$

with $u_0 = \sqrt{1/m}$, $u_k = \sqrt{2/m}$ for $k > 0$, $v_0 = \sqrt{1/n}$, $v_l = \sqrt{2/n}$ for $l > 0$,
where $a_{r,s}$ denotes the pixel from the rth row and the sth column and $\hat{a}_{k,l}$ denotes the DCT coefficient from the kth row and the lth column. The most popular family of the DWTs is the one by the Belgian mathematician Ingrid Daubechies who postulated it in 1988 [27]. The lossless Daubechies-5/3 transform can be taken as an example whose 1D filter can be defined as

$$\begin{cases} H_i = s_{2i+1} - \left\lfloor \frac{1}{2}(s_{2i+2} + s_{2i}) \right\rfloor \\ L_i = s_{2i} + \left\lfloor \frac{1}{4}(H_i + H_{i-1}) + \frac{1}{2} \right\rfloor \end{cases} \quad (2)$$

where L_i and H_i represent cofficients in the low- and high-frequency subbands, respectively, obtained after the application of the transform to the original signal coefficients, s_i. The 2D transformation can be realised by sequentially applying the 1D version row-wise, and then column-wise.

In the spatial domain, one can easily relate the information content of a pixel to its location within the image. That is why spatial domain methods are easy to comprehend and any manipulation for the detection of forgery is all about WYSIWYG. The downside is that, in the spatial domain, the energy is uniformly distributed and each pixel carry an important information about the scene. This may seriously jeopardise the efficiency of the underlying method. For instance, If one goes for the overlapping-block-based comparison, the computational complexity may become too high, especially for large images. In contrast, the transform domain methods have the advantage that the application of DCT or DWT decorrelate the energy and a majority of the information is concentrated in a few coefficients. This reduces the input size on the one hand and rather than comparing the entire pixels of the blocks, a few features are to compare. Even the location advantage of the spatial methods is no more, there at the advent of the localised transforms, such as DWT.

The use of a transform may have one or both of the two goals, namely (a) the reduction of effective image size and (b) the extraction of RFs. Although the former is required to reduce the time/space complexity, the latter is concerned with the realisation of a possible match even if the suspected block has undergone some post-processing. The AI techniques are usually utilised for the extraction of RFs. In most of the methods, the blocks are lexicographically sorted on the basis of the extracted features.

3.2.1 Transform-only methods: In [14], the authors detect copy/move forgery with the quantised DCT coefficients based block matching. The limitations of their technique includes false identification of a few copied areas and low reliability with small copied images. A DCT-based method [24] selects block-wise DCT coefficients to represent the specific block and lexicographically sorts the blocks to check the similarity measure on the basis of some predefined threshold value.

One of the most popular and favoured by the researchers and practitioners transform is the DWT, for its localised nature and the ability to compact most of the image information into the lowest energy sub-band that is dyadically reduced in size proportional to the image. Therefore rather than the suspect image, its lowest energy sub-band can be subjected to the forensic analysis to reduce the complexity – a level-2 sub-band would have sixteen times less coefficients to analyse. On the other hand, DWT may enable the extraction of very good and RFs for comparisons. A DWT-based method [28], first, exhaustively searches for the identification of matching blocks, and then uses phase correlation for the detection of the copied region. However, the technique gives poor results if the copied region is slightly scaled or rotated [2, 28]. In [29], pixel matching and DWT techniques are utilised to reduce the dimensions. Moreover, phase correlation is used for the detection steps in the copied and pasted regions. To improve the forgery localisation, mathematical morphology is employed for the connected regions. The above-mentioned technique has low complexity and exhibits robustness against the post-processing of the copied regions. However, the performance depends on the scene of the copy/move image.

The blind forensic technique for the copy/move forgery detection reported in [30, 31] uses DWT to reduce dimensions and to generate the overlapping blocks of the compressed image. Thereafter, the blocks are sorted lexicographically and phase correlation is used for similar block checking. The technique reduces the time for the detection process. Another DWT method, by the same authors, is proposed in [32], which has a higher detection rate compared with the techniques detailed in [14, 33]. The technique consists of two phases and uses multi-resolution characteristics of the wavelets transform to reduce dimensions. Thereafter, overlapping blocks of fixed sizes are lexicographically sorted and checked through the similarity measures. The technique exhibits robustness even if the forged region is retouched further. Muhammad and Bebis [34] have suggested a dyadic wavelet transform for the blind copy/move forgery detection that is translation invariant. The dyadic transform results in sub-bands after which they check the similarity and dissimilarity of blocks in approximate and detailed sub-bands. The noise inconsistencies are checked in the copied move regions and appropriated using the DWT. Zimba and Xingming [35]

combine DWT and PCA to detect the copy/move forgery, but the method shows poor robustness.

3.2.2 Methods employing post-transform AI/statistical processing: To reduce the complexity, one approach proposes the sorted neighbourhood strategy on the basis of DWT and 'singular value decomposition (SVD)' [36]. In this technique, DWT is applied to shrink the image followed by the use of SVD to select the reduced dimensions of the fixed-sized blocks from the wavelet sub-bands. These SV vectors are sorted lexicographically, which brings duplicated blocks closer, in a neighbourhood, in the sorted list to facilitate the detection process. Such forgery detection techniques are mostly not effective on smooth/uniform areas and highly textured images [14]. In [37], the authors propose a two-level block matching technique wherein the first-level treatment divides the 8×8 fixed-sized overlapping blocks at lower resolutions and apply SVD to reduce the dimensions of the blocks. The resultant blocks are then sorted lexicographically to facilitate matching. The second level further matches the same blocks with the surrounding overlapping blocks. In [38], a method is proposed that employs SVD for the extraction of features and *k*-dimensional (KD) tree is used for the similarity measures of the image features. The SV features are invariant to the geometric transformation and somewhat degradation. The method is claimed to have lower complexity compared with some state-of-the-art methods, such as [14, 19, 28, 33], and robust against scaling, rotation, noise and blurring.

