Signal Processing: *Image Communication* 39 (2015) 46–74

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

A bibliography of pixel-based blind image forgery detection techniques

Muhammad Ali Qureshi*, Mohamed Deriche

Department of Electrical Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

ARTICLE INFO

Article history:
Received 15 April 2015
Received in revised form
13 August 2015
Accepted 16 August 2015
Available online 24 August 2015

Keywords:
Image forensics
Copy-move forgery
Forgery detection methods
Image splicing
Image retouching
Image tampering detection
Image quality

ABSTRACT

With the advent of powerful image editing tools, manipulating images and changing their content is becoming a trivial task. Now, you can add, change or delete significant information from an image, without leaving any visible signs of such tampering. With more than several millions pictures uploaded daily to the net, the move towards paperless workplaces, and the introduction of e-Government services everywhere, it is becoming important to develop robust detection methods to identify image tampering operations and validate the credibility of digital images. This led to major research efforts in image forensics for security applications with focus on image forgery detection and authentication. The study of such detection techniques is the main focus of this paper. In particular, we provide a comprehensive survey of different forgery detection techniques, complementing the limitations of existing reviews in the literature. The survey covers image copy-move forgery, splicing, forgery due to resampling, and the newly introduced class of algorithms, namely image retouching. We particularly discuss in detail the class of pixel-based techniques which are the most commonly used approaches, as these do not require any a priori information about the type of tampering. The paper can be seen as a major attempt to provide an up-to-date overview of the research work carried in this all-important field of multimedia.

1. Introduction

In the early 1900s, the Chinese proverb "A picture is worth a thousand words" became very popular among magazine and newspaper editors. The proverb shows the power of a picture in describing complex scenes in a simple and an efficient manner which otherwise may be very hard to express in words. "Seeing is believing" is another popular idiom used to prove that visual clues are more convincing than verbal clues; but this can often lead to misinterpretation as we will see in this paper. We are living in an era of digital revolution which made it very easy to access, process, and share information. Such a technological advance, however, brought with it major security challenges and even an ignition of suspicion of the masses in relying on digital information, especially pictures. With the exponential growth in technology and the powerful algorithms for manipulating images, including software like Photoshop, Corel Draw, and others, it is becoming very difficult to discriminate between an authentic picture and its manipulated or doctored version. The problem is growing by the day with more than several million pictures uploaded daily to the Web. The forgery or tampering of images is becoming indeed a nightmare for individuals as well as for institutions whether political, social, business, or otherwise. The basic concept of image forgery is the digital manipulation of pictures with the aim of distorting some information in these images. The history of image forgery started in 1840 when Hippolyte produced a fake image of himself committing suicide due to frustration for not

* Corresponding author.
E-mail addresses: aliqureshi@kfupm.edu.sa (M.A. Qureshi), mderiche@kfupm.edu.sa (M. Deriche).

http://dx.doi.org/10.1016/j.image.2015.08.008
0923-5965/

Fig. 1. First fake photograph of Hippolyte Bayard committing suicide [1].

getting proper recognition (see Fig. 1). He discovered a new photographic process for manipulating images which was also, independently, introduced by Daguerre and Talbot in 1839 [1].

More recently, we display in Fig. 2 a forged image showing John Kerry (current US Secretary of State) with Jane Fonda (Hollywood actress) speaking to a crowd at an anti-Vietnam peace rally [2]. This photo was manipulated by a hoaxer, during the 2004 American presidential election campaign, to raise a question about John Kerry's patriotism, but, in reality, the event never took place. The original photo of John Kerry (bottom left) was taken by the photographer Ken Light in 1971 at a Peace Rally in Long Island, while the photo of Jane Fonda (bottom right) was taken by Owen Franken in 1972 [2].

The manipulation of images using computer techniques is not new and gained a lot of popularity and even acceptance in diverse areas such as forensic investigation, information technology (IT), intelligence services, medical imaging, journalism, digital cinema, special effects in movies, etc. The move towards paperless workplaces and the introduction of e-Government services meant more data is stored in digital format and more challenges to securing authentic data. Unfortunately, documents, files, voice data, and image data are all vulnerable to manipulation and doctoring. Such a challenge triggered a wide interest among researchers in developing robust techniques for detecting doctored (or forged) images as well as other forms of information [3,4]. This led to substantial research efforts put in the area of image forensics for security applications. Fig. 3 shows the barcharts of year-wise publications since 2002 for different types of image forgery detection methods. The data was collected from Scopus (http://www.scopus.com), using a combination of search keywords for particular classes of image forgery detection (i.e., copy-move, splicing, and retouching). Overall, we notice a major increase in the number of publications focusing on forgery detection. From these charts, we also notice more research efforts put, in recent times, on developing algorithms for retouching detection (see rate of increase in Fig. 3(c)). Retouching is at the heart of current multimedia industry, advertising, TV commercials, etc., and has been used in diverse entertainment applications with sometimes malicious intentions.

1.1. Existing surveys

During the last decade, a number of comprehensive surveys have been published in this all important area of image forgery and forensics. One of the earliest surveys commonly cited in the literature is the paper published by Farid [5], which focused more on multimedia security. The paper was later followed by few other surveys, written by different researchers [6–11]. These surveys focus on different types and aspects of image forgery detection methods and forensics.

Among these, the work presented in [9] provides an extensive review of copy-move forgery detection algorithms. However, the paper does not provide ample discussion on the different feature matching techniques commonly used in the literature. The survey in [7], on the other hand, provides a different approach to forgery detection algorithms. The paper classifies such methods into acquisition-based, coding-based, and editing-based techniques. Image copy-move, splicing, and enhancement detection methods, for instance, were discussed under the editing-based category, and a short review of anti-forensic techniques, that aim to hide the tampering clues, was also provided. While the paper provides an extensive list of references, the paper does not benchmark the different algorithms, nor does it provide a comprehensive comparison of existing approaches. The work, in [8], is yet another survey focusing on image copy-move, splicing, and retouching detection methods. The authors discuss, in some details, the model-based and the transform-based approaches. Both surveys, in [7,8], do not provide enough quantitative/objective comparisons to appreciate the differences among the presented techniques. The most recent survey, discussed in [10], provides an extensive review of existing techniques with a number of comparison summarized through tables and charts. However, given the nature of the publication, little emphasis was given to the main ideas and the underlying models.

Given the fast growth witnessed in this all important area of research, we are presenting this comprehensive review of different image tampering detection techniques complementing the limitations of existing reviews in the literature; many of which were discussed above. We have selected the forgery detection methods which are based on pixels, and categorized these into: copy-move, splicing, resampling, and retouching algorithms. We discuss and summarize the different classes of algorithms based on the type of features used, their strengths and weaknesses, along with their suitability for different applications. A brief comparison is also provided for different types of feature-matching methods used in copy-move forgery detection. We also provide in this paper a summary of different datasets available, which are used for performance evaluation and for benchmarking different forensics tools. Finally, the paper presents a detailed description (in terms of used features, classification and detection accuracy) of different image copy-move, splicing, and post-processing detection methods tested on different datasets. At the outset of the paper, we also discuss the different concepts and techniques used in anti-forensics and in

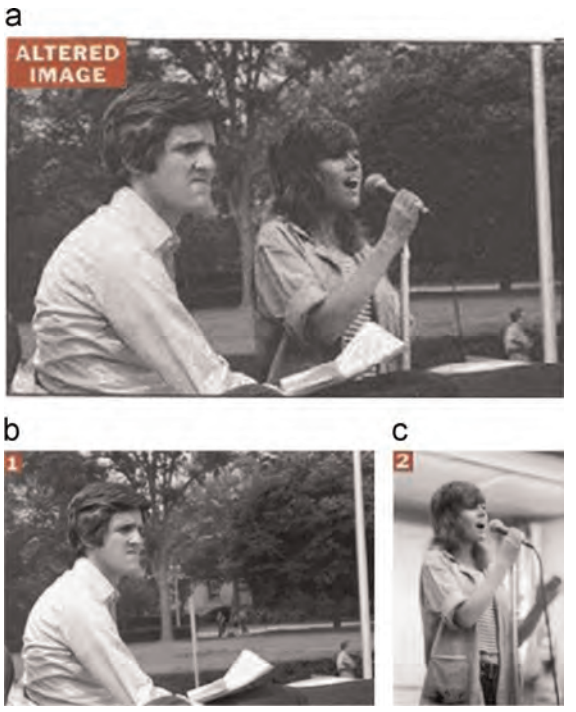

Fig. 2. (a) Tampered image of Ex-U.S. presidential election candidate John Kerry and actress Jane Fonda. (b) Original image of John Kerry prepares to speak about war in Vietnam. (c) Original image of actress Jane Fonda speaks to a group of Vietnam veterans [2].

countering anti-forensics; these two areas have recently attracted a lot of attention amongst the research community. We have tried our utmost to review the latest contributions in this area, specially those published during the last three years. This review can be seen as a major attempt to provide a complete and comprehensive overview of the work carried in this all important field of image forensics and can assist researchers in focusing on the most challenging aspect of image forgery detection.

The paper is organized as follows: Section 2 provides a brief introduction to different types of image forgery commonly found in the literature. Section 3 describes the different classes of forgery detection techniques with their advantages and disadvantages. We then provide a comprehensive survey of pixel-based forgery detection techniques in Section 4. Finally, we conclude the paper with the discussion on the challenges faced in this all important area of multimedia.

2. Types of digital image forgery

Image tampering is defined as adding, deleting and/or changing some important regions from an image with no discernible footprints [1]. There have been various methods used for forging or tampering an image. Digital image forgery can be categorized into Image retouching, Copy-Move forgery, and Image splicing depending upon the type of techniques used to create the tampered images. A brief discussion of these types is given below:

2.1. *Image retouching*

Image retouching is a common technique used in the media industry. It is seen as an acceptable and sometimes a desirable method for manipulating photos. It does not result in any significant change in an image rather it emphasizes (or reduces) some desirable (or undesirable) features of the image (see Fig. 4). It is a popular technique used with magazine photos and in movies. The image is enhanced to make it more attractive and sometimes some regions are transformed (such as removing wrinkles) to obtain the final photo, while such type of manipulation is not seen as forging, we include it here as it involves tampering the original image [12].

2.2. *Copy-move forgery*

Copy-move forgery (or cloning) involves copy and paste operations of image parts to another location in the same image to hide some important information or to duplicate image portions as shown in Fig. 5. Since the copied part came from the same image, there is no significant visible change in image texture properties like color, noise, and texture and leads to tamper detection a challenging task [15,227].

2.3. *Image forgery using splicing*

In image splicing, different image parts from one or more images are used to create a new tampered (or spliced) image. It requires some postprocessing operations on the spliced regions to make the surrounding boundaries visually imperceptible. Splicing, however, disturbs the high order Fourier statistics such as the bispectrum; these statistics can subsequently be used in detecting forgery. Image splicing detection requires the analysis of the whole image content using robust statistical methods [17].

To make the forgery imperceptible, some selected regions have to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping, etc. The interpolation step plays a central role in the resampling process and introduces non-negligible statistical changes. In resampling, specific periodic correlations are introduced in the image pixels and can be measured for forgery detection. Fig. 6 shows a nice example of image splicing in which the top left and center images are the original scenes while the one on the right is the tampered image obtained by merging the two images.

3. Digital image forensics tools

Given the advanced algorithms used in image tampering, determining the credibility and integrity of digital images is becoming a real challenge to the naked eyes as well as to machines. Therefore, it is very important to develop robust detection methods to identify tampering operations and validate the authenticity of digital images. Present digital image forensic approaches are commonly categorized into active and passive (blind) techniques. Active methods involve embedding of a digital signature or

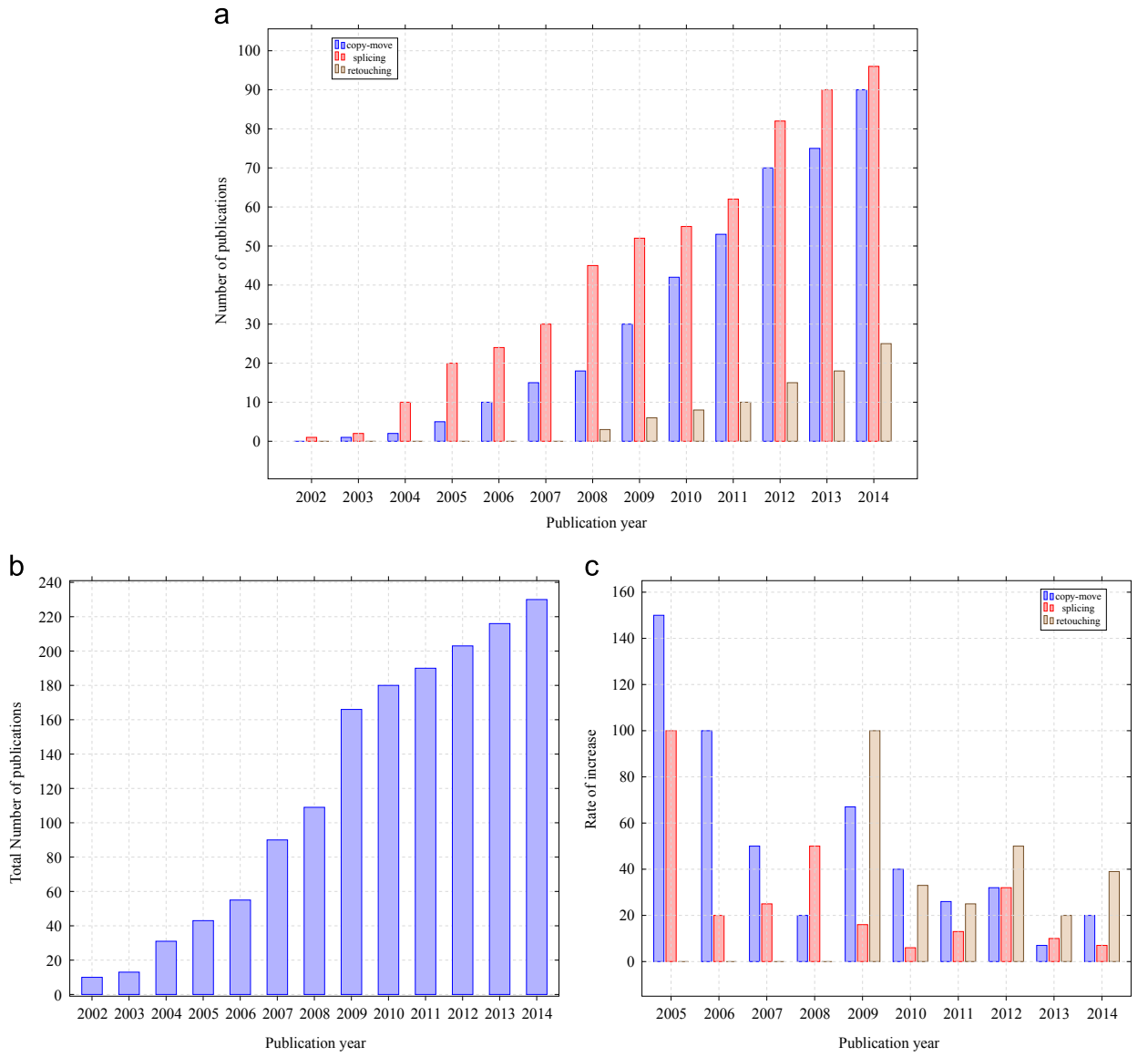

Fig. 3. Total number of year-wise publications since 2002. The data is obtained from Scopus (http://www.scopus.com): (a) publications per class, (b) total number of publications, (c) rate of increase in publications (in %).

a digital watermark inside the original image which can later be used to prove or reject the authenticity of the image [20–23]. However, these methods have strong limitations in a sense that the watermark must be embedded either by the acquisition device (camera) or by an authorized person processing the image, which is an impractical approach due to the unavailability of watermarking capabilities in most image acquisition devices. Moreover, the image quality, itself, can be degraded during the watermarking process. In passive or blind approaches, the source image is not available. They are based on the fact that although the tampering is visually imperceptible, the tampering operations introduce new artifacts due to the change in fundamental statistical properties of a digital image. The inconsistencies resulting from these artifacts can further be used for tampering detection. An image can undergo different forms of attacks during the tampering process. Among these attacks, the simplest one is the copy-move, in which the part of the image is duplicated within the same image. The image parts can also be copied from other images (image splicing) and the image itself or the tampered regions can other different types of transformations to make the tampering invisible. The forensics tools focus mainly on detecting the tampering by exploiting various properties of image tampering process.

In this work, and in consistency with the work discussed earlier by Farid [5], we also opted to group the different blind image forgery detection approaches under five major categories i.e., pixel-based, compression-based, camera-based, physics-based, and geometric-based techniques [5]. Fig. 7 shows the tree diagram of different approaches used under

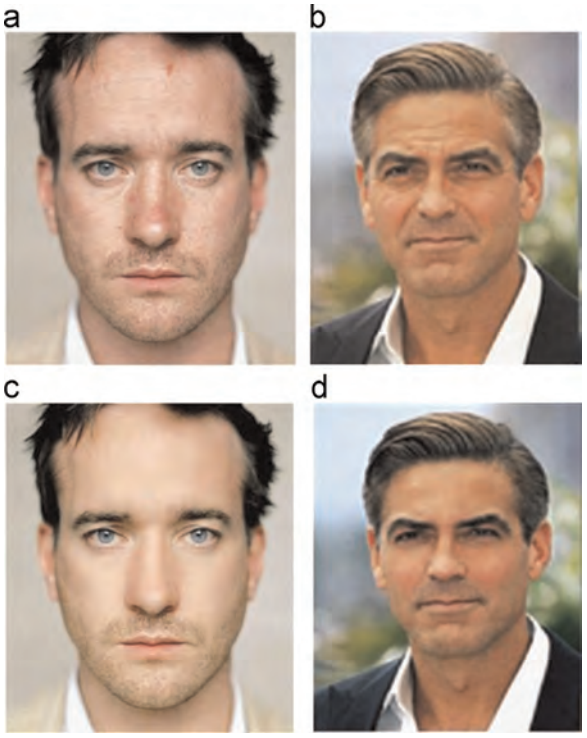

Fig. 4. Examples of photo retouching [before (top) and after (bottom)] [13,14].

