Image Forgery Detection: Survey and Future Directions

Chapter · April 2019

DOI: 10.1007/978-981-13-6351-1_14

2 authors:

Kunj Bihari Meena
Jaypee University of Engineering and Technology
7 PUBLICATIONS **21** CITATIONS

SEE PROFILE

Vipin Tyagi
Jaypee University of Engineering and Technology
102 PUBLICATIONS **849** CITATIONS

SEE PROFILE

Image Forgery Detection: Survey and Future Directions

Kunj Bihari Meena and Vipin Tyagi

1 Introduction

One famous proverb says "A picture is worth a thousand words". Now everybody understands the essence of this idiom. But due to the availability of sophisticated tools for image manipulation, it is very easy to tamper the image by anyone with a modicum of computer skills. Hence, authenticity of image is challenged openly, therefore somewhere the above idiom loses its essence.

According to Merriam-Webster dictionary, digital image forgery is defined as "falsely and fraudulently altering a digital image". Image forgery is not a new concept; it started way back in 1840. French photographer Hippolyte Bayard created the first tampered image (Fig. 1) entitled with, "Self Portrait as a Drowned Man", in which, Bayard has professed to commit suicide [1].

More than a century ago, during American Civil War, a photo of American commanding general, General Ulysses S. Grant came into existence, which claimed that General Grant was sitting on horseback in front of his troops, at City Point, Virginia [2]. Later on, it has been found that image was not authentic; rather it was a composite of three images formed using negatives of the photographs.

Almost a decade ago, Iran has been accused of doctoring an image from its missile tests; the image [3] was released on the official website, Iran's Revolutionary Guard, which claimed that four missiles were heading skyward simultaneously. Recently, in July 2017, a fake image of Russian president Vladimir Putin was circulated over the social media related to the meeting with American president Donald Trump during the G20 summit 2017. This faked image garnered several thousand likes and retweets [4].

K. B. Meena · V. Tyagi (✉)
Jaypee University of Engineering and Technology, Raghogarh, Guna, MP, India
e-mail: dr.vipin.tyagi@gmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_14

Fig. 1 First fake image [1]

Image has remarkable role in various areas such as forensic investigation, criminal investigation, surveillance systems, intelligence system, sports, legal services, medical imaging, insurance claim, and journalism.

Substantial amount of research has been carried out in the last one decade in the field of forgery detection. Figure 2 shows the bar chart of a number of publications versus four types of image forgery detection techniques (copy-move, image splicing, resampling, retouching) for last two decades, over the years 1998–2017, collected from Google Scholar. Few observations from this bar chart are: startling growth has been seen in copy-move forgery detection in last one decade, and a significant focus is also given on image splicing detection in the last one decade over the first decade. However, less focus was given on retouching detection, one reason behind this may be that retouching is the least pernicious type forgery because generally, retouched images are not used for illegal purposes.

Forgery detection techniques are broadly categorized into two categories; active (non-blind, Fig. 3) and passive (blind) [5]. Active forgery detection techniques need some prior information about the image which may have been embedded in the image at the time of capturing the image or during image acquisition or later stages. Digital watermarking [6–8] and digital signature [9, 10] are the examples of active forgery detection techniques, and these approaches can be used to test the authenticity of the

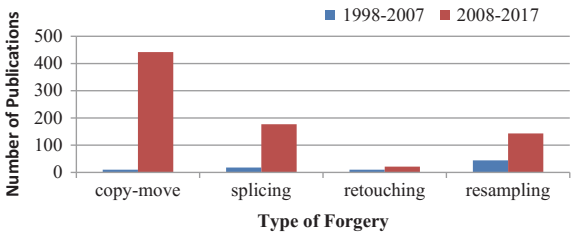

Fig. 2 Number of publications in the field of image forensics over the last two decades

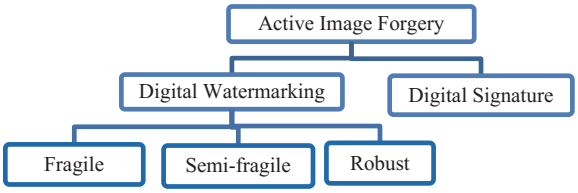

Fig. 3 Active image forgery detection techniques

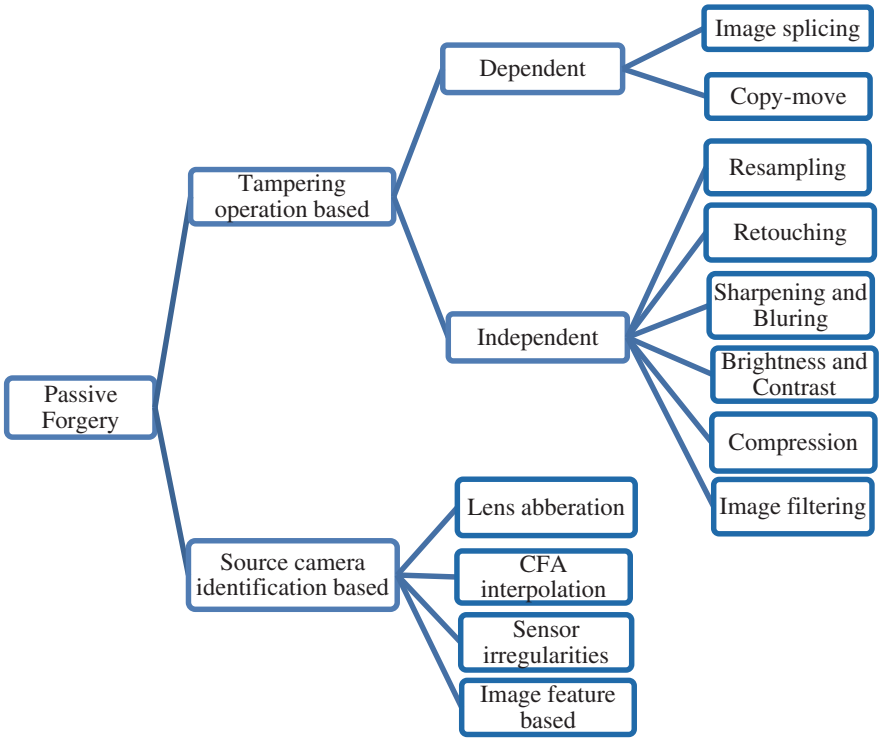

Fig. 4 Classification of passive forgery detection techniques

image based on embedded information. On the basis of application, digital watermarking further can be categorized as fragile, semi-fragile, and robust watermarking [11]. In practicality, it is very rare that images produced for forensic investigation like fingerprint images, crime scene images, photographs of criminals, etc., would contain the watermark or signature, hence it can be concluded that active forgery detection techniques are not useful for forensic investigation of digital images.

On the contrary, passive forgery detection techniques do not need any prior knowledge about the image; rather these techniques identify manipulations by extracting intrinsic features of the image on the basis of the type of doctoring or photo-capturing

device identification. Passive forgery further can be classified (Fig. 4) as dependent forgery and independent forgery. In dependent forgery, either tampering can be done in the same image by copying and pasting (cloning) [12] some area within the image or more than one image can be combined (image splicing) [13–15] to get convincing composite. On the other hand, independent forgery is the forgery in which some properties of the same image are manipulated. An example of independent forgery includes resampling, retouching, image rotation, scaling, resizing, addition of noise, blurring, image compression, etc. No involvement of prior knowledge about image makes passive forgery more practical in real life.

2 Existing Surveys

In the last decade, many surveys have been carried out on image forgery detection. Lanh et al. [16] discussed various techniques to detect image forgery based on camera. They have given conclusive remark that camera-based techniques are better than other forgery detection techniques, in terms of reliability. Farid [17], categorized image forgery tools into five groups, pixel-based techniques, format-based techniques, camera-based techniques, physically based techniques, and geometric-based. He has elaborated each method in detail. Recently, Warif et al. [18], reviewed copy-move forgery detection techniques. They have categorized copy-move forgery detection mainly into two classes: block-based and keypoint-based approach. Table 1 shows existing survey papers available on Google Scholar during 2007–2017.

Detailed classification of forgery detection methods is shown in Fig. 4, wherein blind forgery detection techniques have been categorized as tampering detection based and source camera identification based techniques. Tampering detection techniques have been discussed in this paper. For complete survey on source camera identification based techniques, readers may refer to [16, 23, 24].