A comparison study has been carried out in [25] that elaborates the characteristics of the PCA and DCT in the presence of noise and compression. The aforementioned study advocates the preference of the PCA, both for its accuracy and low time complexity. Mahdian and Saic [26] presented a blur moment invariant method, in which the block dimensions are reduced by the PCA. This method works effectively when some post-processing is performed on the copied region and/or blur degradation, changes are brought in the contrast, or some additional noise is introduced in the image. The limitations of this technique are the higher computational time and poor performance for the identical or smooth areas. Popescu and Farid [33] utilised the PCA method to reduce the dimensions of fixed-sized blocks. Forged regions are then detected by sorting the blocks lexicographically. The technique showed some robustness against small alterations in parts of the image, but was responsive to additive noise and JPEG compression.

3.3 Post-processing invariant methods

A majority of the copy/move forgery detection techniques, presented above are advantageous to use. However, they have a very limited scope. Most of the techniques despite having a fair amount of accuracy, exhibit high computational complexity and are usually less robust to affine transformations (rotation and scaling) and JPEG (re) compression. This part mainly deals with post-processing invariant techniques and is dedicated to methods exhibiting robustness to scaling, rotation and other geometric transformations. In this context, a lot of work, in the literature, has been dedicated to scale invariant feature transform (SIFT). That is why we categorise SIFT-based methods separately.

3.3.1 SIFT-based methods: Huang *et al.* [39] have proposed the use of SIFT, which is used for computing local statistical features. SIFT descriptors detect the changes in rotation and scaling, but are somehow lacking in performance. The technique of [40] is effective when the duplicated regions have distortions because of geometrical transformations and illuminations. The method uses the key points, and then compute features at the detected key points by the SIFT algorithm. For the detection, affine transformation is applied to the identical regions. Thereafter, a robust estimation method known as the random sample consensus is used for the correct key point matching. The accuracy rate is very high for the detection of the precise location. Another region duplication algorithm [41], based on the SIFT features, enhances the performance and accuracy by matching the SIFT features to generate results that are less susceptible to noise and JPEG compression. The technique works effectively against continuous rotation at various angles and exhibits robustness to local luminance and contrast changes. SIFT has been used by Amerini *et al.* [42] in combination with the DCT to detect forgery and also to recover the underlying geometric transforms. In [43], a region duplication algorithm is proposed that is based on the Zernike moments. The algorithm is reported to exhibit superior performance in the context of insensitivity to the noise and image deformation. Various experiments were performed to benchmark these methods and the researchers concluded that if the copied region is rotated before pasting, then the system detects the forgery accurately. However, the method does not perform well when scaling and other affine transforms are performed on the original image.

3.3.2 Specialised invariant methods: Methods robust against geometric transformations fall in this category [http://www.ee.columbia.edu/ln/dvmm/publications/PhD_theses/ttng_thesis.pdf]. Christlein *et al.* [16] have studied various features for uncovering the copy or paste forgery in images of diverse sizes and textures. They analyse that the lexicographic sorting has a lower false positive rate, but not suitable when implemented on geometric transformations. In contrast, the Fourier–Mellin transform (FMT) returns an overall balanced system accuracy on the geometric transformations. The same authors proposed a rotation invariant technique in [44], known as the same affine transformation selection (SATS) method. SATS has been applied in a robust method [45] for the verification of duplicated image portions to the block-wise feature vectors obtained from the lowest frequency DWT sub-band by a sliding window raster scan. On the basis of colour coherence, statistical feature are computed from the coherence characterisation and a support vector machine (SVM) classifier is used for the blur tampering detection with a high accuracy rate [46]. The approach reported in [47] is robust against rotation, scaling, noise and blurring with a very low computational complexity. The technique extracts features by applying FMT and uses the counting bloom filters. A colour image specific algorithm based on the sensor pattern noise was proposed in [48]. Pattern noise is extracted by using the wavelet-based Weiner de-noising filter, which allows features to be selected based on the signal to noise ratio, information entropy, variance of the pattern noise and average of the energy gradient. The method is claimed to be robust against geometric transformations, such as rotation and scaling, noise and JPEG compression.

doi: 10.1049/iet-ipr.2012.0388

Another forgery detection technique based on the rotation of duplicated region uses circle block with different angles for detection [49]. The algorithm solves the main problem of time complexity by reducing the search space with the Gaussian pyramid decomposition and reduces the block dimensions by using PCA. A fast method for forgery detection has been proposed in [50] that is based on the speed-up RFs (SURF). The key points are detected by using SURF and matching is found by using a certain threshold for the detection process. The method is robust against rotation, scaling, additive noise and blurring within an image. Most recently, a passive blind forgery detection scheme was proposed on the basis of content adaptive quantisation table estimation [51]. The technique can be used for the detection of various types of forgeries, such as copy/move, splicing and synthetic. The accuracy rate of the procedure reported in [51] is as high as other previously documented techniques and it is insensitive to the JPEG images.

The methodologies outlined above are handicapped by one or more of the following constraints:

- accuracy,
- processing efficiency,
- robustness to post-processing in the form of (a) affine transformations and (b) compression (especially the JPEG).

Accuracy has improved over the years, but even on that front many techniques have a low detection rate if some of the geometric transforms are applied to the image or if the tampered region is small. A near-to-universal approach is still a far cry. Therefore there is a genuine need to develop techniques that can eliminate the limitations of the current approaches.