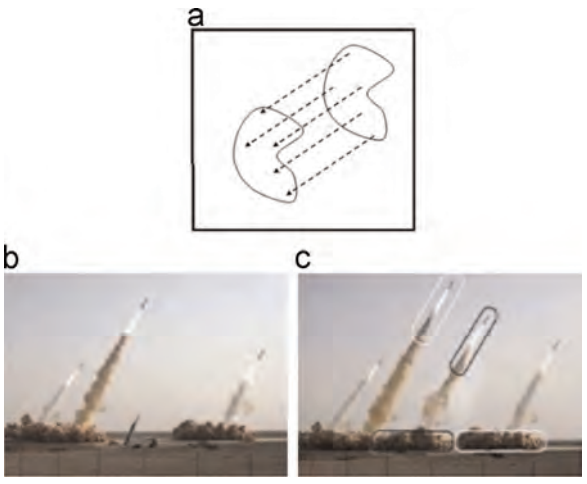

Fig. 5. An example of copy-move forgery (a) copymove tampering process, (b) original image with 3 missiles, (c) forged image with 4 missiles [16].

each of the five categories. A brief description of each of these groups is now discussed.

3.1. Pixel-based techniques

These techniques are based on detecting the statistical irregularities occurred in image pixels during the tampering process. These techniques also analyze correlations among pixels introduced due to the specific form of tampering in a spatial domain or a transformed domain. These techniques are commonly found in practice. More details on this class of approaches are provided in Section 4.

3.2. Compression-based techniques

The transformation of a forged image for the purpose of compression and other applications can make forgery detection a very challenging task. JPEG image compression, for example, is shown to make forgery detection very difficult. However, in forensics analysis, some properties of JPEG compression are exploited to identify the traces left by tampering. These techniques can themselves be grouped into JPEG quantization based [24], double JPEG compression based [25–27], multiple JPEG compression based [28,29], and JPEG blocking based [30].

3.3. Camera-based techniques

The image acquisition process in a digital camera system involves different processing stages. First, the light enters the camera lens then passes to the sensors through Color Filter Array (CFA). The sensor contains an array of photodetectors that capture incident light and convert it into voltages followed by the Analog-to-Digital (A/D) conversion stage. Today digital cameras rely mainly on Complementary Metal-Oxide Semiconductor (CMOS) technology with few manufacturers still using the traditional Charged Coupled Device (CCD) technology. To capture color images from these sensors, CFA is used. The sensors capture only one color and the remaining colors are estimated using interpolations (demosaicing). The correlations introduced in the interpolation step can be used in tampering detection. Before the final storage, the image quality is improved using various enhancement techniques like Gamma correction and white balance. The artifacts introduced in the different stages of the image creation process are exploited to detect traces of tampering. Chromatic aberration [31], source camera identification [32,33], color filter array, demosaicing artifacts [34], and sensor noise [35] imperfections can help in estimation of different camera artifacts. The tampering can be detected by considering the inconsistencies in these different types of artifacts [36].

3.4. Physics-based techniques

Natural photographs are usually taken under different lighting conditions. Thus, the lighting of a forged region may not match the original in splicing operations (where two or more images are used to create a forged image). In physics-based techniques, the inconsistencies in light source between specific objects in the scene are used to reveal the traces of tampering [37–39]. Johnson et al. [38] proposed a tampering detection method that uses the direction of incident light and computed a low-dimensional descriptor of the lighting environment in the image plane. The algorithm estimates the illumination direction from the intensity distribution along manually annotated object boundaries of homogeneous color. Kee et al. [39] extended this approach to exploiting known 3-D surface geometry.

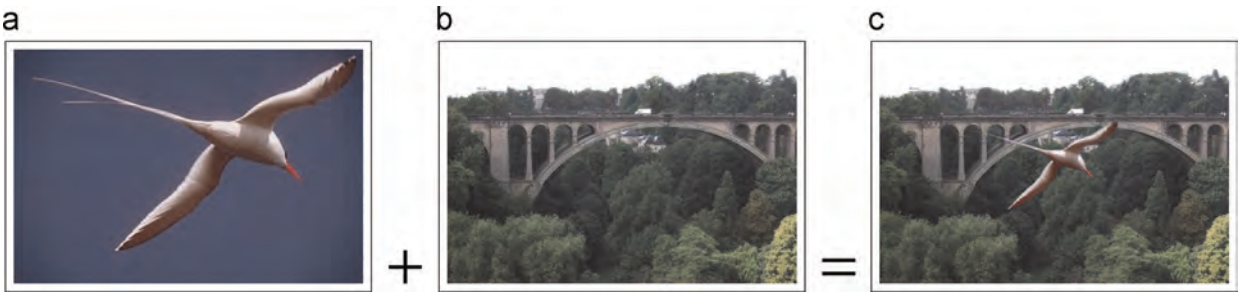

Fig. 6. An example of image splicing [18,19].

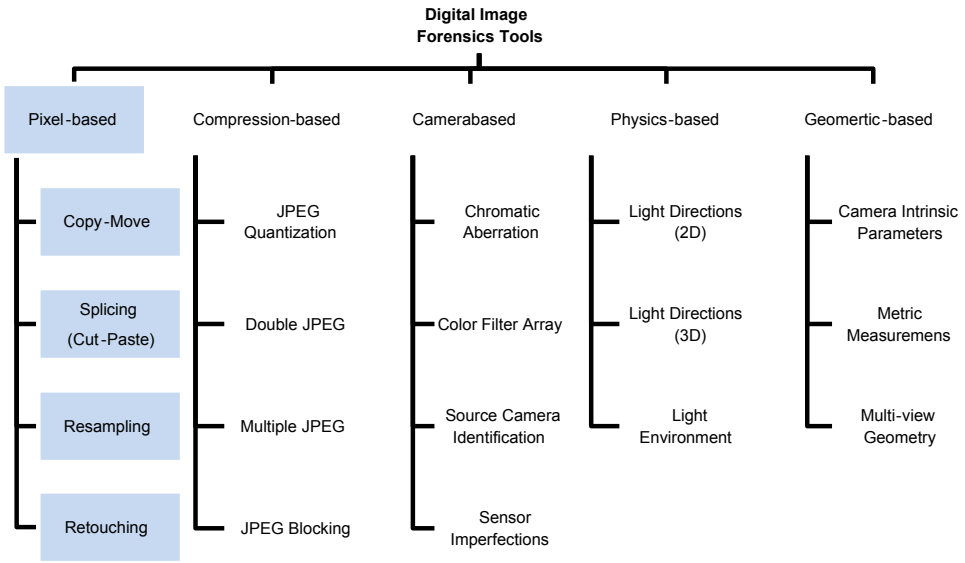

Fig. 7. Tree structure of different approaches used in blind image forensics [5].

3.5. *Geometric-based techniques*

The geometric-based forgery detection techniques use geometric constraints under perspective views. These techniques are further grouped into camera's intrinsic parameters based (like focal length, principal point, aspect ratio, and skew) [40], metric measurement based [41], and multiple view geometry based [42]. For example, in authentic images, the principal point (the intersection of the optical axis and the image plane) is located near to the center of the image. When a small region is moved or translated in the image (copy-move example), or two or more images are combined together (splicing example), it becomes difficult to keep the images principal point in its correct perspective. Thus, by applying projective geometry principles, robust forgery detection algorithms can be developed [40].

The multitude of approaches discussed above show that the forgery detection is a multidimensional problem. Depending upon the particular forgery attack a given image is subjected to; some detection techniques can provide excellent results while others can be completely useless. Among these approaches, the most common and practical ones are the pixel-based techniques. This class of techniques does not require any prior information about geometrical transformations, nor does it require information about the image acquisition process. Our analysis showed that a high percentage of papers published in recent years have focused on pixel-based image forgery detection techniques. For example, in [8], around 70% of the references, and in the survey [10], more than 60% of the references were related to pixel-based detection techniques. For this reason, we chose to focus in this paper on providing a comprehensive survey of forgery detection techniques which only use pixel information. In what follows, we will discuss in detail, the different approaches for forgery detection using pixel-based detection techniques and provide an insight into their advantages and disadvantages.

4. Pixel based image forgery detection methods

Traditionally, digital image processing algorithms have focused on manipulating information or content at the pixel level. Similarly, pixel based blind forgery detection techniques have been the most widely used techniques especially when we know that the simplest and most commonly used approaches to forgery are also pixel based. Such techniques are based on the analysis of inter-pixel

correlations that arise from tampering, either directly or indirectly. As mentioned in the Introduction, the most common pixel-based forgery detection approaches are Copy-move, Image splicing, Resampling, and finally Retouching detection. For the sake of completeness, we have also added a Section 4.5 on generic image processing tools to detect post-processing manipulations in pixel-based image forensics. The different classes are now discussed in more details.

4.1. Copy-move forgery detection techniques

The different parts are copied and/or moved to the same image in copy-move forgery, hence strong correlation exists between these which can be used as an evidence for forgery detection. But the main challenge is to find efficient features and matching algorithms for finding correlated segments. In these methods, first, characteristic features are calculated either by dividing the image into overlapping blocks or calculating local keypoints for the whole image. The positions of each block (or keypoint) are also stored in the feature vector. Then, the feature matching is performed to find similar features within the same image. The forgery localization is done by displaying the matched blocks (or keypoints) in colors corresponding to the locations of the matched features.

One of the earliest copy-move forgery detection algorithms is proposed by Fridrich et al. [15], based on dividing the image into fixed size overlapping blocks and stored as 1-D feature vector. A constraint was made in relation to the choice of block size, as it should be less than the size of maximum copy move block segment. Next, a shift vector approach was employed for feature matching and the blocks with the same shift were declared as tampered regions. This general framework is common among most copy-move forgery detection techniques and the main steps are described as follows:

- A tampered image of size $M \times N$ is first converted into gray-scale (except for the algorithms which require color channels).
- In Block-based detection methods, the image is partitioned into fixed size overlapping blocks with dimensions $b \times b$ resulting into $N_b = (M - b + 1) \times (N - b + 1)$ blocks. The features from each block are computed and stored as a row vector $\boldsymbol{f_i}$ of size $1 \times K$.
  In Keypoint-based methods, the image is scanned for keypoints, and the feature vector $\boldsymbol{f_i}$ is calculated for every keypoint.
  Upper left coordinates (x_i, y_i) of each block (or keypoint) are also stored in $\boldsymbol{f_i}$ for further use. The size of $\boldsymbol{f_i}$ now becomes $1 \times (K + 2)$. The feature vector $\boldsymbol{f_i}$ corresponding to block (or keypoint) is stored in a feature matrix $\mathbf{F}$ of size $N_b \times (K + 2)$.
- Following the above, the rows of the feature matrix $\mathbf{F}$ are sorted. This brings the features of similar blocks (or keypoints) close to one other. Matching feature vector pairs are searched among the nearest neighbors using a threshold. Denoting F_{ij} to be the matched pair consisting of features $\boldsymbol{f_i}$, $\boldsymbol{f_j}$, where $i \neq j$ represent feature indices, the shift vector $\boldsymbol{s}$ between the two matched blocks is obtained as

$$\mathbf{s}_{ij}(dx, dy) = (x_i - x_j, y_i - y_j) \tag{1}$$

- A counter, $\mathbf{C}(\mathbf{s})$, is obtained (and incremented by one) for each matched block pair with the same shift using Eq. (2):

$$\mathbf{C}(dx, dy) = \mathbf{C}(dx, dy) + 1 \tag{2}$$

- For the duplicated regions, the blocks (or keypoints) always exhibit same shift and hence grouped together. The groups of blocks (or keypoint) with shift vector count below a certain threshold T_1 are discarded, whereas T_1 controls the size of smallest detectable copy-move segment.
- In the final post-processing step, morphological operations are performed to minimize false positives. The

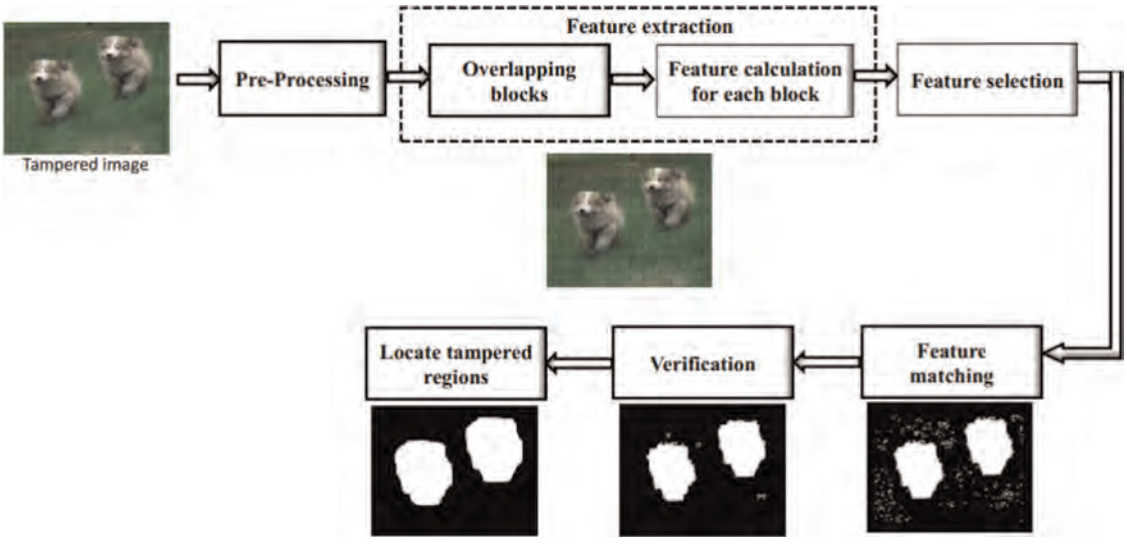

Fig. 8. Block diagram for a typical copy-move forgery detection algorithm [43].

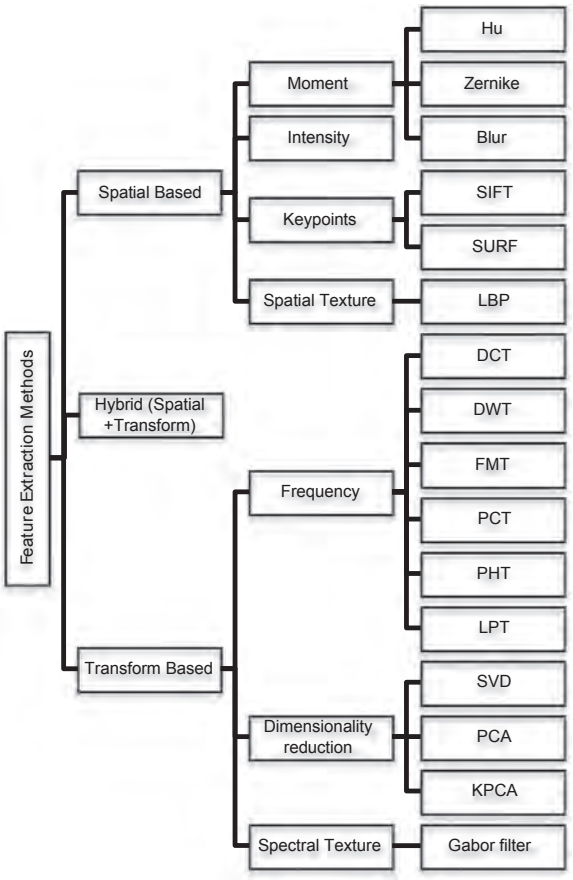

Fig. 9. Classifications of feature extraction methods for copy-move forgery detection techniques.

matched blocks (or keypoints) with the same shift vector are shown with the same color to differentiate different copy-move segments. Fig. 8 shows the block diagram of different steps involved in copy-move forgery detection techniques.

Inspiring from the above, there have been numerous approaches proposed to improve detection performance. All the work following [15] differ only in terms of the features used for the forgery detection process. Here, we propose to classify these algorithms into two broad categories: Spatial, Transform based techniques. A summary of different features used in copy-move forgery detection algorithms is displayed in Fig. 9. The details of different features and their properties are discussed next.

4.1.1. *Spatial domain methods*

In spatial domain, the pixel location directly describes the content in an image. The energy in spatial domain is generally uniformly distributed and neighboring pixels are highly correlated. This makes the matching process highly computational. The copy-move forgery detection techniques in spatial domain can either be based on moments, intensity, keypoints, or texture based features.

Moment-based methods: Under this class of moments, copy-move forgery is detected by calculating Hu, Blur-invariant, Zernike moments, among others. In [44], Mahdian et al. used 24 features based on blur-invariant moments. Their experiments demonstrated the effectiveness of blur-invariant moments in different post-processing operations i.e., blurring, contrast change, and noise addition on duplicated regions. In [45], Wang et al. proposed Hu's moments as features and demonstrated robustness to post-processing operations including rotation, scaling, and translation in the region duplication process. The first 4 moments were used as features to decrease the computational complexity. In [46], Liu et al. computed Hu moments from circular blocks instead of square blocks and used as features, which were found more efficient. However, features are redundant due to non-orthogonal nature of Hu moments as well as sensitive to noise. In [47], Ryu et al. used Zernike moments based features extracted from circular blocks for duplicate regions detection in tampered images. Further improvements in block matching based techniques were achieved by the same authors in [48] by using the phase of Zernike moments in the feature space error-reduction procedure. The Zernike moments are orthogonal, robust to noise, compression, blurring, and most importantly rotation invariant. They are efficient in detecting copy-move blocks for flat regions but fail in detecting scaled copy-move blocks. Due to their orthogonality property, the contribution of each moment is unique and independent of others. The major drawback of all moments based techniques is their high computational cost. Other moment based techniques such as Laws moments [49] have also been used with different degree of success.

Intensity-based methods: Among different intensity based copy-move forgery detection methods, Luo et al. [50] extracted features from non-overlapping blocks for color images. The mean values of red, green and blue channel of each block were used as features. Additional features were computed by horizontal, vertical, and diagonal splitting of each block into two parts. The average ratio of the luminance component from one part over the block average intensities was also used as features and stored as 7-D feature vector, and the feature matching was performed using Lexicographical sorting. The experiments showed noise insensitivity of the features. Similar to [50], in [51,52], image blocks were divided into different directional sub-blocks, and energy features were calculated from these sub-blocks. These methods work with both color and gray scale images. However, all of these approaches assumed no post-processing (e.g., scaling, rotation, and JPEG compression) on the copied regions.

To handle the post-processing in the tampering process, Wang et al. [50] used circular blocks instead of square blocks for feature extraction. The mean values of the image pixels in concentric circles of different radii were used as features. These features were proved to be robust against rotation in duplicated regions. The performance was evaluated in terms of accuracy and computational efficiency. The rotation invariant property of the above-mentioned features was also demonstrated in [53]. In [54,55], Solorio proposed an algorithm for reflection and rotation invariant copy-move forgery detection. The features were calculated from log-polar transformations of pixels in overlapping image blocks.