3 Tampering Detection Techniques

In context to digital image, tampering means any manipulation or alteration in image to change its semantic meaning for illegal or unauthorized purposes. A tremendous amount of images are produced before digital image forensic for investigating whether the image is authentic (no alteration in semantic meaning of image) or tampered. Since photo-editing tools are becoming increasingly ubiquitous, anybody can tamper with the image and may use it with malicious intention. Figure 4 shows various tampering detection techniques.

In this section, four major types of tampering detection techniques (image splicing, copy-move forgery, image resampling, image retouching detection) are presented. Out of these four tampering detection techniques, first two are exploited for detecting

Table 1 Existing survey papers available on Google scholar

S. n.	Author(s)	Contribution	Observations
1	Lanh et al. [16]	Reviewed various techniques in digital camera image forensics	• Intrinsic features based methods of camera hardware are more reliable and better in terms of accuracy as compared to methods based on other camera software parts • Camera identification methods outperform as compared to other forgery detection methods • Hardware dependent characteristics such as aberration and CRF are potentially more reliable than methods based on scene content like lighting and image statistics
2	Farid [17]	Categorized the image forgery detection techniques into five groups (pixel-based, format-based, camera-based, physically based and geometric-based)	• Some forensic tools may not detect advanced forgeries but other forgery detection techniques are much reliable to challenge image fakery • Due to the advancement of image manipulation tools, an arms race between the forger and forensic analyst is inescapable
3	Mahdian and Saic [19]	Reviewed various method based on blind image forgery	• Existing methods produce considerably higher false positive rates than which are reported in the existing papers • Existing methods are not fully automated, need human interpretation • Need to develop more reliable and robust methods
4	Christlein et al. [12]	Reviewed state of the art approaches pertaining to copy-move forgery	• Keypoint-based methods better than block-based methods in term of performance (execution time), however, block-based methods give better detection accuracy
5	Birajdar and Mankar [20]	Reviewed forgery detection techniques with more emphasis on passive tampering detection	• Existing methods are not automated, outputs need a human interpretation • Existing methods are not effective when small regions are copy-moved • Copy-move forgery detection, have shown high time complexity and false positives • Need to extend forgery detection on audio and video

(continued)

Table 1 (continued)

S. n.	Author(s)	Contribution	Observations
6	Qazi et al. [21]	Surveyed various blind forgery detection techniques and classified into mainly three groups (copy-move, splicing, and retouching)	• DCT and PCA based techniques, exhibit high computational complexity and low accuracy rate • DCT-based techniques are not effective when considering highly textured and small forged regions
7	Ansari et al. [22]	Various approaches of pixel-based image forgery detection have been reviewed	• Some algorithms are unable to detect forgery effectively. Some are having high time complexity • Need to develop an efficient and accurate image forgery detection algorithm
8	Warif et al. [18]	CMFD techniques are organized into two approaches, namely: block-based and keypoint-based	• Existing techniques are not fit to solve real-world big data problems • To increase processing speed, dimension reduction techniques like PCA, DWT, and SVD has been suggested • Keypoint-based methods like SIFT and SURF are more reliable when geometrical transformation operations are taken into consideration

dependent forgery and the last two tampering detection techniques are used for examining independent forgery.

3.1 Image Splicing Detection or Photo Composite Detection

In image splicing forgery, some part of image is copied and pasted on the other image to get forged image (Fig. 5). Image splicing is a basic step to create a photomontage from a set of images. To make composite image more realistic, postprocessing (scaling, cropping, retouching, rotating, etc.) operation may be applied on each of the components, furthermore, after performing splicing operation, again postprocessing operation can be applied to hide any discernible effects.

Although experts can identify image splicing forgery by just looking a forged image, in some cases. However, experienced forger can make composite image so elegant that it is almost impossible to say anything about the genuineness of an image, merely by looking at the image. When image splicing operation is carried out, some image statistics get disarranged. However, these statistical changes may not be perceptible to the human visual system. These statistic disarrangements of an image cannot be mitigated, even when expert burglar performs blending [25] and matting [26] operations on the forged image as a postprocessing operation.

Bicoherence features were proposed by Farid [27] to highlight the traces of tampered signal. In this paper, Farid has taken the assumption that in the frequency domain, a natural signal has weak higher order statistical correlations. Then after applying polyspectral analysis (bispectrum/bicoherence), he showed that "unnatural" correlations are introduced if the signal is passed through a nonlinearity. Farid has applied this technique to detect the splicing in human speech. Later on, in [28],

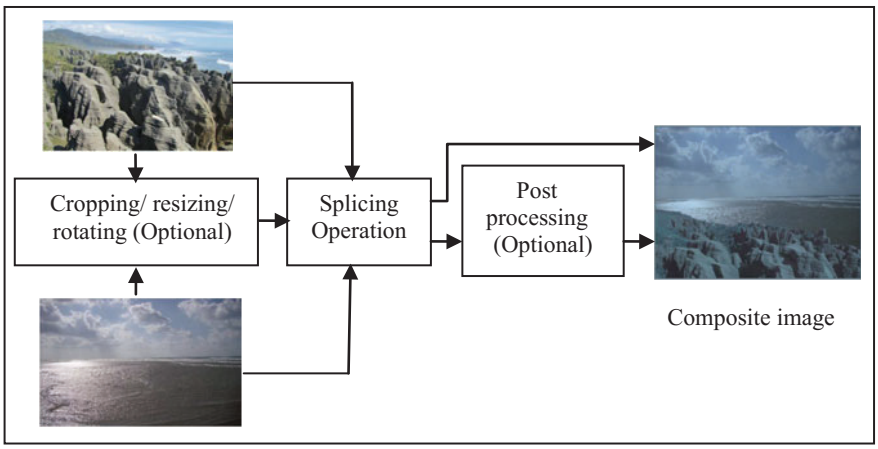

Fig. 5 Process of image splicing

Ng et al. exploited bicoherence feature for detecting image splicing in images. They have proposed two methods, the first method exploits the dependence of the bicoherence features on the image content and the second offsets the splicing-invariant component from bicoherence. Detection accuracy of their method was from 62 to 70%. In their method, features were evaluated with Support Vector Machine (SVM). Later on, the same authors proposed [29] a new method to detect image spicing based on bipolar signal perturbation. They concluded that image splicing process increases the value of the bicoherence magnitude and phase features.

Considering lighting inconsistencies as a fundamental key feature for detecting image splicing, Farid et al. proposed a method for estimating the direction of an illuminating light [30]. Hilbert–Huang Transform (HHT) based technique was proposed in [31]. They have been exploiting SVM classifier and claimed 80.15% detection accuracy. Further work was carried out by Li et al. [32] and they used SVM classifier on moment features and HHT-based features together. They achieved detection accuracy of 85.87%, which is higher than that of the prior work (70% as reported in [28] and 80.15% in [31]) on the same evaluation dataset [33].

A natural image model was proposed by Shi et al. [34], in which statistical features extracted from the test image and 2D arrays were generated by applying multi-size block discrete cosine transform (MBDCT). The statistical features include moments of characteristic functions of wavelet subbands and Markov transition probabilities of difference 2D arrays. Dong et al. [35] devised a method for image splicing detection based on the statistical features extracted from image run length representation and image edge statistics. The support vector machine (SVM) is used as a classifier and achieved detection accuracy was 84.36%. Wang et al. [36], have given a new technique, using image chroma component. Hsu et al., in their research paper [13], presented a fully automatic method to detect splicing of digital images by incorporating three features: geometry invariant CRF estimation, consistency checking, and image segmentation. Unfortunately, the method was not robust enough and showed recall and precision about 70% only. Kakar et al. [37], developed a new approach to detect image forgery based on discrepancies in motion blur and spectral analysis of image gradients. They showed that their technique outperforms other contemporary techniques, which are applicable to motion blur. Carvalho et al. [14], designed a new method based on inconsistencies in the color of the illumination of image, by exploiting SVM meta-fusion classifier.