4 Image splicing

Image splicing techniques significantly change the original image(s) and involve the composition of more than one image that are combined to generate a tampered image. If two images with different backgrounds are spliced, then it is relatively harder to make the boundaries imperceptible. The example reported in [8] and reproduced in Fig. 4 illustrates the concept of image splicing, wherein the original image of a rescue helicopter is flipped, and then the image of shark is blended to obtain a forged image [12].

Blind splicing detection is a challenging problem whereby the joining regions are investigated by a variety of methods. The presence of sharp edges (or changes) between different regions and their surroundings constitute valuable clues to splicing in the image under investigation. Splicing detection methods can be roughly divided into two categories, namely region-based and boundary-based splicing detection. The boundary-based methods detect the irregular modifications at the splicing boundaries. An example is the passive method by Fang *et al.* [52] that relies on the sharp boundaries in colour images. The procedure checks the consistency of colour division in the surrounding pixels of the boundary. The authors argue that the abnormality at the colour edge gives significant evidence of tampering of the images. In region-based methods, the consistency is checked on the generative model of the image that is estimated, in case of non-blind detection, from the original and spliced image to identify the forgery. Farid emphasises the need of such a statistical image model in [53] for splicing detection. One such method extracts the features for classification by the Hilbert–Huang transform (HHT) and statistical model based on the moments of characteristic functions by applying wavelets to distinguish spliced region [54]. The technique shows high accuracy results for passive splicing detection.

One can loosely identify four categories of splicing detection methods that are detailed in the subsequent subsections.

4.1 Camera response function (CRF)

In the literature, we find quite a few methods that rely on the clues of the CRF. Hsu and Chang [55] suggested a detection technique on the basis of the CRFs in different image regions of the spliced image. The CRF is estimated from the segmented image region by applying geometric invariants with the locally planar irradiance points (LPIPs). This strategy gives comparatively better results as techniques that solely reply on visual clues. Another splicing detection method reported in [56] is based on the geometric invariants and consistency of the camera characteristics. The technique computes the geometric invariants of the pixels of doubtful regions and related CRFs of these invariants. An SVM classifier is then used for the anomaly detection. The approach is semi-automatic and requires manual labelling of ambiguous regions that may eventually be a very time consuming and cumbersome task. In [57], a

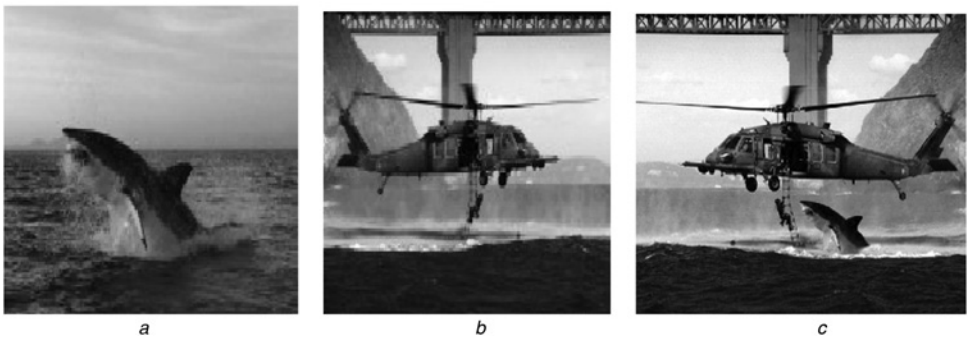

Fig. 4 *Image splicing example*

a Original image 1
b Original image 2
c Spliced image

conceptually similar but automated approach is presented. The method acquires CRF information using LPIPs from the segmented area, instead of anomalies from the estimated CRF of the entire image. In [58], Johnson and Farid introduced a technique to detect composite images that compute the principal points of camera from the image of a person's eyes. Inconsistencies of these points give evidence of tampering, but the idea fails in low-resolution images because of the smaller size of eyes in proportion to the whole image. The variation used in [59] eliminates the drawback of low-resolution image by using other facial features, such as nose or chin instead of the eyes. However, the technique also needs a reference image for the detection process, which is infeasible for many applications.

4.2 Model based

Attempts to model splicing can be frequently found in the literature. Splicing detection with visual clues is a relatively easier procedure compared with the other forgery detection techniques. In [60], a method is proposed for the boundary-based splicing detection that relies on the human visual system (HVS). Splicing correlation is found between the boundary and the fixation points produced by the visual fixation algorithm. However, the technique is highly sensitive to noise and blurring. In [61], a technique is outlined on the basis of image quality metrics (IQMs). The authors have compared their results with the HHT-based method as reported in [54]. A recently proposed technique [12] chooses the analysis of variance as the IQM. The IQMs-based techniques have proven to be considerably successful in the detection of spliced regions. A recently published technique [62] is oriented towards image quality and moment-based features. The authors show through various experiments that their technique outperforms some contemporary splicing forgery detection methods. A model is proposed in [63] that elaborates the bipolar perturbation of the signal and response of the bicoherence features for splicing detection. The same authors investigate the spliced region on the basis of bicoherence features in [64]. The paper suggests further improvements by using the bicoherence features. Johnson and Farid [65] have developed a technique on the basis of inconsistencies of light. When different parts of the image are combined as a single-spliced image, direction of light discriminates the splicing region. The drawback of the aforementioned technique is that when the light effects are same on the original and spliced regions or in the same direction, then it fails in the detection process. The blind technique reported in [66] automatically distinguishes the spliced region, in which the phase and magnitude details are sensitive to the lines, and the edges are suspected to have been caused by splicing. Moments of wavelet characteristic functions are used for the differentiation of real and spliced images. However, the experimental results show that the technique has low detection accuracy among all of the blind methods and is time consuming for the feature extraction process.