Keypoint-based methods: These methods operate on entire image focusing with high entropy regions. Lowe et al. [56] proposed Scale Invariant Feature Transform (SIFT) for feature matching between two images. In SIFT, 128-D feature descriptor is computed for every keypoint. Since, SIFT features are extracted only for keypoints hence increasing computational efficiency. They are invariant to scaling, rotation, and illumination variations that is why are strong aspirant for image forgery localization. Huang et al. [57] first used the SIFT keypoints based local features for finding matched regions within the same image. This concept was later exploited by Amerini et al. [58,59] and Pan et al. [60,61] for geometric tampering estimation using the Random Sample Consensus (RANSAC) algorithm [62]. RANSAC is a very popular robust homography estimation algorithm. It selects 4 points at random and computes a homography matrix **H**. Then, it classifies the remaining points as inliers or outliers depending on their concurrence in **H**. This procedure is repeated iteratively for selected number of iterations and finally, the candidate keypoints are selected from the iteration with the largest number of inliers. In [58,59], G2NN (Generalized 2 Nearest Neighbor) method was used for feature matching followed by feature clustering for tampering localization. While in [60,61], Best-Bin-First (BBF) search algorithm was used for keypoint matching. Further extensions were made by clustering keypoints using J-linkage for better estimation of geometric transformations and multiple cloning detection [63].

These methods were shown to detect multiple duplications with less computational complexity and minimum memory requirements. Jeberi et al. [64] used Mirror reflection Invariant Feature Transform (MIFT) features. Their experiments demonstrated robust localization of copy-move forgery compared to other SIFT based methods. Like SIFT, MIFT features are also invariant to rotation, scaling, and illumination changes. Contrary to SIFT, MIFT features are reflection invariant.

The other keypoint based method is the Speed Up Reduced Features (SURF) using 64-D feature descriptor instead of 128-D for each keypoint. The SURF features are easy to compute as compared to the SIFT. They were used in [65–67] to detect copy-move forgery. Keypoint based methods are computationally efficient as compared to moment based methods. But unfortunately lagging in detecting duplicate regions with smooth background.

Texture-based methods: The human visual system uses mainly texture for image interpretation that can broadly be classified into spatial texture features and spectral texture features. In spatial domain, texture features are extracted using the pixel statistics. They are calculated from any shape and are generally sensitive to noise. In [68], Ardizzone et al. used statistical texture features such as mean, standard deviation, skewness, and kurtosis for copy-move forgery detection in digital images. These features were shown to be simple and robust against JPEG compression, but failed to detect image blocks undergone transformation during the forgery operation. To handle the geometrical transformations in post-processing operations, Li et al. [43] used texture features based on Local Binary Patterns (LBP). In the preprocessing stage, the image was first lowpass filtered and then divided into overlapping circular blocks and finally, rotation invariant uniform LBP was used for feature extraction. The LBP based features were shown to be robust against rotation, flipping, noise contamination, JPEG compression, and blurring as well.

4.1.2. Transform based methods

In transform domain, the coefficients present usually lesser correlation and only few coefficients carry most of the energy, which means that only few coefficients can be used as features for each overlapping block. Transform domain methods can be divided into either frequency based, texture based, or reduced dimension based techniques.

Frequency-based methods: In [15], Fridrich et al. proposed a block-based approach using 256 quantized DCT coefficients as features. Its improved version was proposed by Huang et al. [69] using only 25% low energy DCT coefficients computed for each block. In these methods, the same regions were made close to each other by lexicographical sorting of feature vectors (the coefficients of DCT blocks) and matching was performed using shift vectors. The features based on the DCT coefficients are robust to noise, compression, and retouching but are not good in detecting rotated or scaled copied blocks. The Discrete Wavelet Transform (DWT) was also used for copy-move forgery detection. The DWT coefficients using Haar wavelets were extracted [70,71] while Bayram et al. [72] used the Fourier–Mellin Transform (FMT) to calculate 45 block-based features which where shown to be scale and translation invariant as well as robust to blurring, compression, and noise. But they were not fully rotation invariant as well as the computational time was also high. The matching time was reduced using the counting bloom filter instead of lexicographical sorting. In [73], Mohammad et al. proposed to use the approximation and detail sub-bands of the discrete dyadic undecimated wavelet transform (DyWT). The wavelet subbands were partitioned into overlapping blocks with 50% overlap, and the coefficients from subband blocks were used as features. The similarity between the coefficients from approximation blocks and dissimilarity between the coefficients of detail blocks were used for copy-move detection. The approach was shown to be robust against rotation and JPEG compression post-processing operations on the copied regions with less false positive rate. In [74], Li et al. extracted features from circular blocks using the Polar Harmonic Transform (PHT) while in [75], Li used the Polar Cosine Transform (PCT) to extract features from square blocks. The features calculated from PHT and PCT are orthogonal, rotation-invariant and computationally efficient. There is no numerical stability issue with these transforms, as with the Zernike moments. The rotation and scale invariant features using the Log-Polar transform (LPT) were also proposed in [76,77]. The rotation and scaling is represented by translations in log-polar image. This geometric property, also known as edge or shape invariance, results in features which are rotation and scale invariant. The translations are mapped to a complex

transformation in the log-polar domain. Another advantage of using LPT is its low computational complexity.

Dimensionality reduction-based methods: In [78], Popescu and Farid used Principal Component Analysis (PCA) on small size image blocks to obtain reduced dimension feature vectors which were shown to speed up the feature matching process. PCA projects the data along the direction of maximum variance and so the eigenvectors corresponding to the largest eigenvalues are used as principal components. Features from PCA are robust to additive noise and lossy compression but not appropriate for detecting rotation or scaling transformations. A more advanced approach, Kernel-PCA (KPCA), was also discussed by Hulmukhe et al. [79], to detect "rotation" and "flip" duplications. For detecting "scaled" copy-move blocks, Bashar et al. [80] extracted features from phase correlation in the log-polar domain and KPCA was applied for dimensionality reduction. In [81], Kang et al. proposed to use Singular Value Decomposition (SVD), to extract algebraic and geometric invariant features. In [82], Ting et al. used KD-trees for matching SVD features. The results showed the robustness of this approach against blurring, geometric transformations, and noise. But both KPCA and SVD are computationally inefficient compared to the linear PCA. While the above approaches are useful in representing 2nd order statistics, forgery based on manipulating high-order statistics may not be accurately detected.

Spectral texture-based methods: Texture features can also be calculated from the transform domain image. These are robust and require less computations. But they are limited for mainly square image blocks. In [83], Hsu et al. used the Gabor filter for copy-move image forgery detection due to its optimal localization properties in spatial and frequency domains. The Gabor features with different scales, orientations, and frequencies were calculated for image blocks. These features were shown to be robust against JPEG compression and provided accurate estimation of rotation angle and scaling factor in tampered blocks. In [84], Gharibi et al. reduced the Gabor features dimension using PCA while lexicographical sorting was used to detect duplicated blocks. The proposed technique was shown to be robust against JPEG compression but was not tested on scaled or rotated tampered blocks.

4.1.3. Hybrid methods

To enhance the performance of copy-move forgery detection algorithms, many techniques based on combining two or more techniques have also been proposed. In [85], a phase correlation based technique was discussed using the approximation component of the DWT. The method was shown to be robust against compression, however, scaling and rotation were not discussed. In [86] Zimba et al. used DWT with PCA to reduce the dimension of the feature space. The overlapping blocks were compared using lexicographical sorting. In [87], Li et al. used DWT with SVD for reduced feature dimensions. These features were calculated using the approximation subband coefficients for block based DWT. In [88], SIFT features were reduced using PCA while in [89], the DCT was combined with the DWT for feature calculation.

SIFT features are invariant against rotation and scaling but fail for flat regions, while Zernike moments are invariant against rotation and robust to noise, but scale variant. In [90], a combination of these two methods was used to increase robustness and efficiency. Similarly, in [91], the Zernike moments were used with the undecimated wavelet transform using the scaling and translational invariant properties of the DWT for calculating features invariant to rotation, scaling, and translation. Several other hybrid approaches have also been proposed.

It is worth noting that the major problem with copy-move forgery is the detection of duplicated image regions affected by common post-processing operations, e.g., scaling, rotation, flipping, noise addition, compression, etc. The other challenge is the computational load which can be excessive. Among the algorithms discussed above, keypoint based methods like SIFT can be considered effective in detecting duplicate regions even when the regions undergo transformations like scaling and rotation, and they are also robust to noise and changes in illumination conditions. SIFT has some limitations in dealing with flat duplicate regions. Block based features like Zernike moments are effective in detecting copy-move blocks even for the flat regions but these are not good in detecting scaled copied blocks. Block matching methods using square blocks are not suitable for detection of rotated or scaled duplicated blocks. However, using circular blocks instead of rectangular blocks can significantly make the detection invariant against rotation. Consequently, to improve the performance of detection algorithms, we have witnessed a growing interest in developing hybrid or combined techniques using more than one approach, in detecting copy-move forgery. Finally, we will briefly discuss the stage of matching after the features have been computed in copy-move detection techniques, since this stage is also important in the overall accuracy of the detection process.

4.1.4. Feature matching methods

Once features have been extracted for each image block (or keypoints) from the whole image, a comparison is performed to match features from different blocks (or keypoints) with one another. The main issue is how to qualify similarities among features. The most straightforward approach is an exhaustive search where each feature vector is compared with the others. This approach is computationally inefficient with a time complexity of $O(MN)$ for an image of size $M \times N$. Besides this, it does not work for detecting blocks that have undergone some modifications.

To speed up the feature matching process, lexicographical sorting [15] was used. In lexicographical sorting, feature vectors from image blocks or keypoints are stored as rows in a matrix. Then, this matrix is sorted row-wise which results in similar feature vectors close to one other. The matching speed is increased by comparing every row with its closest neighbor. The time complexity of lexicographical sorting depends on the number of blocks (or keypoints) and number of features in each block (or keypoint). It was first used by Fridrich et al. [15] for finding matching blocks. Later, lexicographical sorting was used in

[45,47,50,51,54,72,78,81,80,85,92] for feature matching. It has a computational complexity of $O(N_f \times N_b \times \log N_b)$. Lexicographic sorting is not a suitable feature matching algorithm when geometric transformations are applied to copied regions. Table 1 shows the feature dimensions of different block-based copy-move forgery detection techniques when lexicographical sorting is used for feature matching.

The time complexity of lexicographical sorting was further improved by Lin et al. [51]. The row-wise feature vectors were sorted using radix sort algorithm. Although, the time complexity was reduced, but the main disadvantage of using radix sorting is that it works only for integer type features.

To improve the efficiency of the matching stage, KD-trees have also been used [44,94,95]. The data is pre-processed into a structure allowing efficient nearest neighbor search. Like binary tree, points in a k-dimensional space are stored in KD-trees as the leaves. For similarity measure, the Euclidean distance is used and for N records, we require $O(N\log_2 N)$ operations. The feature matching performance is better than lexicographical sorting but with relatively larger memory requirements. Its complexity depends on the distribution of similar intensity blocks. It was first used by Langille et al. [95], to search for the similar blocks in images. Instead of Euclidean distance, Zero Normalized Correlation Coefficient (ZNCC) was used for similarity matching.

In [72], the counting bloom filter was used for finding the matching blocks. It computes hashes for feature vectors and concludes that two feature vectors match completely when their hashes are equal. The sorting of feature vectors is avoided and hence, it reduces the time complexity. However, it is very difficult to compute an effective hash.

Table 1
The feature dimensions of different block-based copy-move tampering detection methods.

Method	Feature type	N_f [b]	N_b [a]
Fridrich et al. [15]	DCT	64	255 025
Popescu et al. [78]	PCA	32	255 025
Li et al. [87]	DWT & SVD	8	62 201
Luo et al. [50]	Color	7	255 025
Wen et al. [93]	DWT (appx.band)	3	62 201
Wang et al. [92]	Low freq. part	4	62 201
Huang et al. [69]	Truncated DCT	16	255 025

[a] N_b, number of overlapping blocks $=(M-b+1)\times(N-b+1)$ where b = block size = 8. M, N = image dimensions = 512×512.
[b] N_f, number of features for each block.

Barnes et al. [96] developed a randomized approach for the detection of similar blocks in an image using the PatchMatch algorithm, which was initially proposed in [97]. The PatchMatch algorithm is based on an iterative randomized nearest-neighbor search and has fast convergence rate. The results of [96] were only shown for the detection of simple cloning. Recently, Cozzolino et al. [98] proposed a fast copy-move forgery detection algorithm based on a modified form of the PatchMatch algorithm, for rotation-invariant and scale-invariant forgery detection. The Zernike moments were used as features. The algorithm showed good performance in terms of computational complexity and detection accuracy.

To avoid feature matching of blocks belonging to the same area i.e. (sea or grass), a block clustering approach was proposed in [99]. The block matching was performed in the coarse scales followed by the fine scales. The idea was to group similar blocks into clusters and features for the blocks with each cluster were compared.

In keypoint based methods, feature matching is performed by 2NN, $G2$NN and Best-Bin-first (BBF) search algorithms to get the nearest neighbors [44,57–61]. The BBF search algorithm is a KD-tree variant and is used to find an approximate solution to the nearest neighbor problem in a very-high-dimensional space in lesser time. In 2NN feature matching, for every keypoint, the Euclidian distance between features is computed with the other keypoints. Due to high dimensionality of feature space for keypoints, it is not optimum to compare the difference of distances with a global threshold. Instead 2NN (2 Nearest Neighbors) test is used where for every keypoint, the ratio of the distance of first most similar keypoint with the distance of the second similar keypoint (i.e. $\frac{d_1}{d_2}$) is computed. The keypoint is considered as a matched one if the ratio is smaller than $T_1 \in 0, 1$ (usually $T_1 = 0.5$) but it fails to detect multiple duplications in the same image. To detect multiple duplications, generalized 2NN (i.e., $G2$ NN) was proposed [59]. In $G2$ NN, for every keypoint, its Euclidean distance with the other keypoints is calculated and stored in ascending order as 1D vector say ($d_1, d_2, \ldots, d_{n-1}$). The 2NN test is performed iteratively until the ratio $\frac{d_i}{d_{i+1}} > T_2$, for $i = 1, 2, \ldots, k$ where $1 < k < n$. All the points until k are considered as matched. The same procedure is repeated for all the keypoints. The keypoints which are not matched are discarded and the remaining are clustered for multiple duplication localizations.

Since keypoint based methods are based on the high entropy points, they fail in the smooth regions while the block-based methods can work but with a single threshold in the matching stage, they result in many false matches. To overcome the problem of false matches in smooth regions, Zandi et al. in [100] proposed the use of an

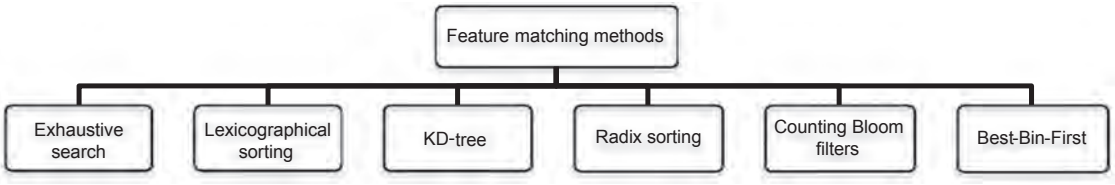

Fig. 10. Different types of feature matching methods used for copy-move forgery detection.

adaptive similarity threshold in the block-based feature matching stage. The similarity of pair of blocks was determined using thresholds proportional to their standard deviations.

Fig. 10 shows the different feature matching algorithms used for copy move forgery detection and their computational complexity is shown in Table 2.

4.2. Image splicing detection techniques

While the majority of research work published on image forensics focused on developing robust algorithms for detecting tampering operations, it is sometimes more important to detect which parts of a given image have been manipulated. For this reason, we note here that researchers working in forensics imaging have either adopted the classification perspective or the localization perspective. The task of image splicing detection among authentic and forged images is an example of binary classification. Fig. 11 shows the workflow for a typical image splicing detection technique. It starts with the pre-processing stage which is usually the color to gray-scale conversion followed by the feature extraction stage. Different types of features are extracted from authentic and tampered images for a given dataset. The feature extraction stage is critical and the classification performance depends on the selection of best features for the problem under investigation. The extracted features are used to train a classifier and the trained model is used to classify the authentic and tampered images. Finally, in the post-processing stage, the tampered regions are localized.

Table 2
Time complexity of different feature matching methods.

Feature matching method	Time complexity
Exhaustive search	$O(MN)$
Lexicographical sort	$O(N_f \times N_b \times \log N_b)$
Radix sort	$O(N_f \times N_b)$
Counting bloom filters	$O(length(MN))$
KD-tree	$O(N\log_2 N)$

Image splicing relies on cut-and-paste techniques from one or more images to produce a new fake image. In 1999, Farid [17] used bicoherence (normalized bispectrum) based features to catch unnatural high order correlations in speech which was utilized to detect audio tampering. Motivated from his work, Ng and Chang [101] used both magnitude and phase of the bicoherence spectrum. The method was tested on the Columbia Image Splicing Detection Evaluation (CISDE) dataset [102] with a reported detection accuracy of 63%. By incorporating features using edge pixel percentage, the performance was further improved to 72% by the same authors [103]. In [104], Hilbert–Huang Transform (HHT) based features were used to exploit the non-stationarity and non-linearity nature of the image splicing operation. The HHT was used for representing the time-varying process. In addition, moments of the characteristic functions were calculated for different wavelet sub-bands and used as features. There was significant improvement in detection accuracy from 72% to 80%, from the work in [103], using the same classifier and dataset. Li et al. [105] combined features from the 1st order histogram of the DWT coefficients with HHT-based features. The method was tested on the same dataset and a detection accuracy of 86% achieved was higher than previously reported results (72% in [103] and 80% in [104]).