Rao et al. developed a new approach [38] to unveil splicing in image, by exploiting motion blur cues. Authors claimed that their approach can expose splicing even under space-variant blurring situations. A new method with detection accuracy of 98.2% to detect image splicing using Markov features in spatial and discrete cosine transform, invented by El-Alfy and Qureshi [39]. They further improved the performance of the proposed approach by applying the PCA (Principle Component Analysis) to select the most relevant features before building the detection model. Meanwhile, two other sophisticated methods were developed for unveiling splicing, in [40, 41]. Noise discrepancies in multiple scales are utilized as indicators for image splicing forgery detection in the paper [42] by Pun et al., they gave conclusive remark that their

proposed method retains good detection accuracy in diverse situations like spliced area with different noise variance.

In [43], Park et al., introduced a method for image splicing detection, using the characteristic function moments for the inter-scale co-occurrence matrix in the wavelet domain with accuracy of 95.6%. They have tested their method on three popular datasets, Columbia, CASIA1, and CASIA2. Concurrently, Zhang and Lu [44], obtained an approach for unveiling image splicing by incorporating Markov model, in the block discrete cosine transform (DCT) domain and the Contourlet transform domain. In their illustrated method, authors have exploited SVM classifier to classify the authentic and spliced images for the gray image dataset. Verdoliva et al. devised an approach [45] by using autoencoder-based anomaly as a key feature.

Recently, Shen et al. [45] developed an algorithm for detecting image splicing by exploiting textural features based on the Gray-Level Co-occurrence Matrices. A support vector machine (SVM) is employed for classification purpose. The illustrated algorithm achieves the detection rates of 98% on CASIA v1.0, 97% on CASIA v2.0 and 91.88% on Columbia Image Splicing Detection Evaluation Dataset, with 96-D feature vector. Meanwhile, Farid [46] described three geometric techniques for detecting traces of digital manipulation in images. His proposed techniques were based on vanishing point, reflection, and shadow's location. Table 2 shows comparison of various algorithms for image.

3.2 Copy-Move Forgery Detection

In copy-move forgery one segment of image is copied and pasted in the other part of same image. Main intention of copy-move forgery is to hide some visual clues or replicating the things in image to mislead peoples. The prominent reason behind the surge in copy-move forgery is simplicity of this forgery. Good collection of tampered images throughout the history of image processing is available in [3]. Common workflow of copy-move forgery detection techniques has been shown in Fig. 6.

A survey on copy-move forgery detection techniques has been carried out in [18]. They have reviewed various research paper published in Web of Science (WOS) during years 2007–2014.

Silva et al. [53] developed a method for detecting copy-move forgery based on multiscale analysis and voting processes of a digital image. This method detects key points by exploiting Speeded-Up Robust Features (SURF) technique; Nearest Neighbor Distance Ratio (NNDR) is used for feature matching. Illustrated method can work under rotation, resizing or any combination of both. Unfortunately, it might not find a sufficient amount of key points in a small or homogeneous region.

Gabor filter based approach for copy-move forgery detection has been introduced by Lee et al. [54], which incorporates lexicographical sorting as a feature matching technique. Time complexity of this method was (O(PNlogN) + O(2JPN)). Meanwhile, in [55], Ardizzone et al. developed a copy-move forgery detection approach

Table 2 Comparative study of existing techniques of image splicing detection

S. n.	Algorithm	Features extracted	Classifier used	Accuracy	Dataset
1	Ng et al. [28]	Bicoherence features	SVM	62–70%	CISDE
2	Fu et al. [31]	Hilbert–Huang Transform (HHT), and wavelet decomposition	SVM	80.15%	CISDE
3	Shi et al. [34]	Moments of characteristic functions of wavelet subbands and Markov transition probabilities of difference 2-D arrays	SVM with RBF kernel	91.87%	CISDE
4	Chen et al. [47]	2D phase congruency and statistical moments of characteristic function	SVM	82.32%	CISDE
5	Dong et al. [35]	Statistic moments of characteristic function of image run length histograms	SVM	80.46–84.36%	CISDE
	Wang et al. [36]	Image chroma component	SVM	84.2%	CISDE
6	Li et al. [32]	HHT and moments feature	SVM	85.87%	CISDE
7	Hsu and Chang [13]	Geometry invariant CRF estimation, consistency checking, and image segmentation	SVM	70% precision, 70% recall	CUISDE

(continued)

Table 2 (continued)

S. n.	Algorithm	Features extracted	Classifier used	Accuracy	Dataset
8	He et al. [48]	Approximate run length along with edge gradient direction	SVM with RBF kernel	80.58%	CISDE
9	He et al. [49]	Markov features in DCT and DWT domain	SVM-RFE	93.55%	CISDE and CASIA v1
10	Carvalho et al. [14]	Inconsistencies in the color of the illumination of images	SVM meta-fusion	85–86%	Dataset of 200 images taken from the Internet
11	Xu et al. [50]	The DCT Markov features in chroma channel	SVM	–	CUISDE
12	Qureshi et al. [39]	Markov features in spatial and discrete cosine transform, Principal Component Analysis (PCA)	SVM with RBF kernel	98.2%	CISDE
13	Bahrami et al. [40]	Partial blur type inconsistency	Block-based partitioning	94.6%	Dataset of 1200 tampered images
14	Zhao et al. [41]	2D noncausal markov model	SVM	93.36%	CISDE
15	Park et al. [43]	Characteristic function moments for the inter-scale co-occurrence matrix in the wavelet domain	SVM with RBF kernel	95.3–95.6%	CASIA1 and CASIA2

(continued)

Table 2 (continued)

S. n.	Algorithm	Features extracted	Classifier used	Accuracy	Dataset
16	Han et al. [51]	Markov feature	SVM	94.87–98.50%	CASIA1 and CASIA2
17	Zhang et al. [44]	Markov feature in block Discrete Cosine Transform (DCT) domain and the Contourlet transform domain	SVM-RFE	96.69%	Dataset of 1150 forged color images
18	Rao and Ni [52]	Deep learning technique, and Convolutional Neural Network (CNN)	SVM	96.38%	CASIA v1.0, CASIA v2.0 and CISDE
19	Shen et al. [45]	Textural features based on the gray-level co-occurrence matrices	SVM	97–98%	CASIA v1.0 and CASIA v2.0

based on matching triangles, by applying mean vertex descriptors. This approach shows better performance in case of complex scenes; however, a lot of false matches occur with regular background.

Cozzolino et al. devised an algorithm [56] by considering dense-field techniques and Zernike moments as keypoint. Their algorithm utilizes nearest neighbor search algorithm and PatchMatch as a feature matching technique. Experiments were performed on copy-move forgery detection techniques in [57] by Li et al. and devised robust method for copy-move forgery detection by employing vlFeat software as feature extraction tool. Furthermore, Authors improved the accuracy of the obtained results by employing RANSAC via the gold standard algorithm. Their experiment showed the average precision as 0.86, however, method has high computation complexity, hence lead to low detection speed.

Pun et al. [58] proposed an algorithm to investigate copy-move forgery by combining keypoint feature and block-based feature. Experimental results show that their proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and downsampling, compared with the existing contemporary copy-move forgery detection schemes. Also, they have measured precision value as 96.6%

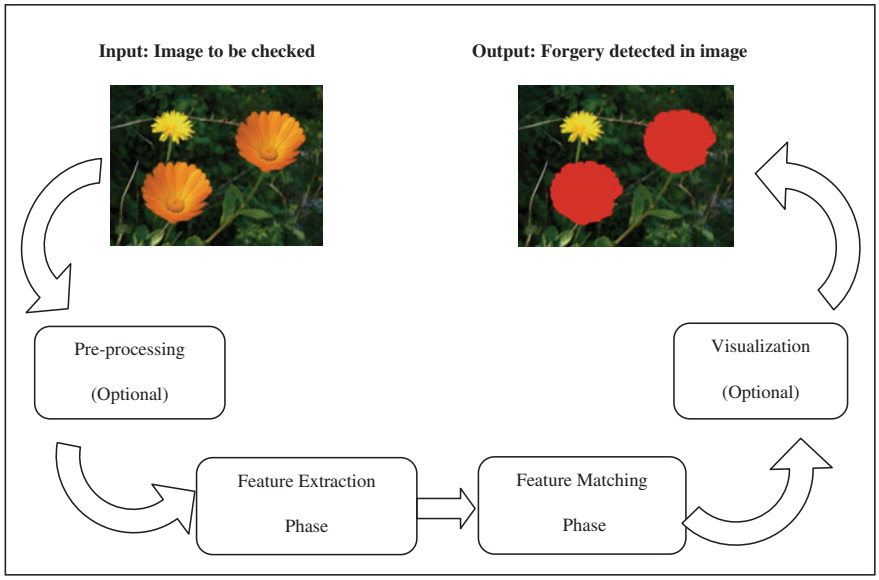

Fig. 6 Common workflow of copy-move forgery detection techniques

and recall value as 100%. Block-based technique to detect copy-move forgery was given by Lee et al. [54], by using a histogram of orientated gradients, which can deal with images distorted by small rotations, blurring, adjustment of brightness, and color reduction. However, their approach fails if high rotation and scaling are introduced by forger.