4.3 Spatial domain

For colour images, a passive splicing detection technique based on the chroma components is outlined in [67]. The methodology consists of a grey level co-occurrence matrix of edge image that is obtained from the chroma image. Threshold images are produced by subtracting the horizontal, vertical and diagonal values from the chroma image values, respectively, on the basis of some predefined threshold. Optimal feature selection is performed by the boosting feature selection and SVM classifier is used for the detection process. Experimental results show the effectiveness of technique by using the ***Cr*** and ***Cb*** channels instead of the luminance channel ***Y*** [67]. Recently, for synthetic and real images, a technique has been proposed in [68] that uses the estimated radial distortion from various regions of the image on the basis of line calibration. The efficiency of this approach is not convincing because when two images of same distortion or noise are spliced, then it gives little or no evidence of tampering. Dong *et al.* [69] analysed the discontinuity of pixels in the image and coherency caused by the splicing. Run length representations were used for feature extraction and SVM was used as the classifier. The technique has a high detection accuracy and low complexity. A feature analysis technique for the detection of splicing traces on the basis of boundary surroundings was proposed in [70]. The aforementioned technique is effective for the kind of images that are usually used in commercial products. A novel approach detailed in [71] computes the edge gradient matrix, followed by the approximate run length computation for the image splicing detection. To further improve the accuracy rate, some of the features are extracted from the histogram of the run length. The method is claimed to have low computational complexity and high detection accuracy with lower feature dimensions.

4.4 Transform domain

A lot of works in splicing digital images that are based on the spectral or transform domain methods. The approach elaborated in [72] is developed to circumvent JPEG resising, which relies on the correlation of the surrounding values of the DCT coefficients as well as the SVM for the detection process. The authors argue that the scale factors may seriously affect the performance of the methods. Moreover, the detection in a highly complex situation is not satisfactory. Sun *et al.* [73] present a wavelet domain method on the basis of the natural image statistical model. Generalised Gaussian model is employed for estimating the parameters and features from each wavelet sub-bands. Owing to the high detection accuracy and simplicity, the above-mentioned technique can be utilised for many applications. The technique proposed in [53] also uses the natural image model for tampering detection. Another region-based passive technique relies on the motion blurring [74]. The method computes blurs by using the spectral matting approach of [75]. Moreover, the method also checks the divergence or the inconsistency within the estimated blur as a difference between the doubtful spliced region and the rest of the image. A comparison with another blur-based technique, described in [76], shows that the methodology reported in [74] gives better accuracy than the existing motion blur approaches, but exhibit lower efficiency in comparison with the DCT-based approaches. Texture change can be an important side effect of splicing. The method of Jing *et al.* [77] blindly looks for such side effects resulted in the image after being tampered. The authors refer to these side effects as the 'eclosion traces' for their resemblance with the metamorphosis in insects. Dual tree wavelet transform is used for the image decomposition to remove the noise attributed to the change in the texture. Based on the gathered information, the image can be reconstructed. This technique provides better accuracy when

doi: 10.1049/iet-ipr.2012.0388

Fig. 5 *Image retouching examples*

a Original image
b Colour change
c Weather change
d Blur background

compared with the technique described in [78] that focuses on the in-harmonic points, which represent the pixels having different intensities from their neighbours. In the context of noise inconsistency, Mahdian and Saic [79] have used the high-resolution wavelet coefficients for the estimation of noise. Obviously, the detection rate of such a technique is not satisfactory when the noise ratio is low. Moreover, if the variance of isolated regions in an image is equal, then the method fails to detect the forgery. In essence, the existing methods of splicing detection have high accuracy rate, but most methods have time complexity issues and validity for geometric transformations is not that satisfactory.

5 Image retouching

Image retouching is another class of forensic methods that pertains to a slight change in the image for various aesthetic and commercial purposes, not necessarily conforming to the standards of morality. The retouching is mostly used to enhance or reduce the image features. Usually this type of forgery is realised by changing the colour or texture of the objects, intensify the weather conditions or simply introducing some blur for defusing the objects. The example [http://www.cs.uccs.edu/cs525/studentproj/projS2006/sasummer/doc/] given in Fig. 5, demonstrates the effects of the retouching. Fig. 5*a* is the original image, whereas Fig. 5*b* shows the change of colours of the headlights and some background objects. Fig. 5*c* changes the weather conditions, from cloudy weather to sunny day. Fig. 5*d* blurs some of the background cars to diffuse the information. Image retouching has long been the norm in commercial photography, usually for photo-sessions, as well as a routine in the showbiz industry. This type of forgery is also known as the image enhancement for its use to improve facial features. The example reported in [8] and shown in Fig. 6, illustrates that in magazines and other related fields, facial features are retouched that may be considered ethically wrong. We also see some of the film industry stars refusing to allow retouching of some of their figure features [http://www.dosomething.org/news/5-celebrities-rejecting-hollywoods-photoshop-fever].

Forgery detection, in case of image retouching, involves finding the enhancements, blurring, illumination and colour changing. Forgery detection may be an easy task, if the original version is available. Otherwise, with blind detection, the task may be very challenging. Detection of blurred objects, because of manipulation, is a common problem in different types of forgeries. For the manipulation of images, two types of modifications are applied, namely local and global modifications [80]. Local modifications are usually used in the copy/move forgery or in the case of splicing. For the detection of contrast enhancements that perceptually impact the image, global modifications are usually investigated. Global modifications are predominantly used for illumination and changes in contrast.