To solve the image splicing detection problem, in [106], Dong et al. also used features based on image run length and edge statistics. The author used the discontinuity in correlation and coherence between image pixels with a

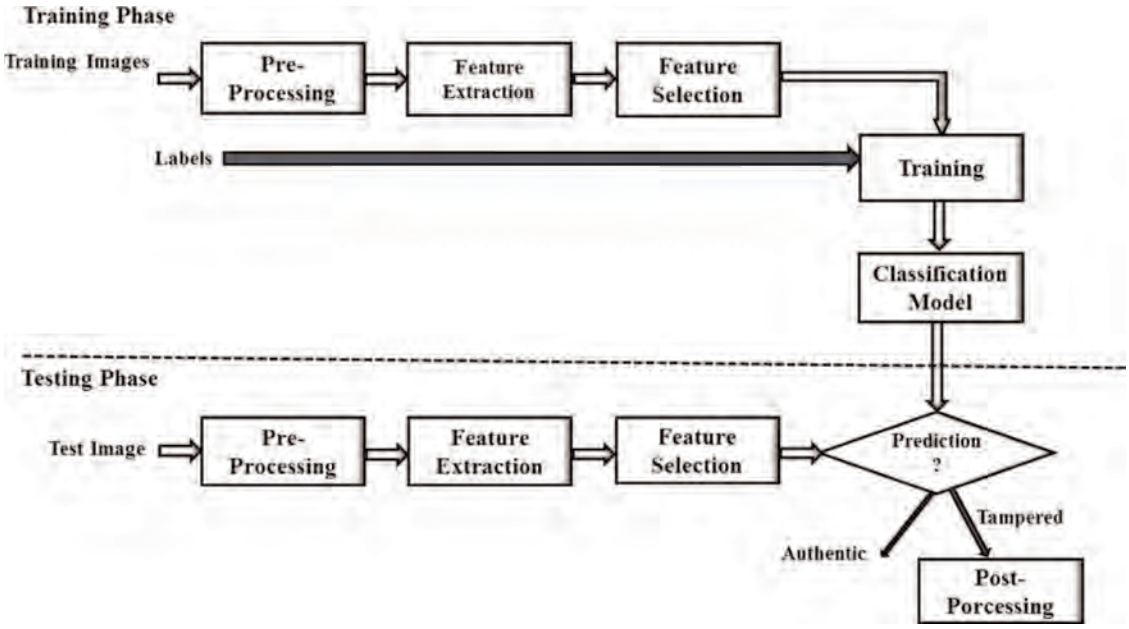

Fig. 11. General framework for image tampering detection methods.

detection accuracy of 76.52%, which was further improved to 80.58% by He et al. [107] using approximate run length features. In [108], Chen et al. proposed features based on 2D phase congruency and statistical moments of characteristic functions of wavelet sub-bands to detect sharp transitions such as lines, edges, and corners introduced by splicing operation. The detection accuracy achieved was 83% on the Columbia CISDE dataset [102]. But the major problem with this approach was the complexity of the feature extraction stage.

In [109,110], Shi et al. proposed a splicing detection algorithm based on two types of statistical features (i.e., Moments and Markov). The moment features were based on the 1-D and 2-D moments of characteristic functions [111], however, the moments based features were computationally expensive. The Markov features were based on the Transition Probability Matrix in the DCT domain, which contributes most to the robustness of the technique and with a detection accuracy of more than 91% on the CISDE dataset [102].

In [112], Zhao et al. used the 3rd order statistical features calculated from Conditional Co-occurrence Probability Matrix (CCPM) to detect image splicing. First, PCA was used to reduce the feature dimensions, and then, classification was performed using SVM. The overall accuracy of 80.80% was achieved on CISDE dataset using an SVM classifier. In [113], Zhang et al. applied LBP operator on multi-size DCT coefficients blocks. The discriminative features were extracted from LBP histograms. The feature dimension was reduced using KPCA, classification was performed using SVM, and it achieved detection accuracy of 89.9% on the CISDE dataset.

In [114] He et al. extended the results of [109] using Markov features calculated from the transition probability matrices of non-overlapping DCT blocks to capture both inter-block correlations between DCT block coefficients and intra-block correlation [115]. The Markov features in the wavelet domain were also calculated to make the algorithm robust against scaling, rotation, and translation [116]. The computational efficiency of the algorithm was increased to 94% using a recursive feature elimination technique (SVM-RFE) [117]. It was further improved by El et al. [118] using spatial domain Markov features with DCT based Markov features. The classification was performed using SVM with reduced feature dimensions using PCA, and detection accuracy of 97% was reported on CISDE dataset.

The before mentioned image splicing detection algorithms were based on the luminance component of images from the Columbia CISDE dataset [102]. An attention is also made to develop splicing detection algorithms for color images. These algorithms are tested on different publicly available color image splicing datasets.

For color images, Wang et al. [119] extracted features from the Gray Level Co-occurrence Matrix (GLCM) of thresholded edge image in YCbCr color space. The optimal features were selected using Boosting Feature Selection (BFS) technique, and highest accuracy of 90.5% was reported with 50 Cr (chrominance) features with an SVM classifier and CASIA v1.0 dataset. Then, Wang et al. [120] used Cb chrominance component to extract the features from the transition probabilities of an edge thresholded image with an accuracy of 95.6% over the CASIA v2.0 dataset. The problem with their approach was that the dataset was not fully used for the experiments. Zhao et al. [121] extracted features from revised form of Run-Length Run-Number (RLRN) technique on different color components with detection accuracy of 94%. Muhammad et al. [122] combined features from the Steerable Pyramid Transform (SPT) and LBP in YCbCr color space. The SPT transform was computed for different scales and orientations. The LBP histograms were calculated for each SPT sub-band and then concatenated to produce a feature vector. SVM was used as classifier and the experiments were performed on the three datasets. The best accuracies achieved were 96.39%, 94.89%, and 97.33%, on the Columbia color, CASIA v1.0 [18], and the CASIA v2.0 [18] image datasets respectively.

In [123], Sutthiwan et al. also used the chrominance component to detect splicing in color images. They extracted 266 moments based and Markov features. By using SVM as classifier, the detection accuracy of 98% was achieved on CASIA v1.0 dataset [18]. The same authors, in [124], utilized the rake transform on statistical features on

Table 3
Summary of splicing detection methods for Columbia CISDE dataset.

Method	Features description	Feature Dim.	Classifier	Accuracy
Ng et al. [101]	Bicoherence features	–	SVM	63.00%
Ng et al. [103]	Bicoherence features & edge pixels percentage	768	SVM	70.50%
Fu et al. [104]	Hilbert–Huang Transform (HHT) & moments of characteristic functions	110	SVM	80.15%
Li et al. [105]	HHT & DWT coefficients histograms	72	SVM	85.87%
Dong et al. [106]	RLE (Run Length & Edge statistics moments)	61	SVM	76.52%
He et al. [107]	ARL (Approximate Run Length)	30	SVM	80.58%
Moghaddasi et al. [128]	RLRN (Run Length Run Number) & Kernal PCA	50	SVM	88.28%
Shi et al. [109]	BDCT Markov & 1D and 2D moments of characteristic functions	266	SVM	91.87%
Zhongwei et al. [114]	BDCT Markov & DWT Markov	100	SVM + RFE	93.55%
El et al. [118]	BDCT Markov & Spatial Markov	50	SVM + PCA	97.33%
Chen et al. [108]	2-D Phase congruency & statistical moments of characteristic functions of wavelet subbands	120	SVM	82.32%
Zhao et al. [112]	CCPM	686	SVM + PCA	88.80%
Lu et al. [125]	High-order Auto-correlation	225	SVM	88.32%
Zhang et al. [113]	BDCT based LBP histograms	768	SVM + KPCA	89.93%
Zhang et al. [129]	CCPM of DCT & Markov	109	SVM	91.50%

the chrominance component to detect splicing in color images over CASIA image splicing datasets. In [125], Lu used the high order local autocorrelation statistical features. The multilevel wavelet transform was computed and 225 features were calculated from detail subbands. The experiments were performed on CISDE dataset and detection accuracy of 88.32% was reported using SVM.

Saleh et al. [126] proposed multi-scale Weber Local Descriptors (WLD)-based image splicing detection method. The features were extracted from differential excitation and gradient orientation of the chrominance components of an image. The detection accuracy reported was 94.19% for CASIA v1.0 and 96.61% for CASIA v2.0 datasets. Alahmadi et al. [127] proposed a detection scheme based on LBP followed by DCT. The standard deviations were used as features and the detection accuracy achieved was 97% for the CASIA v1.0 and 97.5% for the CASIA v2.0 datasets.

Among different pixel based splicing detection algorithms discussed here, the probabilistic-based Markov features have been shown to be very effective in detecting splicing-based tampering which also achieve the highest detection accuracy compared to other approaches. A summary of different splicing detection techniques discussed in this survey is shown in Tables 3–5.

The aforementioned approaches were used for splicing detection, however, most of these are unable to localize the spliced regions in the tampered image. Among different splicing localization techniques, Amerini et al. [130] proposed an image splicing localization algorithm based on first digit features extracted from the DCT coefficients and an SVM classifier. The tampered regions were localized by classifying image blocks into single and double JPEG compressed blocks. The main advantage of the algorithm was its effectiveness with respect to different values of the compression quality factor as well as the size of the tampering regions.

To deal with different types of forgeries, algorithms based on Photo-Response Non-Uniformity (PRNU) analysis have been proposed. The PRNU pattern is due to the sensor imperfections and is unique for each camera. It is present in the original images but absent in the tampered regions. Lukas et al. [131] initially proposed PRNU-based forgery detection algorithm. For the image under test, the estimated PRNU was compared with the camera PRNU and was declared as tampered, if the normalized correlation falls below a certain threshold. Further improvements in PRNU estimation of the original method [131] were made by several authors. The most prominent methods are based on nonlocal filtering [132] and the reformulation of PRNU-based forgery detection as a Bayesian estimation problem [133], among others.

During the image splicing process, for the case of out-of-focus blurred images, the tampered regions are artificially blurred to match the blur of the original image. The inconsistency is left in the blur and can be used as an evidence of tampering. Kakar et al. [134] proposed an image splicing detection technique based on inconsistency in the motion blur. To accommodate different types of blurs, recently, Bahrami et al. [135] proposed a technique for image splicing detection based on inconsistency in the degree of blur and depth information of the image. The local blur kernels were computed for image blocks and then multi-step reblurring is performed on these kernels. The features based on the relative blur degrees were used to classify image blocks based on different degrees of blur followed by a segmentation stage. The results demonstrated improved performance in splicing detection even for highly blurred images.

To support the different research efforts put in developing robust detection algorithms, the IEEE Information Forensics and Security Technical Committee (IFS-TC), in 2013, launched a “challenge” and provided a challenging dataset consisting of authentic and tampered images of different kinds (copy-move and spliced). The details of the dataset are provided in Section 5.3. The competition was organized into two phases. In Phase 1, the classification of authentic and tampered images is required, while in Phase 2, the localization of tampered regions in an image is required [136].

Table 4
Summary of splicing detection methods for CASIA v1.0 dataset.

Method	Feature desc.	Feature dim.	Classifier	Accuracy (%)
Wang et al. [119]	GLCM	Cr-50	SVM + BFS	90.50
		CbCr-100		88.60
		YCbCr-50		69.60
Sutthiwan et al. [124]	BDCT Markov & Rake transform	YCr-332	SVM + BFS	99.14
Sutthiwan et al. [123]	Moment & Markov	Cr-266	SVM	98.00
Zaho et al. [121]	RLRN	Y-60	SVM	69.20
		Cb-60		94.30
		Cr-60		94.70
Moghaddasi et al. [128]	RLRN & KPCA	Y-50	SVM	88.28
		Cb-50		89.36
		Cr-50		88.31
Muhammad et al. [122]	SPT & LBP	Y-480	SVM	66.74
		Cb-480		94.24
		Cr-475		94.89
Saleh et al. [126]	WLD	Cb-960	SVM	92.62
		Cr-960		88.66
		CbCr-1920		94.19
Alahmadi et al. [127]	LBP & DCT	–	SVM	97.00

Table 5
Summary of splicing detection methods for CASIA v2.0 dataset.

Method	Feature desc.	Feature dim.	Classifier	Accuracy (%)
Wang et al. [120]	Markov	Y-16		66.50
		Cb-16		95.60
		Cr-16		95.5
Sutthiwan et al. [124]	BDCT Markov & Rake transform	YCr-332	SVM+BFS	98.97
Zhongwei et al. [114]	BDCT Markov & DWT Markov	Y-100	SVM + RFE	89.76
Muhammad et al. [122]	SPT & LBP	Cb-123	SVM	96.94
		Cr-490		97.18
Saleh et al. [126]	WLD	Cb-960	SVM	96.61
Alahmadi et al. [127]	LBP & DCT	–	SVM	97.50

Cozzolino et al. [137] proposed a tampering detection method for the Phase 1 of IEEE IFS-TC competition. The residual image was created using a high-pass filtering and co-occurrence matrix was generated along 4 consecutive pixels in horizontal and vertical directions. The method used co-occurrence histogram features and an SVM classifier. With a detection accuracy of 94.2%, the method achieved top rank position in the Phase 1 of the competition. The same authors were also awarded the first position in Phase 2 of the competition. They proposed a technique based on the fusion of scores of three techniques, i.e., PRNU based, machine learning based, and block matching based tampering detections. The highest detection accuracy achieved on IEEE IFS-TC dataset, to date, is 40.72% [138]. Similar to [138], Gaborini et al. [139] also proposed a fusion scheme to combine results from three different forgery detection algorithms i.e., PRNU-based, PatchMatch-based, and algorithms based on near-duplicate detection exploiting the image phylogeny analysis [140]. It showed excellent detection performance on the IEEE IFS-TC dataset [136].

4.3. Image resampling detection techniques

In image splicing and copy-move forgery, the targeted image portions undergo identical geometric transformations like rotation, scaling, stretching, skewing, and flipping to maintain the constant aspect ratio across the picture. On the other hand, resampling is based on an important interpolation step that leads to some statistical changes in the tampered image. The traces left by the interpolation step in resampling can be used in tampering detection.

Popescu et al. [141] considered the imperceptible specific correlations introduced in the interpolation process to detect traces of resampling. The Expectation–Maximization (EM) algorithm and probability mapping (p-map) of image pixels in the frequency domain were used to identify the interpolated pixels. The main problem with the method was that it did not perform well on compressed images.

In [142], Gallagher et al. experienced that linear and cubic interpolation introduces periodicity in the 2nd order derivative of signals and can be determined by using the Discrete Fourier Transform (DFT) of the 2nd derivative of the overall image. However, the algorithm performed well only for scaled images and not so much for rotated and skewed images. Similarly, Prasad et al. [143] made the stance stronger when they found that the 2nd derivative of interpolated signals exhibits periodic properties, but the method encountered similar weaknesses experienced in [142].

In [144–147], Kirchner and others proposed for resampling detection in tampered images by using the variance of prediction residuals of resampled signals that was further elaborated in [148–151]. Whereas in [152,153], Mahdian and Saic proposed an algorithm to detect resampling by exploiting periodic properties of covariance structure of interpolated signals and their derivatives. The Radon Transform was applied to the derivative of the image, followed by a search for periodicity. The same authors in [154] performed cyclostationarity analysis to detect specific correlations between spectral components. Additional studies using cyclostationarity analysis in resampling detection were also discussed in [155,156].

In [157], Mahdian studied the effect of noise introduced in the resampling operation. They proposed that noise estimation at various levels in wavelet domain can be used as a clue for tampering detection. In [158], Feng et al. proposed a scheme for detecting resampling by examining the normalized energy density in variable size local windows for the 2nd derivative of an image in the frequency domain that lead to excellent results for both bilinear and bicubic interpolations. In [159], Pfennig and Kirchner used the analytical models of spectral energy distribution of rescaled images [158] and the periodic interpolation artifacts for blind estimation of the exact scaling factor in geometrical transformations (i.e., upsampling or downsampling).

Image recapturing detection is also important in image forensics. In image recapturing, an image is first displayed on a printed medium or Liquid Crystal Display (LCD) and high-quality image is recaptured by a digital camera or a scanner. For humans, these recaptured images cannot be successfully distinguished from the original images. The conventional clues used in image forensics e.g., sensor noise, lens aberration, JPEG artifacts, etc., fail to identify tampering in recaptured imaging. Other artifacts introduced in the tampering process are also removed in the recaptured images. Therefore, a forger can exploit the image recapturing process to fool the image forensic systems, by first displaying the tampered image on a high quality printed material or an LCD, and recapturing it with a high-definition photo camera. To overcome this threat, it is critical to distinguish the recaptured images from the photographic images.

Some of the research efforts in this direction include the work in forensic analysis of scanned prints [160] and LCD screens [161–163]. In [161], Cao et al. proposed image recapturing detection on LCD screens based on combination of different features. The textured anomalies were captured with LBP features at multiple scales (80 features), the loss of fine details were detected with multilevel wavelet statistics (54 features), and the color anomalies (i.e., an increase in color saturation) introduced in the recaptured images were captured using 54 different color features. The combination of 155 features was fed to an SVM classifier and an Equal Error Rate (EER) of 0.5% was reported.

During image recapturing from an LCD screen, aliasing artifacts are introduced due to the high frequency periodic pattern of the monitor pixel grid structure and are difficult to eliminate in post-processing stages. These aliasing artifacts were captured by detecting peaks in the 2D spectrum of the noise residuals in the recaptured images [162].

Recently, Thongkamwitoon et al. [163] proposed image capturing detection technique from LCD screens based on edge blurriness features. The line spread functions of edge profiles were used to train single-capture and recapture dictionaries using the K-SVD approach. An SVM classifier was then used to detect recaptured images using dictionary approximation errors and mean edge spread width. The detection accuracies of 99% for recaptured images and 94% for single captured images were reported on a dataset consisting of more than 2500 high-quality recaptured images.

For automatic recapturing of video sequences, Visentini et al. [164] proposed a model based on radial distortion artifacts. It was observed that recapturing chains introduced high-order components. The curved edge features from video frames were extracted and lens distortion was estimated.

Moreover, with the advent of powerful softwares, it is easy to generate photorealistic Computer Generated (CG) images that are difficult to distinguish from the natural photographic (PG) images. In image forensics, it is important to distinguish between PG and CG images. Khanna et al. [165] proposed a technique to distinguish between an image captured using a digital camera, a scanner, and a CG image based on residual sensor pattern noise features extracted from digital cameras and scanners. A denoising filter bank with four different types of denoising filters was used to generate sensor noise patterns. These fingerprints were then used to train an SVM classifier and a detection accuracy of 85.9% was achieved. The extracted fingerprints were also shown to be robust against different post-processing operations like image sharpening, contrast stretching, and JPEG compression. Similarly, Nguyen et al. [166] proposed an algorithm for discriminating between PG and CG human faces based on estimation of face asymmetry in videos. The main concept was that CG facial expressions exhibit repetitive patterns compared to the natural ones. The results showed better results on small datasets. However, the main problem with the proposed scheme was that it only supports frontal faces and is sensitive to illumination. Recently, Peng et al. [167] proposed a scheme to distinguish PG and CG images using both textural and statistical features. A total of 31 features were extracted and classification accuracy of 97.89% and 97.75% was achieved for CG and PG images respectively, with an SVM classifier. The algorithm was also shown to be robust against additive noise and JPEG compression artifacts.

4.4. Image retouching detection techniques

Since the last decade, electronic and print media as well used image retouching tools like Adobe Photoshop, etc., to make the photos more natural and attractive. Retouched photos are used to create an admirable representation of real beauty. Whereas the literature has different approaches in detecting the originality of an image and are categorized according to the detection of enhancement operation.