A rotation-invariant method to detect copy-move forgery based on circular projection, was presented by Gürbüz et al. [59]. Meanwhile, Zhao et al. [60] proposed a technique to detect copy-move forgery by incorporating split-half recursion matching strategy to match SIFT keypoints. Method first calculates the affine transformation between two matched regions. And then, the ZNCC coefficients are measured to detect duplicate region.

Wenchang et al. introduced a new method [61] to detect copy-move forgery by employing new concept particle swam optimization (PSO) along with SIFT keypoint. In their experiment, authors have employed the best bin first (BBF) algorithm for feature matching. The method showed the precision of 99%, but unable to detect forgery when duplicated region is very small. Zandi et al. proposed a technique [62] based on interest point detector. In this paper, authors first detect all the interest points and then describe features using Polar Cosine Transform. After that, an improved version of the adaptive matching is employed. Furthermore, falsely matched pairs are discarded by an effective filtering algorithm. Moreover, to enhance the result, they have iterated process regarding the prior information. Authors claimed that their method can be exploited in other image processing areas, such as scene recognition or image retrieval, etc. However, method is vulnerable to resizing attack. Behavior knowl-

edge space-based fusion was employed for copy-move forgery detection by Ferreira et al. [63]. In this work, they have overcome the limitations of fusing approaches by introducing new behavior knowledge space representation. Furthermore, authors also proposed multiscale behavior knowledge representation to deal with resizing and noise addition issues. Drawback with this method, however, is that it does not work well when image has several homogeneous regions.

Copy-move forgery detection technique based on scaled ORB has been proposed by Zhu et al. [64]. Their technique first, establishes a Gaussian scale space then, extracts FAST keypoints and the ORB features, in each scale space. Furthermore, technique employs RANSAC algorithm to remove the falsely matched keypoints. Experimental result shows that technique is effective for geometric transformation. However, approach is time-consuming when operated on high-resolution images. Bi et al. [65] designed a copy-move forgery detection technique by incorporating Multi-Level Dense Descriptor (MLDD) as a feature extraction method. They have utilized hierarchical feature matching method. Further, some morphological operations are applied to generate the final detected forgery regions. Approach work effectively with geometric transforms, JPEG compression, noise addition, and downsampling.

Ustubioglu et al. devised an algorithm for copy-move forgery detection by utilizing DCT-phase terms to restrict the range of the feature vector elements and also employed Benford's generalized law to determine the compression history of the image. The method uses element-by-element equality between the features. The method was also robust against postprocessing operations.

A new keypoint-based copy-move forgery detection for small smooth regions was developed by Wang et al. [66] by introducing the superpixel content based adaptive feature point detector. They also employed robust EMs-based keypoint features and fast Rg2NN based keypoint matching. However, serious limitation of method was the high computational complexity. Copy-move forgery detection technique has been devised by combining cellular automata(CA) and local binary patterns(LBP) by Tralic et al. [67]. The combination of CA and LBP allows a simple and reduced description of texture in the form of CA rules that represents local changes in pixel luminance values.

Recently in [68], a copy-move forgery detection method based on CMFD-SIFT, has been proposed by Yang et al. In their method, keypoints are detected by using a modified SIFT-based detector. This method improves the invariance to mirror transformation. Table 3 shows pros and cons of various algorithms for copy-move forgery detection based on several components such as feature extraction techniques, feature matching techniques, performance of algorithm and dataset used.

3.3 Image Resampling Detection

Resampling is mathematical technique to change the resolution (number of samples) of image, mainly for the purpose of increasing the size of image (upsampling) for printing banners and hoardings, etc., or for minimizing the size of image (downsam-

Table 3 Comparative study of existing techniques of copy-move forgery detection techniques published between 2015 and 2017

S. n	Algorithm	Feature extraction technique	Feature matching method	Performance	Pros/cons	Dataset
1	Silva et al. [53]	Multiscale analysis SURF	NNDR	CPU time 1.881 s/image	Pros: works under rotation, resizing, and these operations combined. Cons: not suitable for small or homogeneous region	CMH dataset CMEN datasets
2	Lee [69]	Gabor filter	Lexicographical sorting	O(PNlogN) + O(2JPN))	Pros: work even when image is distorted by slight rotation and scaling, JPEG compression, blurring, and brightness adjustment	CoMoFoD dataset CMFDA
3	Ardizzone et al. [55]	Matching Triangles	Mean Vertex Descriptors	10 s/image	Pros: better performance in case of complex scenes Cons: a lot of false matches image with regular background	CMFDA

(continued)

Table 3 (continued)

S. n	Algorithm	Feature extraction technique	Feature matching method	Performance	Pros/cons	Dataset
4	Cozzolino et al. [56]	Dense-field techniques and Zernike moments	nearest neighbor search algorithm and PatchMatch	11 s/image	Pros: achieves higher robustness on rotations and scale changes Cons: slow performance	Database of 80 images along with [12]
5	Li et al. [57]	VlFeat software, RANSAC	K nearest neighbors	Precision is 86%	Pros: good detection accuracy Cons: slow performance	CMFDA along with MICC-F600 and MICC-F2000
6	Pun et al. [58]	SIFT	Morphological operation	Precision 96.6% and recall 100%	Pros: better accuracy	CMFDA
7	Lee et al. [54]	Histogram of orientated gradients	Lexicographical sorting	Fc factor > 90%	Pros: robust against small rotations, blurring, adjustment of brightness, and color reduction Cons: not suitable with high rotation and scaling	CoMoFoD, second dataset of 30 high-resolution images

(continued)

Table 3 (continued)

S. n	Algorithm	Feature extraction technique	Feature matching method	Performance	Pros/cons	Dataset
8	Gürbüz et al. [59]	Circular projection technique	Lexicographical sorted	Accuracy 99%	Pros: robust against scaling and mirroring operations. Cons: less effective while rotation angle is big	20 test images with sizes of 326 × 245
9	Zhao et al. [60]	SIFT	g2NN	–	Pros: effective with rotation, scaling and multiple copy operations Cons: accuracy decreases with compression	MICC F2000
10	Wenchang et al. [61]	Particle Swam Optimization with SIFT	Best bin first	Precision 99%	Cons: fails to detect too small region	CMFDA
11	Zandi et al. [62]	Interest point detector	Adaptive matching	436 ms/image	Pros: effective under various challenging conditions	SBU-CM161

(continued)

Table 3 (continued)

S. n	Algorithm	Feature extraction technique	Feature matching method	Performance	Pros/cons	Dataset
12	Ferreira et al. [63]	BKS fusion	Multiscale Behavior Knowledge	$O(N^2)$	Cons: less efficient, also fails when image has several homogeneous regions,	CPH dataset
13	Zhu et al. [64]	FAST keypoints and the ORB features	hamming distance	270 ms/image	Pros: effective for geometric transformation Cons: time consuming for forgery detection of high-resolution images.	Dataset of 107 real images and 107 tampered images
14	Bi et al. [65]	Multi-level Dense Descriptor	Hierarchical Feature Matching	F score > 91%	Pros: robust against various attacks	CMFDA dataset
15	Bi et al. [70]	Multiscale feature	Adaptive patch	F = 95.05%	Pros: good performance on downsampling and multiple copies	CMFDA dataset
16	Ustubioglu et al. [71]	DCT-phase term	Element-by-element equality	Accuracy 96%	Pros: robust against various postprocessing operations	Comofod and Kodak databases

(continued)

Table 3 (continued)

S. n	Algorithm	Feature extraction technique	Feature matching method	Performance	Pros/cons	Dataset
17	Wang et al. [66]	Superpixels classification and adaptive keypoints	Reversed g2NN	221 s/image	Pros: effective with geometric transforms Cons: higher computational complexity	CMFDA dataset
18	Zheng et al. [72]	Zernike moments and SIFT along	g2NN	$F = 84.91\%$	Pros: can detect smooth regions	CMFDA dataset CoMoFoD
19	Tralic et al. [67]	Cellular Automata (CA) and LBP	Euclidean distance	$F > 0.92$	Pros: low computational complexity	CoMoFoD
20	Yang et al. [68]	Adaptive SIFT	AHC algorithm	$F > 90\%$	Pros: improves the invariance to mirror transformation	CoMoFoD
21	Huang et al. [73]	FFT, SVD, and PCA	Exhaustive search	Accuracy 98%	Pros: high detection accuracy	CASIA v1.0

pling) for email and website use. In general, almost all sort of digital image forgery (more specifically image splicing) involve scaling, rotation or skewing operations to manipulate the image. In these operations use of resampling and interpolation processes is inevitable. Hence, it is possible to detect the image forgery by tracing the symptoms of resampling in image. Several papers have been published in the past decade to detect the forgery in image on the basis of resampling.