In [80], a contrast detection technique is presented that takes into account the global modifications in the image by detecting the negative or positive changes within the image on the basis of IQMs and the binary similarity measures. As already stated, the IQMs may offer considerable clues to detect the statistical changes. On the other hand, the features of binary similarity measures are used to find the differences. This non-blind technique is quite effective and produces significantly accurate results in cases, when the image is highly modified. A classifier is designed in [81] for the distortion measure between the original and the doctored image. The latter may consist of many types of operations, such as change in brightness and blurring. The classifier gives better performance if more than one operation is applied to the image.

A blind identification algorithm, for the retouching forgery is based on the bi-Laplacian filtering [82]. This technique searches for each block of the image on the basis of a KD tree and derives the adjacent matching blocks. The technique is applicable to the uncompressed images and compressed high-resolution images. The accuracy also

Fig. 6 *Retouching by a magazine in which the real face on right is replaced with the left one*

depends on the size of the tampered area for high-level compressed images. A blind forensic algorithm is detailed in [83], which not only detects the global enhancements that are used to modify the image, but also proposes a method for the histogram equalisation. A similar iterative method is based on the probabilistic model of pixel values that jointly estimates the forensic detection of contrast enhancement [84]. The probabilistic model identifies the histogram entries that are the most likely to occur with the corresponding enhancement artefacts. The algorithm provides accurate estimates if the enhancements are non-standard.

There are a variety of contrast enhancement and gamma correction detection algorithms that can blindly detect the image modifications and enhancements locally and globally [83, 85]. Cao *et al.* [86] present a method for the blind detection of gamma correction for the detection of image forgery. The forensic estimation technique is based on the histogram characteristics that are measured by patterns of the peak gap features. These peak gap features for the gamma correction detection are discriminated by the precomputed histogram of images. Experimental results suggest that this technique is effective for both local and global gamma correction modifications.

Many methods have been proposed for retouching the forgery detection. However, we still believe that the domain has not gained as much attention as the copy/move, and splicing forgeries. Most of the proposed detection techniques work well if the image has been highly modified from the original. Moreover, the techniques are mostly non-blind as the original image is needed to discriminate the statistical changes, which are caused during the contrast modifications and blurring. For example, Wei *et al.* [87] detect blur by extracting the sharp edge points in the contour domain from both the original and the tampered images.

6 Conclusions

A concise survey on the forgery detection methods was presented that may help researchers explore new ideas and provide new solutions to the challenges in the field, especially with blind methods. An attempt has been made to introduce various promising techniques that represent reasonable improvements in the forgery detection methods. Still these improvements are far from being perfect and have certain drawbacks that must be eliminated to obtain effective results. Specifically, the DCT- and PCA-based techniques, described in this survey, exhibit high computational complexity and do not possess effective accuracy rate. Moreover, the DCT-based techniques are inapplicable when considering highly textured and small forged regions. There are techniques exhibiting improved detection accuracy, but having high computational complexity. Moreover, most of the methods may not be that responsive to the geometric transformations, such as rotation and scaling. The factor of human perception is also not counted as a factor during the development of these techniques. Therefore there is a need to develop techniques that are automatic, HVS motivated and effective against geometric transformations. In essence, this work, surveyed detection techniques for three of the most common forgery types, namely copy/move, splicing and retouching. Most of these have been handicapped by one or more factors that include limited accuracy rate, low reliability and high complexity in addition to their sensitivity to various transformations and non-responsiveness to noise.

7 Acknowledgment

Samee U. Khan's work was partly supported by the Young International Scientist Fellowship of the Chinese Academy of Sciences, (grant no. 2011Y2GA01).