4.4.1. Image inpainting detection

Image inpainting is used to recover and/or remove some parts of the image without any perceptual loss [168]. It is based on copy and move of most similar parts of the image with some well-defined rule. It is different from copy-move forgery in a sense that different patches are coming from different locations of the image instead of same continuous area of the image. Its applications are to

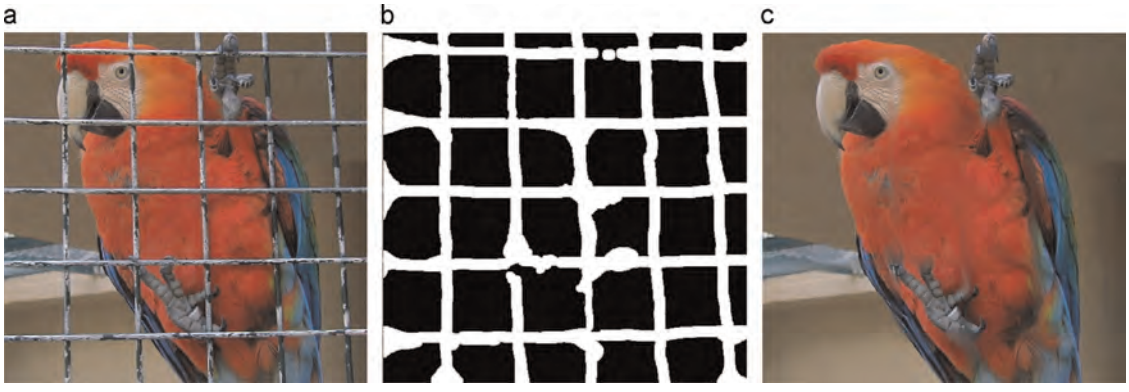

Fig. 12. An example of image inpainting (a) original image, (b) binary mask, (c) inpainted image.

remove text or stamps from images and to remove wrinkles in image retouching. So copy-move forgery detection algorithms are not directly applicable for image inpainting detection. Fig. 12 shows a nice example of image inpainting where the cage is totally removed in the inpainted image.

In [169], Das et al. calculated zero-connectivity features with fuzzy membership functions for inpainting detection in video frames. Chang et al. [170] used Multi-Region Relation (MRR) to recognize inpainted regions from the suspicious regions which was further improved by [171]. Zhao et al. [172] proposed blind inpainting detection for JPEG compressed images. Both the tampered image and its JPEG compressed version at different quality were divided into fixed sized blocks and averaged sum of absolute difference was calculated for the blocks between the two images. Trung et al. [173] used simple block matching approach for inpainting detection. The similar pairs of blocks were searched using the similarity measure, distance measure and cardinality measure (number of same pixels) for 3 different thresholds respectively. The locations of the matched blocks were used to generate the tampering mask. The method was tested for number of images created from different inpainting algorithms.

Recently Liang et al. [171] proposed an efficient algorithm for image inpainting detection. It started with searching for similar blocks to detect suspicious regions and blocks belonging to the uniform areas were filtered using vector similarity. The forgery localization was improved using Multi-Region Relation (MRR), to remove the suspicious blocks belonging to the uniform regions. The computational speed was improved using weight transformation based feature matching. The experiments demonstrated the effectiveness of the algorithm on different inpainted images as well as for copy-move forged images.

Besides the detection of general purpose image enhancement methods, there exists image retouching detection methods suitable only for human facial images. In [174], Hatice Gunes et al. used facial proportions for assessing facial beauty. The localizations of the face, eye, pupil, eyebrow, base of the nose, lip and chin were used as features. The technique confirmed the importance of these features in quantifying human judgement of beauty. The method was further improved by Dantcheva [175], with the addition of impermanent facial features like make-up, hair-style, or presence of glasses. A linear metric based on Mean Opinion Score (MOS) was proven to provide promising results in assessing facial beauty. Li et al. [176] proposed blind retouching detection technique based on Bi-Laplacian filtering. The image blocks were matched using KD-Tree and hierarchical clustering followed by 7-tap Laplacian filtering performed to eliminate the false matches. It showed good performance for uncompressed and high-resolution compressed images.

In [177], Farid and Kee introduced a metric (range 1–5) for quantifying alterations of digital photograph of a human face done by digital photo-editing techniques. A score of one represented minimal retouching while five represented a drastic reworking of the photograph. Different photo retouching models were used to quantify the perceptual improvement due to photometric and geometric modifications. The geometric modification was quantified using 4 statistics: the mean and standard deviation of the motion magnitude computed separately on the face and body of the subject, whereas the photometric modification was quantified by 4 statistics: the means and standard deviations of both the spatial boundaries of local smoothing/sharpening filters and the similarity metric SSIM (Structural Similarity Index Metric). The SSIM is a robust metric traditionally used for full reference image quality assessment. A baseline established by human rankings of 450 “before and after” photos was used to assess alteration in photos. The results showed a strong correlation of the metric score with the subjective judgments which may lead to automatic quantifying the amount of retouching in a photo. But the major weakness in this technique is that it required original image. Such metrics are called Full-Reference (FR) image quality metrics. Evaluating quality, when only the retouched image is present, is still a very challenging problem and provides excellent research opportunities for both forgery detection and image quality assessment [228,229].

Recently, Xie et al. [178] proposed a dataset for facial beauty prediction based on 18 geometrical and 2 Gabor texture features. The prediction of facial beauty was performed using both machine learning and deep learning techniques. The results showed a good correlation with the subjective ratings with an average Pearson correlation coefficient of 0.66 and 0.82, for machine learning and deep learning techniques, respectively.

4.5. Post-processing image operations

During the image tampering process, the tampered regions undergo various post-processing operations with the purpose of concealing the different traces of tampering. These operations can be of diverse nature including image smoothing, contrast enhancement, histogram equalization, median filtering, and/or Gamma correction. In image forensics, it is important to investigate the different processing operations a given image is subjected to during the tampering stage. To this extent, we discuss below the different approaches used for detecting different post-processing operations used in image forensics. We group these methods under four broad categories: i.e., median filter detection, contrast enhancement detection, sharpening detection, and additive noise detection.

4.5.1. Median filtering detection

The median filtering is used to remove the salt and pepper noise and to smooth edges in digital images. Kirchner et al. [179] introduced a simple and efficient technique to detect median filtering in uncompressed digital images. It was based on the fact that in median filtering, in a local window, the output pixel value is one of input pixel values and produces “streaking artifacts” due to the sharing of same values in adjacent rows and columns. The histograms of first order differences for a group of two pixels were used to categorize the original and the median filtered images. For JPEG compressed images, Subtractive Pixel Adjacency Matrix (SPAM) based features [180] were

also calculated from the conditional joint distribution of 1st order difference image. Cao et al. [181] proposed a detection technique based on the statistical characteristics of median filter. The probability of zero values calculated on difference map of image texture signal was used as features. Yuan et al. [182], proposed a blind method based on an idea that 2-D median filter only smooths noise without introducing any new gray levels and, hence, significantly reduces the number of gray levels in a local filter window. A 44-D feature vector computed from five different types of features was used in the classification. It outperformed [181,179] and effective on different types of images (e.g., sampled, denoised, scanned or photographic) as well as rescaled and JPEG compressed images. Kang et al. [183] used auto regressive model for median filtering detection in digital images.

4.5.2. Contrast enhancement detection

Image contrast enhancement is used to increase the dynamic range of image pixel values and is widely used in digital image processing. Stamm and Liu [184–186] contributed different techniques to investigate the processing history in digital images in terms of histogram equalization and contrast enhancement. In their earlier work [184], a global contrast enhancement detection technique was proposed. The idea behind their approach was that histograms of unaltered and contrast enhanced images differ in their contours. The gray value histogram of enhanced image exhibits clear peak/gap artifacts instead of a smooth histogram. But, the method failed in detecting the local contrast enhancement. It was further extended by the same authors in [185], to accommodate the detection of local contrast enhancement, histogram equalization, and noise addition in digital images. In addition to contrast enhancement detection, the splicing localization is proposed by the same authors in [186]. The major problem with the methods in [185,186] is that they fail to detect contrast enhancement in the previously middle/low quality JPEG compressed images.

Mahalakshmi et al. [187] proposed image forgery detection method in case of rescaling, rotation, histogram equalization, and contrast enhancement. The detection performance was poor for images undergone rotation and scaling operations in JPEG compressed images. The problem was solved with the addition of noise in the preprocessing stage of detection algorithm. Cao et al. [188] proposed a technique for both global and local contrast detection in digital images using histogram peak/gap artifacts analysis. The technique performs well for both uncompressed and JPEG compressed images followed by contrast enhancement. But it performs well only for the case, when contrast enhancement is the last post-processing step and fails when JPEG compression is applied after the contrast enhancement. Yuan et al. [189] proposed an algorithm to detect histogram equalization by modeling the histogram equalized image as discrete identity function. The method provides excellent detection performance for low-resolution images, as well as for the histogram equalization followed by JPEG post-compression and post-resizing operations.

Gamma correction is also a contrast enhancement technique. Cao et al. [190] proposed a blind Gamma correction detection technique for image forensic analysis. The histogram features were calculated using peak gaps patterns and a feature comparison was performed between the Gamma corrected images and the unaltered images. The technique was suitable for Gamma correction detection either applied locally or globally in digital images.

4.5.3. Sharpening filtering detection

Image sharpening is an enhancement operation and is mostly used to highlight the image details or increase the contrast of image edge pixels. In image forgery, it is also used to hide the traces left by image tampering operations. Therefore, it is important to detect the sharpening operation for digital image forensic analysis. Cao et al. [191] proposed a blind algorithm for image sharpening detection using ringing artifacts and histogram gradient abnormality with the detection accuracy of 90%. The main limitation with this method is that it does not work for the images with wide histogram before the sharpening operation. Unsharpmasking is another type of high-pass filtering used in digital image retouching. The same authors in [192] also proposed a blind method to detect retouching manipulations from unsharpmask sharpening in digital images. It was based on measuring the overshoot strength for a pixel sequences and averaging them for the whole image. The major problem with this technique is that it only distinguishes between unsharpmask sharpened images and unsharpened images and it does not perform well for the JPEG compressed images.

Ding et al. [193] used LBP which is very powerful texture operator to detect sharpening operation in digital images. In their technique, an edge image was created using Canny edge operator and rotation-invariant LBP operator was applied on the edge image. The LBP histogram features were extracted for both sharpened and unsharpened images in the dataset. The training was performed using an SVM classifier. The method achieved a detection accuracy of over 90%. The same authors in [194] used edge perpendicular binary coding (EPBC) for the detection of unsharpmasking in digital images. In contrast to square window in LBP-based method, here in EPBC, a rectangular window along perpendicular direction to image edge followed by binary coding was used to characterize the change in texture due to unsharpmasking operation.

4.5.4. Additive noise detection

To hide/remove the visual traces left by tampering operations, noise is added to the tampered image. In forensic analysis of digital images, the detection of noise is also important. Cao et al. [195] proposed features calculated from image blocks for global noise detection in digital images. The effect on block-wise pixel value distribution was used to detect noise addition.

The aforementioned techniques were used to detect the type of post-processing operations used in the tampering process. Since, in image tampering, a number of operations can be performed simultaneously, the knowledge of the

Table 6
Summary of retouching and post-processing detection methods.

Method	Features description	Detection	Classifier	Accuracy
Stamm et al. [184]	Gray value histogram	Contrast enhancement, histogram equalization, additive noise	Thresholding classifier	Global contrast=99%, Local contrast=98.5%, Histogram equalization=99%, Additive noise=99%
Cao et al. [188]	Histogram peaks/gaps fingerprints	Global and local contrast enhancement	Thresholding classifier	100%
Cao et al. [181]	Zero value probability on first order difference map	Median filtering	Thresholding classifier	TP >85%
Kirchner et al. [179]	Streaking artifacts (uncompressed images)	Median filtering	SVM	FPR <1.8%
	SPAM features (compressed images)	Median filtering	SVM	P_e=1.1%
Yuan et al. [182]	44-D features based on order statistics and gray level	Median filtering	Soft-margin SVM	
Cao et al. [191]	Histogram gradient aberration	Sharpening	SVM	90%
Ding et al. [193]	Rotation-invariant LBP	Sharpening	SVM	Accuracy >90%
Cao et al. [192]	Overshoot strength	Unsharpmasking using Laplacian filtering	Accuracy <80%	
Ding et al. [194]	EPBC-based	Unsharpmasking	SVM	94.93%
Farid et al. [177]	6 summary statistics	Retouching	nonlinear SVR	R-value=0.8, prediction error=0.30

sequence in which the editing operations are performed can help in the field of image forensics and is still a challenging task. Recently, Stamm et al. [196] proposed a framework to determine the order of contrast enhancement followed by resizing using multiple pairs of hypothesis tests to differentiate between each ordered pair of manipulations.

To summarize the research efforts put on retouching and post-processing detection, we show in Table 6 the different approaches used, as well as their features/classification framework and their overall performance.

5. Image forensics datasets

With the increased growth of research activities in forensic science, it is important to create benchmarking image forgery datasets to evaluate the performance of different forgery detection algorithms. There are several publicly available image forgery datasets supporting image copy-move, splicing, resampling and retouching research efforts. A brief description of these datasets is given below.

5.1. Copy-move forgery datasets

To evaluate the performance of copy-move forgery detection algorithms, the recently developed publicly available datasets are MICC-F2000, [197], MICC-F220 [197], and MICC-F600 [63]. The MICC-F2000 [197] consists of 1300 authentic and 700 tampered color images. The images in the dataset are of diverse contents having dimension of 2048×1536. The tampered images are created by copy-move operation of small rectangular patches from the image. Different post-processing operations (e.g., Rotation, Scaling, Translation (RST) or their combination) have been performed on the tampered blocks. However, ground truth is not provided with the dataset, so it is difficult to evaluate the accuracy of forgery detection algorithms. The MICC-F220 [197] is a subset of MICC-F2000 and it contains 220 equally distributed into tampered and authentic images. Some sample images from this dataset are shown in Fig. 13.

The MICC-F600 [63] is the challenging dataset consisting of high-resolution tampered images. The images are created by rotation, scaling, translation of copy-move regions with different shapes and sizes. The ground truth for the copy-move forgery is also provided in the dataset which is very important to evaluate the performance of detection algorithms. Fig. 14 shows example images from the dataset where the tampered images are shown in the top row while the ground truth images associated to the copy-move forgery are shown in bottom row. A detailed description of these datasets is also summarized in Table 7.

5.2. Image splicing datasets

Among different publicly available image splicing datasets, the Columbia Image Splicing Detection Evaluation (CISDE) dataset is the one being first created by Digital Video and Multimedia Lab (DVMM), at Columbia university [102], consists of 933 authentic and 912 tampered

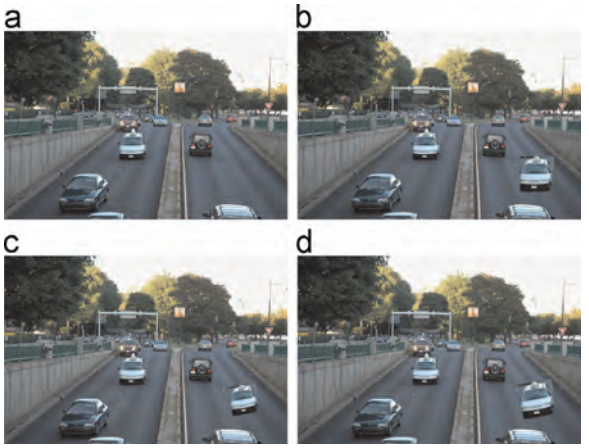

Fig. 13. Examples of authentic and tampered images from MICC-F2000 [197]: (a) original images, (b) copy-move with scaling, (c) copy-move with rotation, (d) copy-move with both rotation and scaling.

images. The images in the dataset are of diverse contents and in gray-scaled bitmap format having dimension of 128×128. The tampered images are created by cut-and-paste along with object boundaries or horizontal/vertical strips, from the same or other images. The images in the dataset are of very low resolution and have sharp edges at the borders of the spliced regions. Some sample images from this dataset are shown in Fig. 15. For color images, the same group developed another dataset, the Columbia Uncompressed Image Splicing Detection Evaluation (CUISDE) dataset [198]. The dataset contains 183 authentic and 180 tampered images in uncompressed format (BMP or TIFF) and with dimensions ranging from 757×568 to 1152×768. The tampered images were created using splicing (copy-move from different images) and without any post-processing, making these, to a certain degree, unnatural.

Fig. 14. Examples of tampered images and the ground truth mask from MICC-F600 dataset [63]: copy-move tampered images (top row), ground truth masks identifying the copy-move (bottom row).

Table 7
Description of various copy-move forgery datasets.

Description	MICC-F2000 [197]	MICC-F220 [197]	MICC-F600 [63]
No. of images	2000	220	600
No. of authentic images	1300	110	440
No. of tampered images	700	110	160
Image types	Color	Color	Color
Image resolutions	2048×1536	722×480, 800×600	3264×2448
Image formats	JPEG	JPEG	PNG
Type of attacks	RST	RST	RST

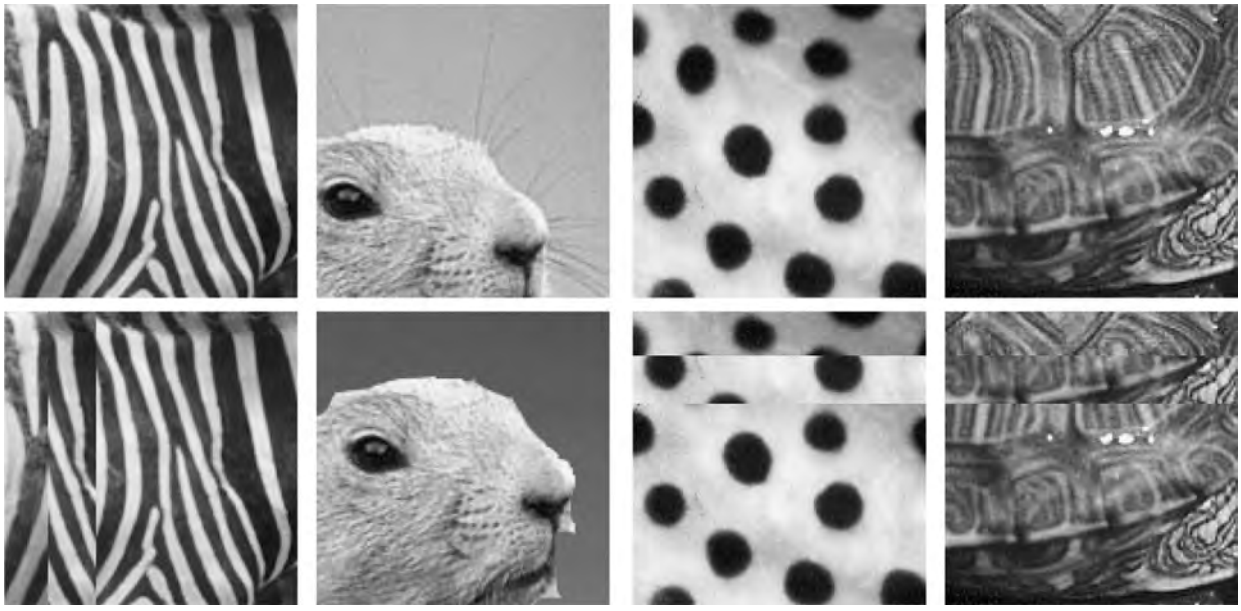

Fig. 15. Examples of authentic and tampered images from Columbia dataset [102]: authentic images (top row), tampered images (bottom row).