Popescu et al. proposed a method [74] to expose digital forgeries by detecting traces of resampling. In blind forgery detection, no prior information is available about image, like which particular postprocessing attack has been applied, which interpolation is used to resample the image or part of image. However, to identify traces of resampling, interpolation details might be a basic telltale cue of resampling detection. Hence, authors in exploited expectation/maximization algorithm

(EM) [75] to determine if a signal has been resampled. Two models were developed, one for those samples that are correlated to their neighbors, and the second model corresponds to those samples that are not correlated. Their method is effective to unveil the sign of linear or cubic interpolation. However, it fails to detect other more sophisticated nonlinear interpolation techniques.

Kirchner [76] introduced a method based on fixed linear predictor. Method extracts periodic artifact and detect resampling. Meanwhile, Mahdian and Saic [77] proposed an algorithm to detect interpolation and resampling with 100% detection accuracy. The method was based on derivative operator and radon transformation. Their method was effective to detect the traces of scaling, rotation, skewing transformations.

Li et al. developed an algorithm in [78] to detecting resampling based on periodicity introduced by resampling and JPEG compression. They employed EM algorithm to obtain the probability map of an image. Further, Fourier-transformed and matched with affine-transform templates employed to detect resampling. They have experimentally concluded that image is not undergone resampling if the periodicity of the probability map obtained. Moreover, they have examined their method on the dataset of 100 grayscale images and claimed the detection accuracy better than [74].

Lien et al. [79] illustrated a new approach to detect forgery by observing the detectable periodic distribution properties generated from the resampling and interpolation processes. Their approach divided resampling as horizontal and vertical and then applied detection technique. Experimentally, authors have claimed 95% detection accuracy of their method which in turn can verify one image of resolution 512×512 only in 50 s on their mentioned system. In [80] Qian et al. developed a method to detect blind image forgery using resampling history detection algorithm. Instead of calculating the exact resampling energy spectrum of second-order derivative rate, authors have proposed a special distance measurement for measuring how far apart two sub-images are away from each other in terms of resampling difference. Method can detect the resampling even when rotation has been performed after resampling.

In [81], Birajdar et al. invented a new technique that blindly detects global rescaling operation and estimates the rescaling factor based on the autocovariance sequence of zero-crossings of second difference of the tampered image. The method is robust to detect rescaling operation for images that have been subjected to various forms of attacks like JPEG compression and arbitrary cropping with accuracy of 99.5%.

Recently, David and Fernando [82] devised a new approach for the detection of resampling by incorporating new tools and concepts from RMT (Random Matrix Theory). RMT provides useful tools for modeling the behavior of the eigenvalues and singular values of random matrices. Striking positive aspect of the method was very low computational complexity. Meanwhile, Qian et al. also proposed a method for detecting resampling forgery in digital image by using linear parametric model. In their method, first resampling is detected in 1D signal then further they have extended it for 2D image.

Table 4 summarizes the pros and cons of various algorithms developed for resampling detection, based on several components such as feature extraction techniques, detection accuracy of algorithm, and dataset used.

Table 4 Comparative study of existing techniques of resampling detection

S. n.	Algorithm	Feature description	Detection accuracy/performance	Pros/cons	Dataset
1	Popescu and Farid [74]	EM algorithm	Accuracy 80%	Pros: work with GIF format also Cons: fail to detect other more sophisticated nonlinear interpolation	Database of 200 grayscale images in TIFF format with 512 × 512 size cropped from a smaller set of 25, 1200 × 1600 images
2	Kirchner [76]	Fixed linear predictor	Accuracy 100% for upsampling	Pros: fast and reliable	Database of 200 uncompressed 8 bit grayscale with resolution 3112 × 2382 pixels
3	Mahdian and Saic [77]	Derivative operator and radon transformation	100%	Pros: capable of detecting traces of scaling, rotation, skewing transformations	Dataset of 40 images corrupted by various transformations
4	Wang and Ping [83]	Singular value decomposition	79.838%	Pros: robust against scaling manipulation Cons: less accurate with rotating transformation and compression	UCID
5	Li et al. [78]	EM algorithm, Fourier transform and affine transform	Better detection accuracy than [74]	Pros: better on resampling detection in JPEG compression Cons: very time consuming	Database of 100 gray-level images of various resolutions and formats (TIFF, BMP, PNG etc.)

(continued)

Table 4 (continued)

S. n.	Algorithm	Feature description	Detection accuracy/performance	Pros/cons	Dataset
6	Lien et al. [79]	Pre-calculated resampling weighting table	Accuracy 95% and CPU time 50 s/image	Pros: better detection accuracy	Dataset with 160 gray images with resolution 512 × 512
7	Qian et al. [80]	DFT	0.5203 s/image	Pros: effective with rotation after resampling	Dataset of 500 images cropped with different resampling rates
8	Feng et al. [84]	SVM	100%	Pros: shows better performance for downsampling	BOSS database
9	Hou et al. [85]	Local linear transform	96.15–98.75%	Pros: good resampling detection performance	Dataset of 1000 colored bmp images cropped into 512 × 512 pixels
10	Birajdar and Mankar [81]	Autocovariance sequence, DFT	99.5%	Pros: work well with various forms of attacks like JPEG compression and arbitrary cropping	UCID dataset USC-SIPI dataset
11	David and Fernando [82]	Asymptotic eigenvalue distribution and Random Matrix Theory (RMT)	0.0066 s/image	Pros: Low computational complexity	Dresden Image Database of a total of 1317 raw images [86]
12	Qiao et al. [87]	Probability of residual noise and LRT detector	0.0996 s/image	Pros: effective with uncompressed/compressed resampled images	500 uncompressed non-resampled images and 500 compressed resampled JPEG images with Quality Factor (QF) from 50 to 90

(continued)

Table 4 (continued)

S. n.	Algorithm	Feature description	Detection accuracy/performance	Pros/cons	Dataset
13	Su et al. [88]	Inverse filtering process with blind deconvolution	90%	Pros: does not affect with JPEG block artifacts Cons: Not effective to detect blurred images	UCID
14	Peng et al. [89]	AR coefficients and normalized histograms	98.3%	Cons: performance degrades with increasing JPEG compression ratio	BOSS dataset
15	Bayar and Stamm [90]	Convolutional Neural Network (CNN)	91.22%	Pros: can detect resampling in recompressed images	Dataset of 6500 images of size at least 2688×1520

3.4 Image Retouching Detection

Retouching can be defined as "polishing of an image". In general, retouching refers to subsequently improving the surface of an image. Contrast enhancement is a widely used technique to remove obvious visual clues from the forged image as a postprocessing operation. However, more involvement of retouching can be seen in entertainment media, magazine covers, etc., where retouching is not used maliciously. Contrast enhancement operations are tantamount to pixel value mappings, which introduce some statistical traces [91]. Therefore, retouching can be exploited as a tool for image forgery detection.