8 References

1 Mahdian, B., Saic, S.: 'Blind methods for detecting image fakery', *IEEE Aerosp. Electron. Syst. Mag.*, 2010, **25**, (4), pp. 18–24
2 Shivakumar, B.L., Baboo, S.S.: 'Detecting copy-move forgery in digital images: a survey and analysis of current methods', *Global J. Comput. Sci. Technol.*, 2010, **10**, pp. 61–65
3 Granty, R.E.J., Aditya, T.S., Madhu, S.S.: 'Survey on passive methods of image tampering detection'. 2010 Int. Conf. on Communication and Computational Intelligence (INCOCCI), 2010, pp. 431–436
4 Lanh, T.V., Chong, K.S., Emmanuel, S., Kankanhalli, M.S.: 'A survey on digital camera image forensic methods'. 2007 IEEE Int. Conf. on Multimedia and Expo, 2007, pp. 16–19
5 Luo, W., Qu, Z., Feng, P., Huang, J.: 'A survey of passive technology for digital image forensics', *Front. Comput. Sci. China*, 2007, **1**, (2), pp. 166–179
6 Mahdian, B., Saic, S.: 'A bibliography on blind methods for identifying image forgery', *Signal Process.: Image Commun.*, 2010, **25**, (6), pp. 389–399
7 Zhang, Z., Ren, Y., Ping, X.J., He, Z.Y., Zhang, S.Z.: 'A survey on passive-blind image forgery by doctor method detection'. Proc. Seventh Int. Conf. on Machine Learning and Cybernetics, 2008, pp. 3463–3467
8 Shaid, S.Z.M.: 'Estimating optimal block size of copy-move attack detection on highly textured image'. Thesis Submitted to the University of Technology, Malaysia, 2009. Available at http://www.csc.fsksm.utm.my/syed/images/files/publications/thesis/estimating_optimal_block_size_for_copy-move_attack_detection_on_highly_textured_image.pdf
9 Farid, H.: 'Digital doctoring: how to tell the real from the fake', *Significance*, 2006, **3**, (4), pp. 162–166
10 Krawtez, N.: 'A pictures worth digital image analysis and forensics'. Black Hat Briefings, 2007, pp. 1–31. Available at www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf.
11 Ng, T.T., Chang, S.F., Lin, C.Y., Sun, Q.: 'Passive-blind image forensics'. Zeng, W., Yu, H., Lin, C.Y., (Eds.), 'Multimedia security technologies for digital rights management' (Academic Press, 2006) pp. 383–412
12 Zhou, Z., Zhang, X.: 'Image splicing detection based on image quality and analysis of variance'. 2010 Second Int. Conf. on Education Technology and Computer (ICETC), 2001, vol. 4, pp. V4-242–V4-246
13 Popescu, A.C., Farid, H.: 'Exposing digital forgeries in color filter array interpolated images', *IEEE Trans. Signal Process.*, 2005, **53**, (10), pp. 3948–3959
14 Fridrich, J., Soukal, D., Lukàš, J.: 'Detection of copy-move forgery in digital images'. Digital Forensic Research Workshop, 2003. Available at http://www.ws2.binghamton.edu/fridrich/Research/copymove.pdf
15 Bayram, S., Sencar, H.T., Memon, N.: 'A survey of copy-move forgery detection techniques'. IEEE Western New York Image Processing Workshop, 2008. Available at http://www.cs.dartmouth.edu/farid/dfd/index.php/publications/show/219
16 Christlein, V., Riess, C., Angelopoulou, E.: 'A study on features for the detection of copy-move forgeries'. Sicherheit, 2010, pp. 105–116
17 Farid, H.: 'Image forgery detection: a survey. Signal processing magazine', *IEEE*, 2009, **26**, (2), pp. 16–25
18 Poisel, R., Tjoa, S.: 'Forensics investigations of multimedia data: a review of the state-of-the-art'. 2011 Sixth Int. Conf. on IT Security Incident Management and IT Forensics (IMF), 2011, pp. 48–61
19 Luo, W., Huang, J., Qiu, G.: 'Robust detection of region-duplication forgery in digital image'. 18th Int. Conf. on Pattern Recognition, 2006. (ICPR 2006), 2006, vol. 4, pp. 746–749
20 Ardizzone, E., Mazzola, G.: 'Detection of duplicated regions in tampered digital images by bit-plane analysis'. Proc. 15th Int. Conf. on Image Analysis and Processing. (ICIAP '09), 2009, pp. 893–901
21 Liu, G., Wang, J., Lian, S., Wang, Z.: 'A passive image authentication scheme for detecting region-duplication forgery with rotation', *J Netw. Comput. Appl.*, 2011, **34**, pp. 1557–1565
22 Sekeh, M.A., Marof, M.A., Rohani, M.F., Motiei, M.: 'Sequential straightforward clustering for local image block matching', *World Acad. Sci. Eng. Technol.*, 2011, **50**, pp. 774–778