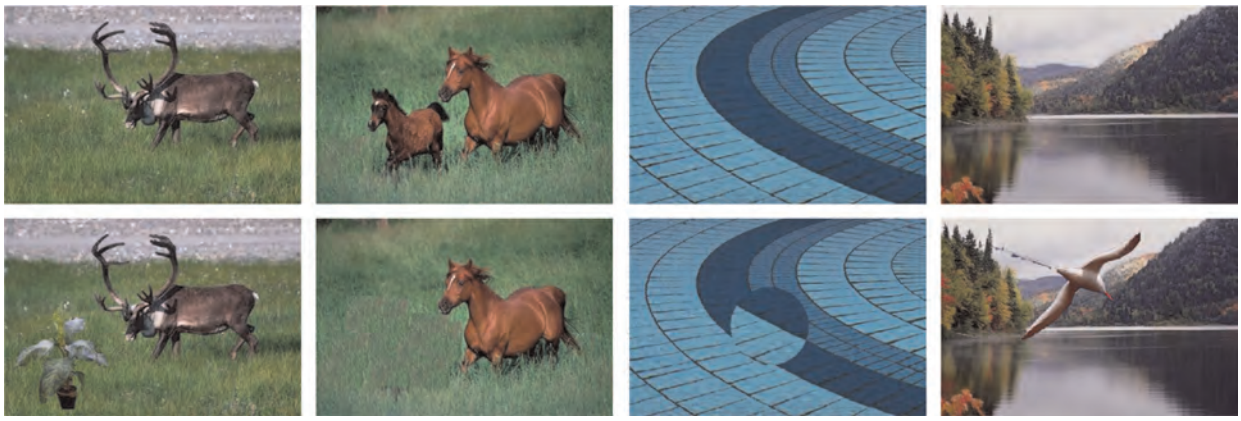

Fig. 16. Examples of images from CASIA V1.0 dataset [19]: authentic images (top row), tampered images (bottom row).

Another image splicing dataset is provided by the Chinese Academy of Sciences, Institute of Automation (CASIA). The CASIA Tampered Image Detection Evaluation (TIDE) v1.0 [19] is color images dataset with 800 authentic and 921 tampered images. There are 459 tampered images created from copy-move forgery operation and the remaining tampered images created using splicing operation from two or more images. Different post-processing operations and geometric transformations (such as rotation, scaling, and blurring) are applied on the tampered images. The images in the dataset are in JPEG format and of low resolutions with dimension of 384×256 pixels. The CASIA TIDE v2.0 [19] is an extended version of the CASIA v1.0 dataset consisting of high resolution 7491 authentic and 5123 tampered color images. The images are in JPEG, BMP, and TIFF format with the dimensions varying from 240×160 to 900×600 pixels. In both CASIA TIDE v1.0 and v2.0 datasets, the dimensions of most of the images are small compared to real test images. Figs. 16 and 17 show some sample images from the CASIA datasets. A detailed description of these datasets is also provided in Table 8.

5.3. IEEE IFS-TC first image forensics challenge dataset

Recently, the IEEE Information Forensics and Security Technical Committee (IFS-TC) launched a challenge that aims at evaluating forgery detection and localization algorithms on a unified protocol as well as on the same dataset [136]. The dataset provided for this purpose contains 7913 images divided into training and testing groups. There are 450 tampered images and 1050 pristine (authentic) images in the training group while rest of the images are used for testing. The dataset provides the class information (either authentic or tampered) of the images in the training group as well as the ground truth masks (for tampering localization) for the tampered images in

Fig. 17. Examples of images from CASIA v2.0 dataset [19]: authentic images (top row), tampered images (bottom row).

Table 8
Description of various image splicing datasets.

Description	CISDE [102]	CUISDE [198]	CASIA v1.0 [19]	CASIA v2.0 [19]
No. of images	1845	363	1721	12 614
No. of authentic images	933	183	800	7491
No. of tampered images	912	180	921	5123
Image types	Gray	Color	Color	Color
Image resolutions	128×128	757×568, 1152×768	384×256	384×256, 900×600
Image formats	BMP	TIFF	JPEG	JPEG , TIFF, BMP

Fig. 18. Examples of authentic and forged images from IFS-TC dataset [136]: authentic images (top row), tampered images with masks (bottom row). (A white (all pixels=255) represents no traces of tampering while a black region (pixels=0) represents a manipulated region.)

that group. The tampered images are created using copy-move and splicing operations. While in the testing group, there are 5713 images including both fake and pristine, without any labeling (no information about the original and fake images information and ground truth mask for the tampered images). There is also another set of 700 tampered images in the testing group for officially testing the tampering localization in the forensics challenge. The images in the dataset are in PNG format and most of them have dimensions 1025×768. Fig. 18 shows some example images from the IFS-TC dataset.

5.4. Image retouching dataset

Given the importance of image retouching in fashion and multimedia industry, a publicly available face dataset namely the SCUT-FBP [178] is provided for objectively estimating the facial beauty and to evaluate the performance of different facial attractiveness estimation methods. It contains 500 different female face images along with the attractiveness rating scores computed from individual scores from 70 observers. Fig. 19 shows sample images from the SCUT-FBP dataset.

Fig. 19. Example images from the SCUT-FBP dataset [178].

6. Anti-forensics and anti–anti forensics

It is worth noting that researchers are more focused on developing robust algorithms for the detection of image tampering while little attention has been given to attackers who work on developing algorithms that could deceive such forging detection algorithms. The research field that challenges digital forensics and systematically explores its limitations against intelligent counterfeiters is called counter-forensics, or anti-forensics [3,199,200]. In anti-forensics, the focus is on the methods that can mislead forensic techniques by hiding traces of tampering. Several techniques have been introduced to hide image manipulations including contrast enhancement [201,202], unsharpmasking [203], median filtering [204], JPEG compression [205–210], JPEG2000 compression [211], and resampling [212]. Other counter forensics techniques involve forging the inherent PRNU noise of camera sensor [213], introducing CFA artifacts artificially [214], among others [215–217,199].

While the focus of the paper is not counter-forensics, it is important to raise the alarm and promote awareness among researchers to pay more attention to such malicious attacks and develop robust algorithms for improving the safety of forensic methods and countering anti-forensic attacks. To tackle with the anti-forensics, counter counter-forensics (or anti anti-forensics) is under investigation. In this regard, Valenzise et al. [218,219] proposed a method to counter anti-forensics of JPEG compression [205] by using image quality features along with the total variation. Similarly, Lai et al. [220] also proposed detectors to expose anti-forensics in JPEG images. Cao et al. [221] introduced a semi-nonintrusive approach to detect anti-forensics of resampling [212] through analyzing the output for resampling with some specially designed images. Zeng et al. [222] identified anti-forensics of median filtering [204] via detecting the peaks in Fourier transform domain for the ratio of horizontal pixel differences with zero values. De et al. [223] proposed methods to counter anti-forensics of contrast enhancement. In counter forensic of SIFT-based copy-move forgery detection, the local and global SIFT keypoints were removed or added from the image to hide the tampering traces. To counter the fake injection and removal of SIFT keypoints, Costanzo et al. [224] proposed an anti anti-forensics technique for copy-move forgery by looking for the inconsistencies like the absence or anomalous distribution of keypoints within high variance image regions. Once again, the coupling of forensics and security is gained more momentum in recent

years and is expected to grow further over the next few years.

7. Discussion and conclusion

Our extended overview of image forgery detection techniques shows that this area of research is still in its flourishing stage, and holds a huge potential for future R&D applications. Although many of the techniques discussed here require some types of assumptions to provide excellent detection results, with more research efforts, we expect some robust methods to become standard tools in the near future.

In the introductory section, we outlined that digital image forgery detection approaches have traditionally been categorized into active and passive techniques. Under the active framework, robust techniques have been developed for forgery detection, including watermarking and signature generation. These, however, have limited applications as they require some preprocessing at the image creation stage. More importantly, most of the internet images are not embedded with digital signature or watermark. Under such a scenario, digital images cannot be authenticated using active techniques. Unlike passive techniques do not require no watermark or digital signature embedding in advance. Among the different approaches used under this blind scenario, we showed that pixel-based techniques continue to be the simplest and most common approaches used in practice.

Before leaving this topic, it is worth noting that most of the research efforts are focused on developing robust algorithms for the detection of image tampering while little attention has been given to attackers who work on developing algorithms that could deceive such forging detection algorithms. The research field that challenges digital forensics and systematically explores its limitations against intelligent counterfeiters is called counter-forensics, or anti-forensics [3,199,200]. In counter-forensics, the focus is on the methods that can mislead forensic techniques by hiding traces of tampering. Several techniques have been introduced to hide image manipulations including filtering, contrast enhancement, compression, and/or resampling, among others. While the focus of the paper in not counter-forensics, it is important to raise the alarm and promote awareness among researchers to pay more attention to such malicious attacks and develop robust algorithms for improving the safety of forensic methods and countering counter-forensic attacks.

Another important challenge that we discussed in this survey is the problem of multiple manipulations/tampering. While a given technique may be powerful in detecting copy-move tampering, the same technique may not be applicable for resampling. For this reason, among others, we are witnessing a growing interest in developing hybrid techniques combining more than one approach at a time (e.g., combination of spatial or transform domain based methods). Moreover, the use of different image quality models in forgery detection is also a new research direction that is starting to attract the researchers in this field [225,226].

In the future, we foresee integrated forensic systems that can authenticate both image and video subjected to various types of tampering attacks. Numerous challenges in this field still exist, however, which offer researchers great challenges and opportunities. More importantly, we will see more work in developing authentication approaches that combine both image, video, and audio. Ideas developed for images will be reframed for audio and video and vice versa.

A final comment is worth noting in relation to quantifying the performance of different forgery detection approaches discussed in the literature. While there were several efforts put forward in developing benchmarking databases, there is still a need for creating more comprehensive and publicly available authentic and forged images datasets as well as ground truth covering different kinds of tampering attacks along with detailed information about the forgery including location, type, and size of forged portions in the tampered image. This will eventually be helpful in carrying extensive comparisons of different detection algorithms in terms of some specific performance indices.

Acknowledgments

The authors would like to thank the editor and the anonymous reviewers for their valuable comments. The work was supported in part by a DSR-funded project at KFUPM under Project no. IN121012.

References

[1] P. Lester, Photojournalism: An Ethical Approach, Lawrence Erlbaum Associates Inc., Hillsdale, NJ, USA, 1991.
[2] Photo tampering throughout history, ⟨http://http://www.fourandsix.com/photo-tampering-history?currentPage=4⟩, Accessed: 2015-03-27, 2004.
[3] M.C. Stamm, M. Wu, K. Liu, Information forensics: an overview of the first decade, IEEE Access 1 (2013) 167–200.
[4] J.A. Redi, W. Taktak, J.-L. Dugelay, Digital image forensics: a booklet for beginners, Multimed. Tools Appl. 51 (1) (2011) 133–162.
[5] H. Farid, Image forgery detection: a survey, IEEE Signal Process. Mag. 26 (2) (2009) 16–25.
[6] B. Mahdian, S. Saic, A bibliography on blind methods for identifying image forgery, Signal Process.: Image Commun. 25 (6) (2010) 389–399.
[7] A. Piva, An overview on image forensics, ISRN Signal Process. (2013) 1–22.
[8] T. Qazi, K. Hayat, S.U. Khan, S.A. Madani, I.A. Khan, J. Kołodziej, H. Li, W. Lin, K.C. Yow, C.-Z. Xu, Survey on blind image forgery detection, IET Image Process. 7 (7) (2013) 660–670.
[9] O.M. Al-Qershi, B.E. Khoo, Passive detection of copy-move forgery in digital images: state-of-the-art, Forensic Sci. Int. 231 (1–3) (2013) 284–295.
[10] G.K. Birajdar, V.H. Mankar, Digital image forgery detection using passive techniques: a survey, Digit. Investig. 10 (3) (2013) 226–245.
[11] M. Ali Qureshi, M. Deriche, A review on copy move image forgery detection techniques, in: 11th International Multi-Conference on Systems, Signals & Devices (SSD), IEEE, Barcelona, Spain, 2014, pp. 1–5.
[12] K. Eismann, Photoshop Restoration and Retouching, Peachpit Press, 2005.
[13] 40 Amazing Before and After Photo Retouching Photos, ⟨http://10steps.sg/inspirations/artworks/40-cool-before-and-after-photo-retouching-photos⟩, Accessed: 2015-03-27, March 2013.

[14] Jopseph Casers: Sin Photoshop Y Con Photoshop, ⟨http://merengala.blogspot.com/2010/12/sin-photoshop-y-con-photoshop.html⟩, Accessed: 2015-03-27, April 2013.
[15] A.J. Fridrich, B.D. Soukal, A.J. Lukáš, Detection of copy-move forgery in digital images, in: Digital Forensic Research Workshop (DFRWS), Citeseer, 2003.
[16] M. Nizza, P.J. Lyons, In an iranian image, a missile too many, ⟨http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/⟩, Accessed: 2015-02-21, 2008.
[17] H. Farid, Detecting Digital Forgeries Using Bispectral Analysis, Technical Report AIM-1657, AI Lab, Massachusetts Institute of Technology, 1999.
[18] J. Dong, W. Wang, CASIA tampered image detection evaluation (TIDE) database, v1. 0 and v2. 0, ⟨http://forensics.idealtest.org:8080/⟩, Accessed: 2014-01-17, 2011.
[19] J. Dong, W. Wang, T. Tan, CASIA image tampering detection evaluation database, in: IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP), IEEE, Beijing, China, 2013, pp. 422–426.
[20] I.J. Cox, M.L. Miller, J.A. Bloom, Digital Watermarking, Morgan Kaufmann, Orlando, FL, USA, 2001.
[21] M. Barni, F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, Signal Processing and Communications, Marcel Dekker, New York, USA, 2004.
[22] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd edition, . Morgan Kaufmann, Francisco, CA, USA, 2008.
[23] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, 1st edition, . CRC Press, Boca Raton, FL, USA, 1996.
[24] D. Fu, Y.Q. Shi, W. Su, A generalized Benford's law for JPEG coefficients and its applications in image forensics, in: Electronic Imaging, vol. 6505, International Society for Optics and Photonics, San Jose, CA, USA, 2007, p. 65051L.
[25] B. Li, Y.Q. Shi, J. Huang, Detecting doubly compressed JPEG images by using mode based first digit features, in: 10th Workshop on Multimedia Signal Processing, IEEE, Cairns, QLD, Australia, 2008, pp. 730–735.
[26] T. Bianchi, A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 1003–1017.
[27] T. Bianchi, A. Piva, Detection of nonaligned double JPEG compression based on integer periodicity maps, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 842–848.
[28] S. Milani, M. Tagliasacchi, S. Tubaro, Discriminating multiple JPEG compression using first digit features, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Kyoto, Japan, 2012, pp. 2253–2256.
[29] C. Pasquini, G. Boato, F. Perez-Gonzalez, Multiple JPEG compression detection by means of Benford–Fourier coefficients, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Atlanta, GA, USA, 2014, pp. 113–118.
[30] Z. Fan, R.L. De Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, IEEE Trans. Image Process. 12 (2) (2003) 230–235.
[31] M.K. Johnson, H. Farid, Exposing digital forgeries through chromatic aberration, in: 8th Workshop on Multimedia and Security, ACM, New York, NY, USA, 2006, pp. 48–55.
[32] A. Swaminathan, M. Wu, K.R. Liu, Nonintrusive component forensics of visual sensors using output images, IEEE Trans. Inf. Forensics Secur. 2 (1) (2007) 91–106.
[33] J. Lukas, J. Fridrich, M. Goljan, Digital camera identification from sensor pattern noise, IEEE Trans. Inf. Forensics Secur. 1 (2) (2006) 205–214.
[34] A.E. Dirik, N.D. Memon, Image tamper detection based on demosaicing artifacts., in: International Conference on Image Processing (ICIP), IEEE, San Diego, CA, USA, 2009, pp. 1497–1500.
[35] M. Chen, J. Fridrich, M. Goljan, J. Lukáš, Determining image origin and integrity using sensor noise, IEEE Trans. Inf. Forensics Secur. 3 (1) (2008) 74–90.
[36] S. Bayram, H. Sencar, N. Memon, I. Avcibas, Source camera identification based on CFA interpolation, in: International Conference on Image Processing (ICIP), vol. 3, IEEE, Genova, Italy, 2005, p. III-69.
[37] M.K. Johnson, H. Farid, Exposing digital forgeries by detecting inconsistencies in lighting, in: 7th Workshop on Multimedia and Security, ACM, Geneva, Switzerland, 2005, pp. 1–10.
[38] M.K. Johnson, H. Farid, Exposing digital forgeries in complex lighting environments, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 450–461.
[39] E. Kee, H. Farid, Exposing digital forgeries from 3-D lighting environments, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Seattle, WA, USA, 2010, pp. 1–6.
[40] M.K. Johnson, H. Farid, Detecting photographic composites of people, in: 6th International Workshop on Digital Watermarking (IWDW), Springer, Guangzhou, China, 2007, pp. 19–33.
[41] M.K. Johnson, H. Farid, Metric Measurements on a Plane from a Single Image, Technical Report TR2006-579, Department of Computer Science, Dartmouth College, 2006.
[42] W. Zhang, X. Cao, Z. Feng, J. Zhang, P. Wang, Detecting photographic composites using two-view geometrical constraints, in: International Conference on Multimedia and Expo (ICME), 2009, pp. 1078–1081.
[43] L. Li, S. Li, H. Zhu, S.-C. Chu, J.F. Roddick, J.-S. Pan, An efficient scheme for detecting copy-move forged images by Local Binary Patterns, J. Inf. Hiding Multimed. Signal Process. 4 (1) (2013) 46–56.
[44] B. Mahdian, S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, Forensic Sci. Int. 171 (2) (2007) 180–189.
[45] J.-W. Wang, G.-J. Liu, Z. Zhang, Y. Dai, Z. Wang, Fast and robust forensics for image region-duplication forgery, Acta Autom. Sin. 35 (12) (2009) 1488–1495.
[46] G. Liu, J. Wang, S. Lian, Z. Wang, A passive image authentication scheme for detecting region-duplication forgery with rotation, J. Netw. Comput. Appl. 34 (5) (2011) 1557–1565.
[47] S.-J. Ryu, M.-J. Lee, H.-K. Lee, Detection of copy–rotate–move forgery using Zernike moments, in: Information Hiding, Springer, Berlin, Heidelberg, 2010, pp. 51–65.
[48] S.-J. Ryu, M. Kirchner, M.-J. Lee, H.-K. Lee, Rotation invariant localization of duplicated image regions based on Zernike moments, IEEE Trans. Inf. Forensics Secur. 8 (8) (2013) 1355–1370.
[49] M.A. Qureshi, M. Deriche, A fast no reference image quality assessment using laws texture moments, in: Global Conference on Signal and Information Processing (GlobalSIP), IEEE, Atlanta, GA, USA, 2014, pp. 979–983.
[50] W. Luo, J. Huang, G. Qiu, Robust detection of region-duplication forgery in digital image, in: 18th International Conference on Pattern Recognition, (ICPR), vol. 4, IEEE, Hong Kong, 2006, pp. 746–749.
[51] H.-J. Lin, C.-W. Wang, Y.-T. Kao, et al., Fast copy-move forgery detection, WSEAS Trans. Signal Process. 5 (5) (2009) 188–197.
[52] V.K. Singh, R. Tripathi, Fast and efficient region duplication detection in digital images using sub-blocking method, Int. J. Adv. Sci. Technol. 35 (2011) 93–102.
[53] V. Christlein, C. Riess, E. Angelopoulou, On rotation invariance in copy-move forgery detection, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Seattle, WA, USA, 2010, pp. 1–6.
[54] S. Bravo-Solorio, A.K. Nandi, Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Process. 91 (8) (2011) 1759–1770.
[55] S. Bravo-Solorio, A.K. Nandi, Exposing duplicated regions affected by reflection, rotation and scaling, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Prague, Czech Republic, 2011, pp. 1880–1883.
[56] D.G. Lowe, Object recognition from local scale-invariant features, in: 7th International Conference on Computer Vision (ICCV), vol. 2, IEEE, Kerkyra, Greece, 1999, pp. 1150–1157.
[57] H. Huang, W. Guo, Y. Zhang, Detection of copy-move forgery in digital images using SIFT algorithm, in: Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA), vol. 2, IEEE, Wuhan, China, 2008, pp. 272–276.
[58] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, , G. Serra, Geometric tampering estimation by means of a sif-based forensic analysis, in: International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Dallas, TX, USA, Dallas, TX, USA, 2010, pp. 1702–1705.
[59] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy-move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1099–1110.
[60] X. Pan, S. Lyu, Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Secur. 5 (4) (2010) 857–867.
[61] X. Pan, S. Lyu, Detecting image region duplication using SIFT features, in: International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Dallas, TX, USA, 2010, pp. 1706–1709.
[62] M.A. Fischler, R.C. Bolles, Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography, Commun. ACM 24 (6) (1981) 381–395.