Stamm et al. proposed a method [92] for detecting contrast enhancement in an image on the basis of gray value histogram. They have developed a model for the histogram of an unaltered image and then exploited this model to detect manipulated artifacts. Detection accuracy of the algorithm was claimed to be about 99%. Cao et al. [93] developed a technique to detect sharpening alteration in digital images. Authors have measured gradient aberration of the gray histogram generated from unsaturated luminance regions of an image and exploited to unveil traces of sharpening manipulation. Cao et al. [94] proposed a new method to detect unsharp masking sharpening based on the feature overshoot artifacts occurred around side-planar edges. By experimental study, authors claimed, their method to be accurate to detect sharpening on small size images even when post-JPEG compression and noising attacks employed. Same authors further explained a method [95] for detecting the contrast enhancement in digital images. This time, they have utilized the histogram

peak/gap artifacts feature to detect global contrast enhancement applied to the previously JPEG-compressed images. Their proposed method is effective for detecting forgery when contrast enhancement is employed as the last step of manipulation. However, method fails to detect forgery when image is highly compressed.

In [91], Lin et al. explained that the contrast enhancement can disturb the interchannel similarities of high-frequency components, and then proposed a new method to detect the cut past forgery by detecting symptoms of contrast enhancement. Unfortunately, this method also fails when image is compressed after forgery. Ding et al. [96], proposed a new method to detect the special characteristic of the texture modification caused by the USM sharpening by employing edge perpendicular binary coding.

Recently, Zhu et al. presented a new approach [97] to detect image sharpening operation based on the overshoot artifact metric. First, they have detected edges using canny operator, then, non-subsampled contourlet transform (NSCT) is employed to classify image edge points. In the final stage, they have measured the overshoot artifact for each edge points and then, on the basis of overshoot artifacts judgment were made on sharpening operation. Table 5 shows various algorithms for retouching detection, based on several components such as; feature extracted, classifier applied, detection accuracy, and dataset used for testing the algorithm.

4 Datasets Available

Table 6 shows several publicly available datasets, which are frequently used by researchers.

5 Conclusion and Future Directions

In this paper, various existing methods on blind image forgery detection are reviewed. A broad classification of image forgery detection techniques is given. More specifically, a comprehensive overview of four main types of forgery detection techniques such as image splicing, copy-move, resampling, and retouching detection is given. Various existing methods have been reviewed in each category and observed that existing techniques suffer from one or more following limitations. (1) Detection accuracy (2) High computation complexity (3) Vulnerable against various attacks such as rotation, scaling, JPEG compression, blurring, and brightness adjustment, etc. (4) A lot of false matches with regular background.

Apart from abovementioned limitations, one major issue of these detection techniques is the limited scope of utilization, for example, method developed for copy-move forgery cannot work with image splicing or resampling and vice versa. In

Table 5 Comparative study of existing techniques of retouching detection

S. n.	Algorithm	Extracted feature	Classifier	Detection accuracy	Dataset used
1	Stamm and Ray [92]	Gray value histogram	Thresholding classifier	Global contrast 99%, Local contrast 98.5%, Histogram equalization 99%	341 images captured using different digital cameras
2	Cao et al. [93]	Ringing artifacts	Fisher linear classifier	Precision 0.85	Dataset of 403 JPEG images
3	Cao et al. [94]	Overshoot strength	Thresholding classifier	88%	Dataset of 400 JPEG images with the size from 1200 × 900 to 2832 × 2128 pixels
4	Lin et al. [91]	Interchannel correlation	Thresholding classifier	90%	Dataset of 100 uncompressed color images of size 1600 × 1200
5	Cao et al. [95]	Histogram peak/gap artifacts	Thresholding classifier	100%	BOSS public dataset and UCID
6	Ding et al. [96]	Rotation-invariant LBP	SVM	90%	UCID
7	Zhu et al. [97]	Multiresolution overshoot artifact	NSCT	92%	UCID

spite of burgeoning research in the field of image forgery detection, no detection method can be used as a solution for detecting all kind of forgeries. Hence, there is a great need to develop a robust, sophisticated forgery detection technique which could eliminate aforementioned limitations. Furthermore, researchers may extend these techniques to detect forgeries in videos.

Table 6 Description of various available datasets related to forgery detection

S. n	Dataset	Forgery type	Total images	Resolution	Description
1	CISDE [33]	Splicing	1845	128 × 128	Contains 933 forged images and 912 authentic images, all are gray images in PNG format
2	CUISDE [98]	Splicing	361	757 × 568, 1152 × 768	Contains 180 forged images and 181 authentic images, all are colored images in TIFF format
3	CASIA v1.0 [99]	Splicing	1725	324 × 256	Contains 925 forged images and 800 authentic images, all are colored images in JPEG format
4	CASIA v2.0 [100]	Splicing	12614	240 × 160–900 × 600	Contains 5123 forged images and 7491 authentic images, all are colored images in JPEG format Also contains uncompressed images and JPEG images with different Q factors
5	CMFDA [12]	Copy-move	48	420 × 300–3888 × 2592	Contains original and forged image applied with JPEG compression, rotation and scaling operation

(continued)

Table 6 (continued)

S. n	Dataset	Forgery type	Total images	Resolution	Description
6	CoMoFoD dataset [101]	Copy-move	260	512 × 512–3000 × 2000	Contains original and forged images, applied with translation, rotation, scale, distortion or a combination of them
7	MICC-F600 [102]	Copy-move	600	800 × 533–3888 × 2592	Contains original and forged images, that are randomly taken from MICC-F2000 and SATS-130 datasets
8	MICC-F2000 [103]	Copy-move	2000	2018 × 1536	Contains original and forged image, applied with translation, rotation, scale
9	SBU-CM161 [104]	Copy-move	240	800 × 580	Contains images based on 16 original JPEG images with rotation, scaling, compression
10	CPH [53]	Copy-move	216	845 × 634–296 × 972	Contains images with forgeries created through mixed operations such as resizing, rotation, scaling, compression, illumination matching
11	SCUT-FBP [105]	Retouching	500	384 × 512	Contains 500 different female face images along with the attractiveness rating scores computed from individual scores from 70 observers

(continued)

Table 6 (continued)

S. n	Dataset	Forgery type	Total images	Resolution	Description
12	BOSS public dataset [106]	Retouching	800	2000 × 3008–5212 × 3468	Contains unaltered photograph images in raw format
13	UCID [107]	Retouching	1338	384 × 512	Contains uncompressed images in TIFF format on various topics such as natural scenes, man-made objects, indoors and outdoors

References

1. Revolvy.com: Hippolyte Bayard (French, 1801–1887). https://www.revolvy.com/topic/Hippolyte Bayard&item_type = topic
2. Loc.gov: Civil War Glass Negatives and Related Prints. https://www.loc.gov/pictures/collection/cwp/mystery.html (2008)
3. Photo Tampering Throught History. http://pth.izitru.com/
4. Tait, A.: How a badly faked photo of Vladimir Putin took over Twitter. http://www.newstatesman.com/science-tech/social-media/2017/07/how-badly-faked-photo-vladimir-putin-took-over-twitter (2017)
5. Tyagi, V.: Understanding Digital Image Processing. CRC Press (2018). ISBN 9781315123905
6. Wang, S., Zheng, D., Zhao, J., Tam, W.J., Speranza, F.: An image quality evaluation method based on digital watermarking. IEEE Trans. Circuits Syst. Video Technol. **17**, 98–105 (2007)
7. Singh, P., Chadha, R.S.: A survey of digital watermarking techniques, applications and attacks. IEEE Int. Conf. Ind. Inform. **2**, 165–175 (2013)
8. Arnold, M., Schmucker, M., Wolthusen, S.D.: Techniques and Applications of Digital Watermarking and Content Protection. A Cataloging in Publication Record, Artech House Inc, Norwood, MA, USA (2003)
9. Lu, C., Liao, H.M., Member, S.: Structural digital signature for image authentication: an incidental distortion resistant scheme. IEEE Trans. Multimed. **5**, 161–173 (2003)
10. Schneider, M., Chang, S.: A robust content based digital signature for image authentication. In: IEEE International Conference on Image Processing. pp. 227–230 (1996)
11. Cox, I.J., Miller, M.L., Bloom, J.A., Kalker, T.: Digital Watermarking and Steganography Second Edition
12. Christlein, V., Riess, C.C., Jordan, J., Riess, C.C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**, 1841–1854 (2012)
13. Hsu, Y., Chang, S.: Camera response functions for image forensics: an automatic algorithm for splicing detection. IEEE Trans. Inf. Forensics Secur. **5**, 816–825 (2010)
14. Carvalho, T.J.De, Member, S., Riess, C., Member, A., Angelopoulou, E., Pedrini, H., Rocha, A.D.R.: Exposing digital image forgeries by illumination color classification. IEEE Trans. Inf. Forensics Secur. **8**, 1182–1194 (2013)