doi: 10.1049/iet-ipr.2012.0388

23 Lin, H., Wang, C., Kao, Y.: 'An efficient method for copy-move forgery detection'. Proc. Eighth WSEAS Int. Conf. on Applied Computer and Applied Computational Science, 2009, pp. 250–253
24 Cao, Y., Gao, T., Fan, L., Yang, Q.: 'A robust detection algorithm for copy-move forgery in digital images', *Forensic Sci. Int.*, 2012, **214**, (1–3), pp. 33–43
25 Shih, F.Y., Yuan, Y.: 'A comparison study on copy-cover image forgery detection', *Open Artif. Intell. J.*, 2010, **4**, pp. 49–54
26 Mahdian, B., Saic, S.: 'Detection of copy-move forgery using a method based on blur moment invariants', *Forensic Sci. Int.*, 2007, **171**, (2–3), pp. 180–189
27 Daubechies, I.: 'Ten lectures on wavelets' (SIAM, Philadelphia, PA, 1992)
28 Myna, A.N., Venkateshmurthy, M.G., Patil, C.G.: 'Detection of region duplication forgery in digital images using wavelets and log-polar mapping'. Proc. Int. Conf. on Computational Intelligence and Multimedia Applications (ICCIMA 2007) – volume 03, 2007, pp. 371–377
29 Zhang, J., Feng, Z., Su, Y.: 'A new approach for detecting copy-move forgery in digital images'. 11th IEEE Singapore Int. Conf. on Communication Systems, 2008, 2008, pp. 362–366
30 Khan, S., Kulkarni, A.: 'An efficient method for detection of copy-move forgery using discrete wavelet transform', *Int. J. Comput. Sci. Eng.*, 2010, **02**, (05), pp. 1801–1806
31 Khan, S., Kulkarni, A.: 'Robust method for detection of copy-move forgery in digital images'. 2010 Int. Conf. on Signal and Image Processing (ICSIP), 2010, pp. 69–73
32 Khan, S., Kulkarni, A.: 'Detection of copy-move forgery using multiresolution characteristic of discrete wavelet transform'. Proc. Int. Conf. on Workshop on Emerging Trends in Technology. ICWET '11, New York, NY, USA, 2011, pp. 127–131
33 Popescu, A.C., Farid, H.: 'Exposing digital forgeries by detecting duplicated image regions' (Dartmouth College, Computer Science, Hanover, NH, 2004) TR2004-515
34 Muhammad, G., Bebis, G.: 'Blind copy move image forgery detection using dyadic undecimated wavelet transform'. Proc. Int. Conf. on Signal and Image Processing, 2010, Available at http://www.cse.unr.edu/~bebis/DSP11.pdf
35 Zimba, M., Xingming, S.: 'DWT-PCA (EVD) based copy-move image forgery detection', *Int. J. Digit. Content Technol. Appl.*, 2011, **5**, (1), pp. 251–258
36 Li, G., Wu, Q., Tu, D., Sun, S.: 'A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD'. 2007 IEEE Int. Conf. on Multimedia and Expo, 2007, pp. 1750–1753
37 Yang, Q., Huang, C.: 'Copy-move forgery detection in digital image'. Proc. 10th Pacific Rim Conf. Multimedia: Advances in Multimedia Information Processing. (PCM'09), 2009, pp. 816–825
38 Ting, Z., Rang-ding, W.: 'Copy-move forgery detection based on SVD in digital image'. Second Int. Congress on Image and Signal Processing, 2009. (CISP '09), 2009, pp. 1–5
39 Huang, H., Guo, W., Zhang, Y.: 'Detection of copy-move forgery in digital images using SIFT algorithm'. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. (PACIIA '08), 2008, vol. 2, pp. 272–276
40 Pan, X., Lyu, S.: 'Region duplication detection using image feature matching', *IEEE Trans. Inf. Forensics Secur.*, 2010, **5**, (4), pp. 857–867
41 Pan, X., Lyu, S.: 'Detecting image region duplication using SIFT features'. 2010 IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1706–1709
42 Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: 'A SIFT-based forensic method for copy–move attack detection and transformation recovery', *IEEE Trans. Inf. Forensics Secur.*, 2011, **6**, (3), pp. 1099–1110
43 Ryu, S., Lee, M., Lee, H.: 'Detection of copy-rotate-move forgery using zernike moments'. Information Hiding. 2010, pp. 51–65
44 Christlein, V., Riess, C., Angelopoulou, E.: 'On rotation invariance in copy-move forgery detection'. Proc. 2010 Second IEEE Workshop on Information Forensics and Security (WIFS), 2010, pp. 1–6
45 Zimba, M., Xingming, S.: 'Detection of image duplicated regions affected by rotation, scaling and translation using block characteristics of DWT coefficients', *Int. J. Digit. Content Technol. Appl.*, 2011, **5**, (11), pp. 143–150
46 Bo, W., Xianwei, K.: 'Exposing copy-paste-blur forgeries based on color coherence', *Chin. J. Electron.*, 2009, **18**, (03), pp. 487–490
47 Bayram, S., Sencar, H.T., Memon, N.: 'An efficient and robust method for detecting copy-move forgery'. Proc. IEEE Int. on Conf. Acoustics, Speech and Signal Processing. (ICASSP '09), 2009, pp. 1053–1056
48 Peng, F., Nie, Y., Long, M.: 'A complete passive blind image copy-move forensics scheme based on compound statistics features', *Forensic Sci. Int.*, 2012, **212**, pp. e21–e25
49 Wang, J., Liu, G., Li, H., Dai, Y., Wang, Z.: 'Detection of image region duplication forgery using model with circle block'. Int. Conf. on Multimedia Information Networking and Security, 2009. (MINES '09), 2009, vol. 1, pp. 25–29
50 Bo, X., Junwen, W., Guangjie, L., Yuewei, D.: 'Image copy-move forgery detection based on SURF'. 2010 Int. Conf. on Multimedia Information Networking and Security (MINES), 2010, pp. 889–892
51 Lin, G., Chang, M., Chen, Y.: 'A passive-blind forgery detection scheme based on content-adaptive quantization table estimation', *IEEE Trans. Circuits Syst. Video Technol.*, 2011, **21**, (4), pp. 421–434
52 Fang, Z., Wang, S., Zhang, X.: 'Image splicing detection using color edge inconsistency'. 2010 Int. Conf. on Multimedia Information Networking and Security (MINES), 2010, pp. 923–926
53 Farid, H.: 'A picture tells a thousand lies', *New Sci.*, 2003, **179**, (2411), pp. 38–41
54 Li, X., Jing, T., Li, X.H.: 'Image splicing detection based on moment features and Hilbert-Huang transform'. 2010 IEEE Int. Conf. on Information Theory and Information Security (ICITIS), 2010, pp. 1127–1130
55 Hsu, Y., Chang, S.: 'Image splicing detection using camera response function consistency and automatic segmentation'. 2007 IEEE Int. Conf. on Multimedia and Expo, 2007, pp. 28–31
56 Hsu, Y., Chang, S.: 'Detecting image splicing using geometry invariants and camera characteristics consistency'. 2006 IEEE Int. Conf. Multimedia and Expo, 2006, pp. 549–552
57 Hsu, Y., Chang, S.: 'Camera response functions for image forensics: an automatic algorithm for splicing detection', *IEEE Trans. Inf. Forensics Secur.*, 2010, **5**, (4), pp. 816–825
58 Johnson, M.K., Farid, H.: 'Detecting photographic composites of people'. Shi, Y.Q., Kim, H.J., Katzenbeisser, S., (Eds.), 'Digital watermarking' (Springer, Guangzhou, China, 2008), (LNCS Vol. 5041) pp. 19–33
59 Kee, E., Farid, H.: 'Detecting photographic composites of famous people' (Department of Computer Science, Dartmouth College, 2009) TR2009-656
60 Qu, Z., Qiu, G., Huang, J.: 'Detect digital image splicing with visual cues' (Springer-Verlag, Berlin, Heidelberg, 2009) pp. 247–261
61 Zhang, Z., Zhou, Y., Kang, J., Ren, Y.: 'Study of image splicing detection'. Proc. Fourth Int. Conf. on Intelligent Computing: Advanced Intelligent Computing Theories and Applications – with Aspects of Theoretical and Methodological Issues. (ICIC '08), 2008, pp. 1103–1110
62 Math, S., Tripathi, R.C.: 'Image quality feature based detection algorithm for forgery in images', *Int. J. Comput. Graph. Animat.*, 2011, **01**, (01), pp. 13–21
63 Ng, T.T., Chang, S.: 'A model for image splicing'. 2004 Int. Conf. on Image Processing, 2004. (ICIP '04), 2004, vol. 2, pp. 1169–1172
64 Ng, T.T., Chang, S., Sun, Q.: 'Blind detection of photomontage using higher order statistics'. Proc. 2004 Int. Symp. on Circuits and Systems, 2004. (ISCAS '04), 2004, vol. 5, pp. V-688–V-691
65 Johnson, M., Farid, H.: 'Exposing digital forgeries by detecting inconsistencies in lighting'. Proc. Seventh Workshop on Multimedia and Security. (MM&Sec '05), 2005, pp. 1–10
66 Chen, W., Shi, Y.Q., Su, W.: 'Image splicing detection using 2-D phase congruency and statistical moments of characteristic function'. Proc. SPIE 6505, Security, Steganography and Watermarking of Multimedia Contents IX, San Jose, California, January 28 – February 1, 2007, 2007, pp. 65050R–65050R-8. Available at http://www.dx.doi.org/10.1117/12.704321
67 Wang, W., Dong, J., Tan, T.: 'Effective image splicing detection based on image chroma'. 2009 16th IEEE Int. Conf. on Image Processing (ICIP), 2009, pp. 1257–1260
68 Chennamma, H.R., Rangarajan, L.: 'Image splicing detection using inherent lens radial distortion', *IJCSI Int. J. Comput. Sci. Issues*, 2011, **7**, pp. 149–158
69 Dong, J., Wang, W., Tan, T., Shi, Y.Q.: 'Digital watermarking' (Springer-Verlag, Berlin, Heidelberg, 2009) pp. 76–87
70 Jing, W., Hongbin, Z.: 'Exposing digital forgeries by detecting traces of image splicing'. Proc. Eighth Int. Conf. Signal Processing (vol. 2 of ICSP 2006). Available at http://www.ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4129006
71 He, Z., Sun, W., Lu, W., Lu, H.: 'Digital image splicing detection based on approximate run length', *Pattern Recognit. Lett.*, 2011, **32**, (12), pp. 1591–1597
72 Liu, Q., Sung, H.A.: 'A new approach for jpeg resize and image splicing detection'. Proc. First ACM Workshop on Multimedia in Forensics (MiFor '09), 2009, pp. 43–48