[63] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, G. Serra, Copy-move forgery detection and localization by means of robust clustering with J-Linkage, Signal Process.: Image Commun. 28 (6) (2013) 659–669.
[64] M. Jaberi, G. Bebis, M. Hussain, G. Muhammad, Accurate and robust localization of duplicated region in copy-move image forgery, Mach. Vis. Appl. 25 (2) (2014) 451–475.
[65] B. Shivakumar, S.S. Baboo, Detection of region duplication forgery in digital images using SURF, Int. J. Comput. Sci. Issues 8 (4) (2011) 199–205.
[66] B. Shivakumar, S.S. Baboo, Automated forensic method for copy-move forgery detection based on Harris Interest Points and SIFT descriptors, Int. J. Comput. Appl. 27 (3) (2011) 9–17.
[67] X. Bo, W. Junwen, L. Guangjie, D. Yuewei, Image copy-move forgery detection based on SURF, in: International Conference on Multimedia Information Networking and Security (MINES), IEEE, Nanjing, Jiangsu, China, 2010, pp. 889–892.
[68] E. Ardizzone, A. Bruno, G. Mazzola, Copy-move forgery detection via texture description, in: 2nd ACM Workshop on Multimedia in Forensics, Security and Intelligence, ACM, NY, USA, 2010, pp. 59–64.
[69] Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT-based detection of copy-move forgery in images, Forensic Sci. Int. 206 (1) (2011) 178–184.
[70] S. Khan, A. Kulkarni, Reduced time complexity for detection of copy-move forgery using discrete wavelet transform, Int. J. Comput. Appl. 6 (7) (2010) 31–36.
[71] M.K. Bashar, K. Noda, N. Ohnishi, H. Kudo, T. Matsumoto, Y. Takeuchi, Wavelet-based multiresolution features for detecting duplications in images, in: Conference on Machine Vision and Intelligence, 2007, pp. 264–267.
[72] S. Bayram, H.T. Sencar, N. Memon, An efficient and robust method for detecting copy-move forgery, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Taipei, Taiwan, 2009, pp. 1053–1056.
[73] G. Muhammad, M. Hussain, G. Bebis, Passive copy move image forgery detection using undecimated dyadic wavelet transform, Digit. Investig. 9 (1) (2012) 49–57.
[74] L. Li, S. Li, J. Wang, Copy-move forgery detection based on PHT, in: World Congress on Information and Communication Technologies (WICT), IEEE, Trivandrum, India, 2012, pp. 1061–1065.
[75] Y. Li, Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching, Forensic Sci. Int. 224 (1–3) (2013) 59–67.
[76] W. Li, N. Yu, Rotation robust detection of copy-move forgery, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 2113–2116.
[77] Q. Wu, S. Wang, X. Zhang, Detection of image region-duplication with rotation and scaling tolerance, in: International Conference on Computer and Computational Intelligence (ICCCI), Springer, Kaohsiung, Taiwan, 2010, pp. 100–108.
[78] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions, Technical Report TR2004-515, Department of Computer Science, Dartmouth College, Hanover, New Hampshire, 2004.
[79] M.K.V. Hulmukhe, N. KKWIEER, S. Sane, M.A.A. Borse, Exploring duplicated regions in natural images, in: International Conference in Computational Intelligence (ICCIA), 2012.
[80] M. Bashar, K. Noda, N. Ohnishi, K. Mori, Exploring duplicated regions in natural images, IEEE Trans. Image Process. (99) (2010) 1–40.
[81] X. Kang, S. Wei, Identifying tampered regions using singular value decomposition in digital image forensics, in: International Conference on Computer Science and Software Engineering, vol. 3, IEEE, Wuhan, China, 2008, pp. 926–930.
[82] Z. Ting, W. Rang-ding, Copy-move forgery detection based on svd in digital image, in: 2nd International Congress on and Signal Processing (CISP), IEEE, Tianjin, China, 2009, pp. 1–5.
[83] H.-C. Hsu, M.-S. Wang, Detection of copy-move forgery image using Gabor descriptor, in: International Conference on Anti-Counterfeiting, Security and Identification (ASID), IEEE, Taipei, Taiwan, 2012, pp. 1–4.
[84] F. Gharibi, J. RavanJamjah, F. Akhlaghian, B.Z. Azami, J. Alirezaie, Robust detection of copy-move forgery using texture features, in: 19th Iranian Conference on Electrical Engineering (ICEE), IEEE, Tehran, Iran, 2011, pp. 1–4.
[85] J. Zhang, Z. Feng, Y. Su, A new approach for detecting copy-move forgery in digital images, in: 11th International Conference on Communication Systems (ICCS), IEEE, Guangzhou, China, 2008, pp. 362–366.
[86] M. Zimba, S. Xingming, DWT-PCA (EVD) based copy-move image forgery detection, Int. J. Digit. Content Technol. Appl. 5 (1) (2011) 251–258.
[87] G. Li, Q. Wu, D. Tu, S. Sun, A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, in: International Conference on Multimedia and Expo (ICME), IEEE, Beijing, China, 2007, pp. 1750–1753.
[88] Y. Ke, R. Sukthankar, PCA-SIFT: a more distinctive representation for local image descriptors, in: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, (CVPR), vol. 2, IEEE, Washington, DC, USA, 2004, pp. II-506.
[89] M. Ghorbani, M. Firouzmand, A. Faraahi, DWT-DCT (QCD) based copy-move image forgery detection, in: 18th International Conference on Systems, Signals and Image Processing (IWSSIP), IEEE, Sarajevo, Bosnia, 2011, pp. 1–4.
[90] M. Zahra, Image duplication forgery detection using two robust features, Res. J. Recent Sci. 1 (12) (2012) 1–6.
[91] G. Muhammad, M.S. Hossain, Robust copy-move image forgery detection using undecimated wavelets and Zernike moments, in: 3rd International Conference on Internet Multimedia Computing and Service, ACM, Chengdu, China, 2011, pp. 95–98.
[92] J. Wang, G. Liu, H. Li, Y. Dai, Z. Wang, Detection of image region duplication forgery using model with circle block, in: International Conference on Multimedia Information Networking and Security (MINES), vol. 1, IEEE, Hubei, China, 2009, pp. 25–29.
[93] J.-W. Wang, G.-J. Liu, Z. Zhang, Y.-W. Dai, Z.-Q. Wang, Robust forensics for image regional duplication and forgery based on DWT and Zernike moment, Opt. Precis. Eng. 17 (7) (2009) 1687–1693.
[94] V. Christlein, C. Riess, E. Angelopoulou, A study on features for the detection of copy-move forgeries, in: SICHERHEIT, vol. 2010, 2010, pp. 105–116.
[95] A. Langille, M. Gong, An efficient match-based duplication detection algorithm, in: 3rd Canadian Conference on Computer and Robot Vision, IEEE, Quebec, Canada, 2006, pp. 64–64.
[96] C. Barnes, E. Shechtman, D.B. Goldman, A. Finkelstein, The generalized patchmatch correspondence algorithm, in: 11th European Conference on Computer Vision (ECCV), vol. 6313, Springer, Heraklion, Crete, Greece, 2010, pp. 29–43.
[97] C. Barnes, E. Shechtman, A. Finkelstein, D. Goldman, Patchmatch: a randomized correspondence algorithm for structural image editing, ACM Trans. Graph. 28 (3) (2009) 24:1–24:11.
[98] D. Cozzolino, G. Poggi, L. Verdoliva, Copy-move forgery detection based on patchmatch, in: International Conference on Image Processing (ICIP), IEEE, Paris, France, 2014, pp. 5312–5316.
[99] M.A. Sekeh, M.A. Maarof, M.F. Rohani, B. Mahdian, Efficient image duplicated region detection model using sequential block clustering, Digit. Investig. 10 (1) (2013) 73–84.
[100] M. Zandi, A. Mahmoudi-Aznaveh, A. Mansouri, Adaptive matching for copy-move forgery detection, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Atlanta, GA, USA, 2014, pp. 119–124.
[101] T.-T. Ng, S.-F. Chang, A model for image splicing, in: International Conference on Image Processing (ICIP), vol. 2, IEEE, Singapore, 2004, pp. 1169–1172.
[102] T.-T. Ng, S.-F. Chang, Q. Sun, A Data Set of Authentic and Spliced Image Blocks, Columbia University, ADVENT Technical Report, 2004, pp. 203–204.
[103] T.-T. Ng, S.-F. Chang, Q. Sun, Blind detection of photomontage using higher order statistics, in: International Symposium on Circuits and Systems (ISCAS), vol. 5, IEEE, Vancouver, BC, Canada, 2004, pp. 688–691.
[104] D. Fu, Y.Q. Shi, W. Su, Detection of image splicing based on Hilbert–Huang transform and moments of characteristic functions with wavelet decomposition, in: 5th International Workshop on Digital Watermarking, vol. 4283, Springer, Jeju Island, Korea, 2006, pp. 177–187.
[105] X. Li, T. Jing, X. Li, Image splicing detection based on moment features and Hilbert–Huang transform, in: International Conference on Information Theory and Information Security (ICITIS), IEEE, Beijing, China, 2010, pp. 1127–1130.
[106] J. Dong, W. Wang, T. Tan, Y.Q. Shi, Run-length and edge statistics based approach for image splicing detection, in: 7th International Workshop on Digital Watermarking (IWDW), vol. 5450, Springer, Berlin, Heidelberg, 2009, pp. 76–87.
[107] Z. He, W. Sun, W. Lu, H. Lu, Digital image splicing detection based on approximate run length, Pattern Recognit. Lett. 32 (12) (2011) 1591–1597.
[108] W. Chen, Y.Q. Shi, W. Su, Image splicing detection using 2-d phase congruency and statistical moments of characteristic function, in:

Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 6505, Citeseer, San Jose, CA, USA, 2007.
[109] Y.Q. Shi, C. Chen, W. Chen, A natural image model approach to splicing detection, in: 9th Workshop on Multimedia & Security, ACM, 2007, pp. 51–62.
[110] Y.Q. Shi, C. Chen, W. Chen, A Markov process based approach to effective attacking JPEG steganography, in: 8th International Workshop on Information Hiding, vol. 4437, Springer, Alexandria, VA, USA, 2007, pp. 249–264.
[111] Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, C. Chen, Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network, in: International Conference on Multimedia and Expo (ICME), IEEE, Amsterdam, Netherlands, 2005.
[112] X. Zhao, S. Wang, S. Li, J. Li, A comprehensive study on third order statistical features for image splicing detection, in: 10th International Workshop on Digital Forensics and Watermarking, vol. 7128, Springer, Atlantic City, NY, USA, 2012, pp. 243–256.
[113] Y. Zhang, C. Zhao, Y. Pi, S. Li, Revealing image splicing forgery using Local Binary Patterns of DCT coefficients, in: International Conference on Communications, Signal Processing, and Systems, vol. 202, Springer, Gold Coast, Australia, 2012, pp. 181–189.
[114] Z. He, W. Lu, W. Sun, J. Huang, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognit. 45 (12) (2012) 4292–4299.
[115] C. Chen, Y.Q. Shi, JPEG image steganalysis utilizing both intrablock and interblock correlations, in: International Symposium on Circuits and Systems (ISCAS), IEEE, Seattle, WA, USA, 2008, pp. 3029–3032.
[116] A. Srivastava, A.B. Lee, E.P. Simoncelli, S.-C. Zhu, On advances in statistical modeling of natural images, J. Math. Imaging Vis. 18 (1) (2003) 17–33.
[117] I. Guyon, J. Weston, S. Barnhill, V. Vapnik, Gene selection for cancer classification using support vector machines, Mach. Learn. 46 (1–3) (2002) 389–422.
[118] E.-S.M. El-Alfy, M.A. Qureshi, Combining spatial and DCT based markov features for enhanced blind detection of image splicing, Pattern Anal. Appl. 18 (3) (2014) 713–723.
[119] W. Wang, J. Dong, T. Tan, Effective image splicing detection based on image chroma, in: 16th International Conference on Image Processing (ICIP), IEEE, San Diego, CA, USA, 2009, pp. 1257–1260.
[120] W. Wang, J. Dong, T. Tan, Image tampering detection based on stationary distribution of Markov chain, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 2101–2104.
[121] X. Zhao, J. Li, S. Li, S. Wang, Detecting digital image splicing in chroma spaces, in: Digital Watermarking, Springer, Seoul, Korea, 2011, pp. 12–22.
[122] G. Muhammad, M.H. Al-Hammadi, M. Hussain, G. Bebis, Image forgery detection using steerable pyramid transform and local binary pattern, Mach. Vis. Appl. 25 (4) (2014) 985–995.
[123] P. Sutthiwan, Y.-Q. Shi, J. Dong, T. Tan, T.-T. Ng, New developments in color image tampering detection, in: International Symposium on Circuits and Systems (ISCAS), IEEE, Paris, France, 2010, pp. 3064–3067.
[124] P. Sutthiwan, Y.Q. Shi, W. Su, T.-T. Ng, Rake transform and edge statistics for image forgery detection, in: International Conference on Multimedia and Expo (ICME), IEEE, Suntec City, Singapore, 2010, pp. 1463–1468.
[125] W. Lu, W. Sun, F.-L. Chung, H. Lu, Revealing digital fakery using multiresolution decomposition and higher order statistics, Eng. Appl. Artif. Intell. 24 (4) (2011) 666–672.
[126] S.Q. Saleh, M. Hussain, G. Muhammad, G. Bebis, Evaluation of image forgery detection using multi-scale weber local descriptors, in: 9th International Symposium on Advances in Visual Computing (ISVC), vol. 8034, Springer, Rethymnon, Crete, Greece, 2013, pp. 416–424.
[127] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, et al., Splicing image forgery detection based on DCT and Local Binary Pattern, in: Global Conference on Signal and Information Processing (GlobalSIP), IEEE, Austin, TX, USA, 2013, pp. 253–256.
[128] Z. Moghaddasi, H.A. Jalab, R. Md Noor, S. Aghabozorgi, Improving RLRN image splicing detection with the use of PCA and Kernel PCA, Sci. World J. (2014), http://dx.doi.org/10.1155/2014/606570.
[129] J. Zhang, Y. Zhao, Y. Su, A new approach merging markov and DCT features for image splicing detection, in: International Conference on Intelligent Computing and Intelligent Systems (ICIS), vol. 4, IEEE, Shanghai, China, 2009, pp. 390–394.
[130] I. Amerini, R. Becarelli, R. Caldelli, A.D. Mastio, Splicing forgeries localization through the use of first digit features, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Atlanta, GA, USA, 2014, pp. 143–148.
[131] J. Lukáš, J. Fridrich, M. Goljan, Detecting digital image forgeries using sensor pattern noise, Proc. SPIE 6072 (2006) 362–372.
[132] G. Chierchia, S. Parrilli, G. Poggi, C. Sansone, L. Verdoliva, On the influence of denoising in PRNU based forgery detection, in: 2nd ACM workshop on Multimedia in Forensics, Security and Intelligence (MiFOR), ACM, Firenze, Italy, 2010, pp. 117–122.
[133] G. Chierchia, G. Poggi, C. Sansone, L. Verdoliva, PRNU-based forgery detection with regularity constraints and global optimization, in: 15th International Workshop on Multimedia Signal Processing (MMSP), IEEE, Pula, Croatia, 2013, pp. 236–241.
[134] P. Kakar, N. Sudha, W. Ser, Exposing digital image forgeries by detecting discrepancies in motion blur, IEEE Trans. Multimed. 13 (3) (2011) 443–452.
[135] K. Bahrami, A.C. Kot, J. Fan, Splicing detection in out-of-focus blurred images, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Guangzhou, China, 2013, pp. 144–149.
[136] IEEE Information Forensics and Security Technical Committee (IFS-TC) ⟨http://ifc.recod.ic.unicamp.br/fc.website/index.py?sec=0⟩, 2013.
[137] D. Cozzolino, D. Gragnaniello, L. Verdoliva, Image forgery detection through residual-based local descriptors and block-matching, in: International Conference on Image Processing (ICIP), IEEE, Paris, France, 2014, pp. 5297–5301.
[138] D. Cozzolino, D. Gragnaniello, L. Verdoliva, Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques, in: International Conference on Image Processing (ICIP), IEEE, Paris, France, 2014, pp. 5302–5306.
[139] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro, Multi-Clue image tampering localization, in: International Workshop on Information Forensics and Security (WIFS), IEEE, 2014, pp. 125–130.
[140] Z. Dias, A. Rocha, S. Goldenstein, Image phylogeny by minimal spanning trees, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 774–788.
[141] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting traces of resampling, IEEE Trans. Signal Process. 53 (2) (2005) 758–767.
[142] A.C. Gallagher, Detection of linear and cubic interpolation in JPEG compressed images, in: 2nd Canadian Conference on Computer and Robot Vision, IEEE, Victoria, BC, Canada, 2005, pp. 65–72.
[143] S. Prasad, K. Ramakrishnan, On resampling detection and its application to detect image tampering, in: International Conference on Multimedia and Expo (ICME), IEEE, Toronto, Canada, 2006, pp. 1325–1328.
[144] M. Kirchner, Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue, in: 10th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2008, pp. 11–20.
[145] M. Kirchner, T. Gloe, On resampling detection in re-compressed images, in: 1st International Workshop on Information Forensics and Security (WIFS), IEEE, London, UK, 2009, pp. 21–25.
[146] M. Kirchner, Linear row and column predictors for the analysis of resized images, in: 12th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2010, pp. 13–18.
[147] M. Kirchner, On the detectability of local resampling in digital images, in: Electronic Imaging, vol. 6819, International Society for Optics and Photonics, San Jose, CA, USA, 2008, pp. 68190F-7.
[148] B. Mahdian, S. Saic, On periodic properties of interpolation and their application to image authentication, in: 3rd International Symposium on Information Assurance and Security (IAS), IEEE, Manchester, UK, 2007, pp. 439–446.
[149] W. Weimin, W. Shuozhong, T. Zhenjun, Estimation of rescaling factor and detection of image splicing, in: 11th International Conference on Communication Technology (ICCT), IEEE, Hangzhou, China, 2008, pp. 676–679.
[150] N. Dalgaard, C. Mosquera, F. Pérez-González, On the role of differentiation for resampling detection, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 1753–1756.
[151] G.-S. Song, Y.-I. Yun, W.-H. Lee, A new estimation approach of resampling factors using threshold-based peak detection, in: International Conference on Consumer Electronics (ICCE), IEEE, Berlin, Germany, 2011, pp. 731–732.
[152] B. Mahdian, S. Saic, Blind authentication using periodic properties of interpolation, IEEE Trans. Inf. Forensics Secur. 3 (3) (2008) 529–538.