15. Popescu, A.C., Farid, H.: Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Inf. Forensics Secur. **53**, 758–767 (2005)
16. Lanh, T.V.L.T., Van Chong, K.-S., Chong, K.-S., Emmanuel, S., Kankanhalli, M.S.: A survey on digital camera image forensic methods. In: 2007 IEEE International Conference on Multimedia and Expo, pp. 16–19 (2007)
17. Farid, H.: A survey of image forgery detection techniques. IEEE Signal Process. Mag. **26**, 16–25 (2009)
18. Warif, N.B.A., Wahab, A.W.A., Idris, M.Y.I.: Copy-move forgery detection: survey, challenges and future directions. J. Netw. Comput. Appl. (2016)
19. Mahdian, B., Saic, S.: A bibliography on blind methods for identifying image forgery. Signal Process. Image Commun. **25**, 389–399 (2010)
20. Birajdar, G.K., Mankar, V.H.: Digital image forgery detection using passive techniques: a survey. Digit. Investig. **10**, 226–245 (2013)
21. Qazi, T., Hayat, K., Khan, S.U., Madani, S.A., Khan, I.A., Kołodziej, J., Li, H., Lin, W., Yow, K.C., Xu, C.-Z.: Survey on blind image forgery detection. Image Process. IET. **7**, 660–670 (2013)
22. Ansari, M.D., Ghrera, S.P., Tyagi, V.: Pixel-based image forgery detection: a review. IETE J. Educ. **55**, 40–46 (2014)
23. Ali, M., Deriche, M.: A bibliography of pixel-based blind image forgery detection techniques. Signal Process. Image Commun. **39**, 46–74 (2015)
24. Lukas, J., Fridrich, J., Goljan, M.: Detecting digital image forgeries using sensor pattern noise. In: Proceedings of SPIE, vol. 6072, pp. 60720Y–60720Y–11 (2006)
25. Yatziv, L., Sapiro, G.: Fast image and video colorization using chrominance blending. IEEE Trans. Image Process. 1120–1129 (2006)
26. Chuan, Y.Y., Curless, B., Salesin, D.H., Szeliski, R.: A bayesian approach to digital matting. Comput. Vis. Pattern Recognit. (2001)
27. Farid, H.: Detecting digital forgeries using bispectral analysis. Mit Ai Memo Aim-1657 Mit (1999)
28. Ng, T., Chang, S., Sun, Q.: Blind detection of photomontage using higher order statistics. In: IEEE International Symposium on Circuits System, pp. 7–10 (2004)
29. Ng, T., Chan, S.F.: A model of Image Splicing. In: IEEE International Conference on Image Process (2004)
30. Johnson, M.K., Farid, H.: Exposing digital forgeries by detecting inconsistencies in lighting. In: Proceedings of 7th Workshop on Multimed Security—MM&Sec'05, pp. 1–10 (2005)
31. Fu, D., Shi, Y.Q., Su, W.: Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions. Int. Work. Digit. Watermarking 177–187 (2006)
32. Li, X., Jing, T., Li, X.: Image splicing detection based on moment features and Hilbert-Huang transform. IEEE Int. Conf. Inf. Theory Inf. Secur. (2010)
33. Columbia DVMM Research Lab,Image Splicing Detection Evaluation Dataset. www.ee.columbia.edu/dvmm/researchProjects/AuthenticationWatermarking/Blind (2004)
34. Shi, Y.Q., Chen, C., Chen, W.: A natural image model approach to splicing detection. In: Proceedings of 9th Workshop Multimedia Security, pp. 51–62 (2007)
35. Dong, J., Wang, W., Tan, T., Shi, Y.Q.: Run-length and edge statistics based approach for image splicing detection. IWDW Int. Work. Digit. Watermarking. 5450 LNCS, 76–87 (2009)
36. Wang, W., Dong, J., Tan, T.: Effective image splicing detection based on image chroma. In: IEEE International Conference on Image Process, pp. 1257–1260 (2009)
37. Kakar, P., Member, S., Sudha, N., Member, S., Ser, W., Member, S.: Exposing digital image forgeries by detecting discrepancies in motion blur. IEEE Trans. Multimed. **13**, 443–452 (2011)
38. Rao, M.P., Rajagopalan, A.N., Member, S.: Harnessing motion blur to unveil splicing. IEEE Trans. Inf. Forensics Secur. **9**, 583–595 (2014)
39. El-Alfy, E.S., Qureshi, M.A.: Combining spatial and DCT based Markov features for enhanced blind detection of image splicing. Pattern Anal. Appl. 18, 713–723 (2015)

40. Bahrami, K., Member, S., Kot, A.C., Li, L., Li, H., Member, S.: Blurred image splicing localization by exposing blur type inconsistency. IEEE Trans. Inf. Forensics Secur. **6013**, 1–10 (2015)
41. Zhao, X., Wang, S., Li, S., Li, J.: Passive image-splicing detection by a 2-D noncausal Markov model. IEEE Trans. Circuits Syst. Video Technol. **25**, 185–199 (2015)
42. Pun, C.M., Liu, B., Yuan, X.C.: Multi-scale noise estimation for image splicing forgery detection. J. Vis. Commun. Image Represent. **38**, 195–206 (2016)
43. Park, T.H., Han, J.G., Moon, Y.H., Eom, I.K.: Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain. EURASIP J. Image Video Process **30** (2016)
44. Zhang, Q., Lu, W.: Joint image splicing detection in DCT and contourlet transform domain. J. Vis. Commun. Image Represent. (2016)
45. Shen, X., Shi, Z., Chen, H.: Splicing image forgery detection using textural features based on the grey level co-occurrence matrices. IET Image Process. **11**, 44–53 (2017)
46. Farid, H.: How to Detect Faked Photos (2017)
47. Chen, W., Shi, Y.Q., Su, W.: Image splicing detection using 2-D phase congruency and statistical moments of characteristic function. In: Security Steganography and Watermarking Multimedia Contents IX, vol. 6505, pp. 1–8 (2007)
48. He, Z., Sun, W., Lu, W., Lu, H.: Digital image splicing detection based on approximate run length. Pattern Recognit. Lett. **32**, 1591–1597 (2011)
49. He, Z., Lu, W., Sun, W., Huang, J.: Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognit. **45**, 4292–4299 (2012)
50. Xu, B., Liu, G., Dai, Y.: Detecting image splicing using merged features in chroma space. Sci. World J. (2014)
51. Han, J.G., Park, T.H., Moon, W.H., Eom, I.K.: Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion. J. Electron. Imaging. (2016)
52. Rao, Y., Ni, J.: A deep learning approach to detection of splicing and copy-move forgeries in images. In: 8th IEEE International Workshop Information Forensics Security WIFS (2016)
53. Silva, E., Carvalho, T., Ferreira, A., Rocha, A.: Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent. **29**, 16–32 (2015)
54. Lee, J.C., Chang, C.P., Chen, W.K.: Detection of copy-move image forgery using histogram of orientated gradients. Inf. Sci. (Ny) **321**, 250–262 (2015)
55. Ardizzone, E., Bruno, A., Mazzola, G.: Copy-move forgery detection by matching triangles of keypoints. IEEE Trans. Inf. Forensics Secur. **10**, 2084–2094 (2015)
56. Cozzolino, D., Poggi, G., Verdoliva, L.: Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. **10**, 2284–2297 (2015)
57. Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. (2015)
58. Pun, C., Member, S., Yuan, X., Bi, X.: Oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. **10**, 1705–1716 (2015)
59. Gürbüz, E., Ulutaş, G., Ulutaş, M.: Rotation invariant copy move forgery detection method. In: Proceedings of 9th International Conference on Electrical and Electronics Engineering, pp. 202–206 (2015)
60. Zhao, F., Zhang, R., Guo, H., Zhang, Y.: Effective digital image copy-move location algorithm robust to geometric transformations. In: IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC) (2015)
61. Wenchang, S.H.I., Fei, Z., Bo, Q.I.N., Bin, L.: Improving image copy-move forgery detection with particle swarm optimization techniques. China Commun. 139–149 (2016)
62. Zandi, M., Mahmoudi-Aznaveh, A., Talebpour, A.: Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans. Inf. Forensics Secur. **11**, 2499–2512 (2016)