73 Sun, S., Wu, Q., Li, G.: 'Detection of image compositing based on a statistical model for natural images', *Acta Autom. Sin.*, 2010, **35**, pp. 1564–1567

74 Kakar, P., Natarajan, S., Ser, W.: 'Detecting digital image forgeries through inconsistent motion blur'. 2010 IEEE Int. Conf. on Multimedia and Expo (ICME), 2010, pp. 486–491

75 Levin, A., Rav-Acha, A., Lischinski, D.: 'Spectral matting'. IEEE Conf. on Computer Vision and Pattern Recognition, 2007. (CVPR '07), 2007, pp. 1–8

76 Hsiao, D.Y., Pei, S.C.: 'Detecting digital tampering by blur estimation'. First Int. Workshop on Systematic Approaches to Digital Forensic Engineering, 2005, 2005, pp. 264–278

77 Jing, T., Peng, Y., Zhang, F., Huo, Y.: 'Blind detection of digital forgeries using detection trace of eclosion'. Proc. Int. Conf. Computational Intelligence and Software Engineering, 11–13 December 2009, CiSE, 2009, pp. 1–4

78 Ying, C., Yuping, W.: 'Exposing digital forgeries by detecting traces of smoothing'. The Ninth Int. Conf. Young Computer Scientists. (ICYCS 2008), 2008, pp. 1440–1445

79 Mahdian, B., Saic, S.: 'Using noise inconsistencies for blind image forensics', *Image Vis. Comput.*, 2009, **27**, (10), pp. 1497–1503. Special Section: Computer Vision Methods for Ambient Intelligence

80 Boato, G., Natale, F.G.B.D., Zontone, P.: 'How digital forensics may help assessing the perceptual impact of image formation and manipulation'. Proc. Fifth Int. Workshop on Video Processing and Quality Metrics for Consumer Electronics – VPQM 2010, 2010. Available at http://www.enpub.fulton.asu.edu/resp/vpqm/vpqm10/Proceedings_VPQM2010/vpqm_p56.pdf

81 Avcibas, I., Bayram, S., Memon, N., Ramkumar, M., Sankur, B.: 'A classifier design for detecting image manipulations'. Proc. IEEE Int. Conf. on Image Processing, 2004, pp. 2645–2648

82 Li, X.F., Shen, X.J., Chen, H.P.: 'Blind identification algorithm for the retouched images based on bi-Laplacian', *J. Comput. Appl.*, 2011, **31**, pp. 239–242

83 Stamm, M.C., Liu, K.J.R.: 'Blind forensics of contrast enhancement in digital images'. Proc. 15th IEEE Int. Conf. Image Processing 2008, (ICIP'2008), 2008, pp. 3112–3115

84 Stamm, M.C., Liu, K.J.R.: 'Forensic estimation and reconstruction of a contrast enhancement mapping'. Proc. IEEE Int. Conf. Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1698–1701

85 Stamm, M., Liu, K.J.R.: 'Forensic detection of image manipulation using statistical intrinsic fingerprints', *IEEE Trans. Inf. Forensics Secur.*, 2010, **5**, (3), pp. 492–506

86 Cao, G., Zhao, Y., Ni, R.: 'Forensic estimation of gamma correction in digital images'. Proc. 17th IEEE Int. Conf. on Image Processing, (ICIP'2010), 2010, pp. 2097–2100

87 Wei, L.X., Zhu, J., Yang, X.: 'An image forensics algorithm for blur detection based on properties of sharp edge points', *Adv. Mater. Res.*, 2012, **341–342**, pp. 743–747

doi: 10.1049/iet-ipr.2012.0388