[153] B. Mahdian, S. Saic, Detection and description of geometrically transformed digital images, in: Media Forensics and Security, Proceedings of SPIE Electronic Imaging, vol. 7254, International Society for Optics and Photonics, San Jose, CA, USA, 2009, pp. 1–10.
[154] B. Mahdian, S. Saic, A cyclostationarity analysis applied to image forensics, in: Workshop on Applications of Computer Vision (WACV), IEEE, Snowbird, Utah, 2009, pp. 1–6.
[155] D. Vázquez-Padín, C. Mosquera, F. Pérez-González, Two-dimensional statistical test for the presence of almost cyclostationarity on images, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 1745–1748.
[156] D. Vazquez-Padin, F. Perez-Gonzalez, Prefilter design for forensic resampling estimation, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Iguacu Falls, Brazil, 2011, pp. 1–6.
[157] B. Mahdian, S. Saic, Detection of resampling supplemented with noise inconsistencies analysis for image forensics, in: International Conference on Computational Sciences and Its Applications (ICCSA), IEEE, Perugia, Umbria, Italy, 2008, pp. 546–556.
[158] X. Feng, I.J. Cox, G. Doërr, Normalized energy density-based forensic detection of resampled images, IEEE Trans. Multimed. 14 (3) (2012) 536–545.
[159] S. Pfennig, M. Kirchner, Spectral methods to determine the exact scaling factor of resampled digital images, in: 5th International Symposium on Communications Control and Signal Processing (ISCCSP), IEEE, Rome, Italy, 2012, pp. 1–6.
[160] H. Gou, A. Swaminathan, M. Wu, Intrinsic sensor noise features for forensic analysis on scanners and scanned images, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 476–491.
[161] H. Cao, A.C. Kot, Identification of recaptured photographs on LCD screens, in: International Conference on Acoustics Speech and Signal Processing (ICASSP), IEEE, Dallas, TX, USA, 2010, pp. 1790–1793.
[162] H. Muammar, P.L. Dragotti, An investigation into aliasing in images recaptured from an lcd monitor using a digital camera, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Vancouver, BC, Canada, 2013, pp. 2242–2246.
[163] T. Thongkamwitoon, H. Muammar, P.-L. Dragotti, An image recapture detection algorithm based on learning dictionaries of edge profiles, IEEE Trans. Inf. Forensics Secur. 10 (5) (2015) 953–968.
[164] M. Visentini-Scarzanella, P.L. Dragotti, Modelling radial distortion chains for video recapture detection, in: 15th International Workshop on Multimedia Signal Processing (MMSP), IEEE, Pula, Croatia, 2013, pp. 412–417.
[165] N. Khanna, G.T.-C. Chiu, J.P. Allebach, E.J. Delp, Forensic techniques for classifying scanner, computer generated and digital camera images, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Las Vegas, NV, USA, 2008, pp. 1653–1656.
[166] D.-T. Dang-Nguyen, G. Boato, F.G. De Natale, Discrimination between computer generated and natural human faces based on asymmetry information, in: 20th European Signal Processing Conference (EUSIPCO), IEEE, Bucharest, Romania, 2012, pp. 1234–1238.
[167] F. Peng, J.-t. Li, M. Long, Identification of natural images and computer-generated graphics based on statistical and textural features, J. Forensic Sci. 60 (2) (2015) 435–443.
[168] A. Criminisi, P. Pérez, K. Toyama, Region filling and object removal by exemplar-based image inpainting, IEEE Trans. Image Process. 13 (9) (2004) 1200–1212.
[169] S. Das, G.D. Shreyas, L.D. Devan, Blind detection method for video inpainting forgery, Int. J. Comput. Appl. 60 (11) (2012) 33–37.
[170] I.-C. Chang, J.C. Yu, C.-C. Chang, A forgery detection algorithm for exemplar-based inpainting images using multi-region relation, Image Vis. Comput. 31 (1) (2013) 57–71.
[171] Z. Liang, G. Yang, X. Ding, L. Li, An efficient forgery detection algorithm for object removal by exemplar-based image inpainting, J. Visual Commun. Image Represent 30 (2015) 75–85.
[172] Y.Q. Zhao, M. Liao, F.Y. Shih, Y.Q. Shi, Tampered region detection of inpainting JPEG images, Optik-Int. J. Light Electron Opt. 124 (16) (2013) 2487–2492.
[173] D.T. Trung, A. Beghdadi, M.-C. Larabi, Blind inpainting forgery detection, in: Global Conference on Signal and Information Processing (GlobalSIP), IEEE, Atlanta, GA, USA, 2014, pp. 1019–1023.
[174] H. Gunes, M. Piccardi, Assessing facial beauty through proportion analysis by image processing and supervised learning, Int. J. Human–Comput. Stud. 64 (12) (2006) 1184–1199.
[175] A. Dantcheva, J. Dugelay, Female facial aesthetics based on soft biometrics and photo-quality, in: International Conference for Multimedia and Expo (ICME), IEEE, Barcelona, Spain, 2011.
[176] X.-F. Li, X.-J. Shen, H.-P. Chen, Blind identification algorithm for retouched images based on Bi-Laplacian, J. Comput. Appl. 31 (1) (2011) 239–242.
[177] E. Kee, H. Farid, A perceptual metric for photo retouching, Proc. Natl. Acad. Sci. 108 (50) (2011) 19907–19912.
[178] D. Xie, L. Liang, L. Jin, J. Xu, M. Li, Scut-fbp: a benchmark dataset for facial beauty perception ⟨http://www.hcii-lab.net/data/SCUT-FBP/⟩, Accessed: 2015-06-14, 2015.
[179] M. Kirchner, J. Fridrich, On detection of median filtering in digital images, in: IS&T/SPIE Electronic Imaging, vol. 7541, International Society for Optics and Photonics, San Jose, CA, USA, 2010, pp. 754110–754110-12.
[180] T. Pevny, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE Trans. Inf. Forensics Secur. 5 (2) (2010) 215–224.
[181] G. Cao, Y. Zhao, R. Ni, L. Yu, H. Tian, Forensic detection of median filtering in digital images, in: International Conference on Multimedia and Expo (ICME), IEEE, Suntec City, Singapore, 2010, pp. 89–94.
[182] H.-D. Yuan, Blind forensics of median filtering in digital images, IEEE Trans. Inf. Forensics Secur. 6 (4) (2011) 1335–1345.
[183] X. Kang, M.C. Stamm, A. Peng, K.R. Liu, Robust median filtering forensics using an autoregressive model, IEEE Trans. Inf. Forensics Secur. 8 (9) (2013) 1456–1468.
[184] M. Stamm, K.R. Liu, Blind forensics of contrast enhancement in digital images, in: 15th International Conference on Image Processing (ICIP), IEEE, San Diego, CA, USA, 2008, pp. 3112–3115.
[185] M.C. Stamm, K.R. Liu, Forensic estimation and reconstruction of a contrast enhancement mapping, in: International Conference on Acoustics Speech and Signal Processing (ICASSP), IEEE, Dallas, TX, USA, 2010, pp. 1698–1701.
[186] M.C. Stamm, K.R. Liu, Forensic detection of image manipulation using statistical intrinsic fingerprints, IEEE Trans. Inf. Forensics Secur. 5 (3) (2010) 492–506.
[187] S.D. Mahalakshmi, K. Vijayalakshmi, S. Priyadharsini, Digital image forgery detection and estimation by exploring basic image manipulations, Digit. Investig. 8 (3) (2012) 215–225.
[188] G. Cao, Y. Zhao, R. Ni, X. Li, Contrast enhancement-based forensics in digital images, IEEE Trans. Inf. Forensics Secur. 9 (3) (2014) 515–525.
[189] H.-D. Yuan, Identification of global histogram equalization by modeling gray-level cumulative distribution, in: China Summit & International Conference on Signal and Information Processing (ChinaSIP), IEEE, Beijing, China, 2013, pp. 645–649.
[190] G. Cao, Y. Zhao, R. Ni, Forensic estimation of gamma correction in digital images, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 2097–2100.
[191] G. Cao, Y. Zhao, R. Ni, Detection of image sharpening based on histogram aberration and ringing artifacts, in: International Conference on Multimedia and Expo (ICME), IEEE, New York, NY, USA, 2009, pp. 1026–1029.
[192] G. Cao, Y. Zhao, R. Ni, A.C. Kot, Unsharp masking sharpening detection via overshoot artifacts analysis, IEEE Signal Process. Lett. 18 (10) (2011) 603–606.
[193] F. Ding, G. Zhu, Y.Q. Shi, A novel method for detecting image sharpening based on local binary pattern, in: Digital-Forensics and Watermarking, Springer, Auckland, New Zealand, 2014, pp. 180–191.
[194] F. Ding, G. Zhu, J. Yang, J. Xie, Y.-Q. Shi, Edge perpendicular binary coding for USM sharpening detection, IEEE Signal Process. Lett. 22 (2015) 327–331.
[195] G. Cao, Y. Zhao, R. Ni, B. Ou, Y. Wang, Forensic detection of noise addition in digital images, J. Electron. Imaging 23 (2) (2014) 023004.
[196] M.C. Stamm, X. Chu, K.R. Liu, Forensically determining the order of signal processing operations, in: International Workshop on Information Forensics and Security (WIFS), IEEE, Guangzhou, China, 2013, pp. 162–167.
[197] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy-move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Secur. 6 (3 PART 2) (2011) 1099–1110.
[198] Y.-F. Hsu, S.-F. Chang, Detecting image splicing using geometry invariants and camera characteristics consistency, in: International Conference on Multimedia and Expo (ICME), 2006, pp. 549–552.

[199] R. Böhme, M. Kirchner, Counter-forensics: attacking image forensics, in: Digital Image Forensics, Springer, New York, 2013, pp. 327–366.
[200] M. Kirchner, Notes on digital image forensics and counter-forensics (Ph.D. thesis), Dartmouth College, 2012.
[201] G. Cao, Y. Zhao, R. Ni, H. Tian, Anti-forensics of contrast enhancement in digital images, in: 12th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2010, pp. 25–34.
[202] C.-W. Kwok, O.C. Au, S.-H. Chui, Alternative anti-forensics method for contrast enhancement, in: Digital Forensics and Watermarking, vol. 7128, Springer, Atlantic City, NY, USA, 2012, pp. 398–410.
[203] L. Laijie, Y. Gaobo, X. Ming, Anti-forensics for unsharp masking sharpening in digital images, Int. J. Digit. Crime Forensics 5 (3) (2013) 53–65.
[204] Z.-H. Wu, M.C. Stamm, K.R. Liu, Anti-forensics of median filtering, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Vancouver, BC, Canada, 2013, pp. 3043–3047.
[205] M.C. Stamm, K. Liu, Anti-forensics of digital image compression, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1050–1065.
[206] M.C. Stamm, S.K. Tjoa, W.S. Lin, K. Liu, Undetectable image tampering through JPEG compression anti-forensics, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 2109–2112.
[207] W. Fan, K. Wang, F. Cayre, Z. Xiong, A variational approach to JPEG anti-forensics, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Vancouver, BC, Canada, 2013, pp. 3058–3062.
[208] W. Fan, K. Wang, F. Cayre, Z. Xiong, JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality, IEEE Trans. Inf. Forensics Secur. 9 (8) (2014) 1211–1226.
[209] H. Li, W. Luo, J. Huang, Countering anti-JPEG compression forensics, in: 19th International Conference on Image Processing (ICIP), IEEE, Orlando, FL, USA, 2012, pp. 241–244.
[210] G. Valenzise, M. Tagliasacchi, S. Tubaro, The cost of JPEG compression anti-forensics, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Prague, Czech Republic, 2011, pp. 1884–1887.
[211] M.C. Stamm, K. Liu, Wavelet-based image compression anti-forensics, in: 17th International Conference on Image Processing (ICIP), IEEE, Hong Kong, 2010, pp. 1737–1740.
[212] M. Kirchner, R. Böhme, Hiding traces of resampling in digital images, IEEE Trans. Inf. Forensics Secur. 3 (4) (2008) 582–592.
[213] T. Gloe, M. Kirchner, A. Winkler, R. Böhme, Can we trust digital image forensics? in: 15th International Conference on Multimedia, ACM, Augsburg, Bavaria, Germany, 2007, pp. 78–86.
[214] R. Böhme, M. Kirchner, Synthesis of color filter array pattern in digital images, Proc. SPIE, Media Forensics Secur. XI, 7254 (2009) 18–22.
[215] A. Rocha, W. Scheirer, T. Boult, S. Goldenstein, Vision of the unseen: current trends and challenges in digital image and video forensics, ACM Comput. Surv. 43 (4) (2011) 26:1–26:42.
[216] G. Cao, Y. Zhao, R. Ni, H. Tian, Anti-forensics of contrast enhancement in digital images, in: 12th ACM Workshop on Multimedia and Security, ACM, New York, NY, USA, 2010, pp. 25–34.
[217] M. Fontani, A. Bonchi, A. Piva, M. Barni, Countering anti-forensics by means of data fusion, in: IS&T/SPIE Electronic Imaging, vol. 9028, International Society for Optics and Photonics, San Francisco, CA, USA, 2014, pp. 90280Z-90280Z–15.
[218] G. Valenzise, V. Nobile, M. Tagliasacchi, S. Tubaro, Countering JPEG anti-forensics, in: 18th International Conference on Image Processing (ICIP), IEEE, Brussels, Belgium, 2011, pp. 1949–1952.
[219] G. Valenzise, M. Tagliasacchi, S. Tubaro, Revealing the traces of JPEG compression anti-forensics, IEEE Trans. Inf. Forensics Secur. 8 (2) (2013) 335–349.
[220] S. Lai, R. Böhme, Countering counter-forensics: the case of JPEG compression, in: 13th International Conference on Information Hiding, vol. 6958, Springer, Prague, Czech Republic, 2011, pp. 285–298.
[221] G. Cao, Y. Zhao, R. Ni, Forensic identification of resampling operators: a semi non-intrusive approach, Forensic Sci. Int. 216 (1) (2012) 29–36.
[222] H. Zeng, T. Qin, X. Kang, L. Liu, Countering anti-forensics of median filtering, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Florence, Italy, 2014, pp. 2704–2708.
[223] A. De Rosa, M. Fontani, M. Massai, A. Piva, M. Barni, Second-order statistics analysis to cope with contrast enhancement counter-forensics, IEEE Signal Process. Lett. 22 (8) (2015) 1132–1136.
[224] A. Costanzo, I. Amerini, R. Caldelli, M. Barni, Forensic analysis of SIFT keypoint removal and injection, IEEE Trans. Inf. Forensics Secur. 9 (9) (2014) 1450–1464.
[225] I. Amerini, F. Battisti, R. Caldelli, M. Carli, A. Costanzo, Exploiting perceptual quality issues in countering sift-based forensic methods, in: International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Florence, Italy, 2014, pp. 2664–2668.
[226] F. Battisti, M. Carli, A. Neri, Image forgery detection by means of no-reference quality metrics, in: IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics, Burlingame, CA, USA, 2012, p. 83030K.
[227] Trung Thanh Dang, Azeddine Beghdadi, M-C Larabi, A perceptual image completion approach based on a hierarchical optimization scheme, Signal Processing 103 (2014) 127–141.
[228] Trung Thanh Dang, Azeddine Beghdadi, Mohamed-Chaker Larabi, Perceptual quality assessment for color image inpainting, in: 20th International Conference on Image Processing (ICIP), IEEE, Melbourne, Australia, 2013, pp. 398–402.
[229] Mohamed Deriche, An Image Quality Index Based on Mutual Information and Neural Networks, Arabian Journal for Science and Engineering 39 (3) (2014) 1983–1993.