63. Ferreira, A., Felipussi, S.C., Alfaro, C., Fonseca, P., Vargas-Munoz, J.E., Dos Santos, J.A., Rocha, A.: Behavior knowledge space-based fusion for copy-move forgery detection. IEEE Trans. Image Process. **25**, 4729–4742 (2016)
64. Zhu, Y., Shen, X., Chen, H.: Copy-move forgery detection based on scaled ORB. Multimed. Tools Appl. **75**, 3221–3233 (2016)
65. Bi, X., Pun, C.M., Yuan, X.C.: Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf. Sci. (Ny) **345**, 226–242 (2016)
66. Wang, X., Li, S., Liu, Y.: A new keypoint-based copy-move forgery detection for small smooth regions. Multimed. Tools Appl. (2016)
67. Tralic, D., Grgic, S., Sun, X., Rosin, P.L.: Combining cellular automata and local binary patterns for copy-move forgery detection. Multimed. Tools Appl. 16881–16903 (2016)
68. Yang, B., Sun, X., Guo, H., Xia, Z., Chen, X.: A copy-move forgery detection method based on CMFD-SIFT. Multimed. Tools Appl. (2017)
69. Lee, J.C.: Copy-move image forgery detection based on Gabor magnitude. J. Vis. Commun. Image Represent. **31**, 320–334 (2015)
70. Bi, X.L., Pun, C.M., Yuan, X.C.: Multi-scale feature extraction and adaptive matching for copy-move forgery detection. Multimed. Tools Appl. 1–23 (2016)
71. Ustubioglu, B., Ulutas, G., Ulutas, M., Nabiyev, V.V.: A new copy move forgery detection technique with automatic threshold determination. AEU Int. J. Electron. Commun. **70**, 1076–1087 (2016)
72. Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., Yang, H.: Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimens. Syst. Signal Process. **27**, 989–1005 (2016)
73. Huang, D., Huang , C., Hu, W.: Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimed. Tools Appl. **76**(1), 1509–1530 (2017)
74. Popescu, A.C., Farid, H.: Exposing Digital Forgeries by Detecting Traces of Resampling Resampling Detecting Resampling Experiment Results (2005)
75. Dempster, A., Laird, N., Rubin, D.: Maximum lilelihood from in- complete data via the EM algorithm. J. Roy. Stat. Soc. **99**, 1–38 (1977)
76. Kirchner, M.: Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue. In: Proceedings of 10th ACM Workshop Multimedia Security—MM&Sec'11 (2008)
77. Mahdian, B., Saic, S.: Blind authentication using periodic properties of interpolation. IEEE Trans. Inf. Forensics Secur. **3**, 529–538 (2008)
78. Li, S.P., Han, Z., Chen, Y.Z., Fu, B., Lu, C., Yao, X.: Resampling forgery detection in JPEG-compressed images. In: Proceedings of 2010 3rd International Congress on Image Signal Process CISP 2010, vol. 3, pp. 1166–1170 (2010)
79. Lien, C.-C., Shih, C.-L., Chou, C.-H.: Fast Forgery detection with the intrinsic resampling properties. J. Inf. Secur. **1**, 11–22 (2010)
80. Qian, R., Li, W., Yu, N., Hao, Z.: Image forensics with rotation-tolerant resampling detection. In: IEEE International Conference on Multimedia Expo Workshops ICMEW, pp. 61–66 (2012)
81. Birajdar, G.K., Mankar, V.H.: Blind method for rescaling detection and rescale factor estimation in digital images using periodic properties of interpolation. AEU Int. J. Electron. Commun. **68**, 644–652 (2014)
82. David, V., Fernando, P.: A Random Matrix Approach to the Forensic Analysis of Upscaled Images. IEEE Trans. Inf. Forensics, XX (2017)
83. Wang, R., Ping, X.J.: Detection of resampling based on singular value decomposition. In: Proceedings of Fifth International Conference on Image Graph, pp. 879–884 (2009)
84. Feng, X., Cox, I.J., Doërr, G.: Normalized energy density-based forensic detection of resampled images. IEEE Trans. Multimed. **14**, 536–545 (2012)
85. Hou, X.D., Zhang, T., Xiong, G., Zhang, Y., Ping, X.: Image resampling detection based on texture classification. Multimed. Tools Appl. **72**, 1681–1708 (2013)
86. Gloe, T., Ohme, R.: The dresden image database for benchmarking digital image forensics. In: ACM Symposium on Applied Computing, pp. 1584–1590

87. Qiao, T., Zhu, A., Retraint, F.: Exposing image resampling forgery by using linear parametric model. Multimed. Tools Appl. (2017)
88. Su, Y., Jin, X., Zhang, C., Chen, Y..: Hierarchical image resampling detection based on blind deconvolution q. J. Vis. Commun. Image Represent. 1–11 (2017)
89. Peng, A., Wu, Y., Kang, X.: Revealing traces of image resampling and resampling antiforensics. Adv. Multimed. (2017)
90. Bayar, B., Stamm, M.C.: On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection. In: IEEE International Conference on Acoustics Speech Signal Process, pp. 2152–2156 (2017)
91. Lin, X., Li, C., Hu, Y.: Exposing image forgery through the detection of contrast enhancement. In: International Conference on Image Process, pp. 4467–4471 (2013)
92. Stamm, M., Ray, K.J.: Blind forensics of contrast enhancement in digital images. In: Proceedings of International Conference on Image Process ICIP, pp. 3112–3115 (2008)
93. Cao, G., Zhao, Y., Ni, R.: Detection of image sharpening based on histogram aberration and ringing Artifacts. In: IEEE International Conference on Multimedia and Expo, pp. 1026–1029 (2009)
94. Cao, G., Zhao, Y., Ni, R., Kot, A.C.: Unsharp masking sharpening detection via overshoot artifacts analysis. IEEE Signal Process. Lett. **18**, 603–606 (2011)
95. Cao, G., Zhao, Y., Ni, R., Li, X.: Contrast enhancement-based forensics in digital images. IEEE Trans. Inf. Forensics Secur. **9**, 515–525 (2014)
96. Ding, F., Zhu, G., Yang, J., Xie, J., Shi, Y.Q.: Edge perpendicular binary coding for USM sharpening detection. IEEE Signal Process. Lett. **22**, 327–331 (2015)
97. Zhu, N., Deng, C., Gao, X.: Image sharpening detection based on multiresolution overshoot artifact analysis. Multimed. Tools Appl. (2016)
98. Hsu, Y.F., Chang, S.F.: Detecting image splicing using geometry invariants and camera characteristics consistency. In: International Conference on Multimedia and Expo, pp. 549–552 (2006)
99. Dong, J., Wang, W.: CASIA tampered image detection evaluation database
100. Dong, J., Wang, W.: CASIA2 tampered image detection evaluation (TIDE) database
101. Tralic, D., Zupancic, I., Grgic, S., Grgic, M.: CoMoFoD—New database for copy-move forgery detection
102. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. Del, Serra, G.: A SIFT-based forensic method for copy—move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. 1099–1110 (2011)
103. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., Serra, G.: Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process. Image Commun. 659–669 (2013)
104. Zandi, M., Mahmoudi-Aznaveh, A., Mansouri, A.: Adaptive matching for copy-move forgery detection. In: IEEE International Workshop on Information Forensics and Security, pp. 119–124 (2014)
105. Xie, D., Liang, L., Jin, L., Xu, J., Li, M.: A benchmark dataset for facial beauty perception. http://www.hcii-lab.net/data/SCUT-FBP
106. Bas, P., Filler, T., Pevný, T.: Break our steganographic system: the ins and outs of organizing BOSS. In: Proceedings of Information Hiding, Prague, Czech Repub, pp. 59–70 (2011)
107. Stich, M., Schaefer, G.: UCID—an uncompressed colour image database. In:Proceedings of SPIE, Storage Retrieval Methods and Application Multimedia, pp. 472–480 (2004)