J Inf Process Syst, Vol.14, No.1, pp.6~31, February 2018
https://doi.org/10.3745/JIPS.02.0078

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Survey on Passive Image Copy-Move Forgery Detection

Zhi Zhang*, Chengyou Wang*, and Xiao Zhou*

Abstract

With the rapid development of the science and technology, it has been becoming more and more convenient to obtain abundant information via the diverse multimedia medium. However, the contents of the multimedia are easily altered with different editing software, and the authenticity and the integrity of multimedia content are under threat. Forensics technology is developed to solve this problem. We focus on reviewing the blind image forensics technologies for copy-move forgery in this survey. Copy-move forgery is one of the most common manners to manipulate images that usually obscure the objects by flat regions or append the objects within the same image. In this paper, two classical models of copy-move forgery are reviewed, and two frameworks of copy-move forgery detection (CMFD) methods are summarized. Then, massive CMFD methods are mainly divided into two types to retrospect the development process of CMFD technologies, including block-based and keypoint-based. Besides, the performance evaluation criterions and the datasets created for evaluating the performance of CMFD methods are also collected in this review. At last, future research directions and conclusions are given to provide beneficial advice for researchers in this field.

Keywords

Copy-Move Forgery Detection (CMFD), Image Forensics, Image Tamper Detection, Passive Forgery Detection

1. Introduction

Nowadays, the digital image is still one of the most significant carriers to help people obtain large amounts of information. It is said that an image is worth innumerable words, which describes the fact that an image contains tremendous information. However, with the increasing use of modern sophisticated image editing software, such as Adobe Photoshop and GNU image manipulation program (GIMP), digital images are easily manipulated and altered without leaving any clues, and the credibility of image content cannot be identified even by trained observers. The tampered images altered maliciously by promulgator may pose the severe social problems, especially in medical diagnosis, court sentence, patent infringements, and insurance claims. One of the most famous events of the forged images is Iranian missile test in July 2008 [1] that is published on the front-pages of a few major news websites, including *The New York Times*, *The Chicago Tribune*, *The Los Angeles Times*, etc. The tampered photo was obtained from the web site of Iran's *Sepah News*, as shown in Fig. 1. A genuine Iranian missile photo is exhibited in Fig. 1(a); while Fig. 1(b) and (c) show the published version of Iranian missile situation, in which the third missile from the left was digitally appended to the original

Manuscript received October 20, 2017; accepted December 26, 2017.
Corresponding Author: Chengyou Wang (wangchengyou@sdu.edu.cn)
* School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China (zhi@mail.sdu.edu.cn, {wangchengyou, zhouxiao}@sdu.edu.cn)

photo to cover up the fact that it did not fire. A day later, the Associated Press news agency published the original photo (Fig. 1(a)) that further proved that published picture was synthetic. The similar event triggered by the counterfeit image is occurring every day. To validate the creditability of digital image content, image forensics technology is urgent to develop to avoid a huge loss of social benefits.

(a) (b) (c)

Fig. 1. Actual event of Iranian missile: (a) genuine Iranian missile photo, (b) forged Iranian missile photo published on BBC NEWS, and (c) forged Iranian missile photo with marked region-duplication.

Since the advent of synthetic images, many researchers have been devoting to the field of image forensics aim at different image forgery manners, such as copy-move [2], splicing [3], resampling [4], filtering [5], and double JPEG (joint photographic experts group) compression [6]. The classification of images forensics technologies is given in [7], as shown in Fig. 2. Image forensics technologies are divided into two categories: active forensics and passive forensics. Active forensics verifies the integrity of auxiliary information to decide whether the image has been tampered with, for instance, digital signature [8] and digital watermarking [9]. However, this type of technology requires special software or hardware to insert the authentication information into images or extract authentication information from images before being distributed. Passive forensics verifies the authenticity of the image by analyzing its contents and structure. In this survey, we focus on blind image forensics technologies for copy-move. Copy-move is one of the most common manners to alter the images by manipulators, which is usually used to obscure the objects by flat regions or append the objects within a same image. Copy-move forgery detection (CMFD) technologies are mainly divided into two classes, block-based methods and keypoint-based methods, which will be discussed in detail in the later subsequent sections.

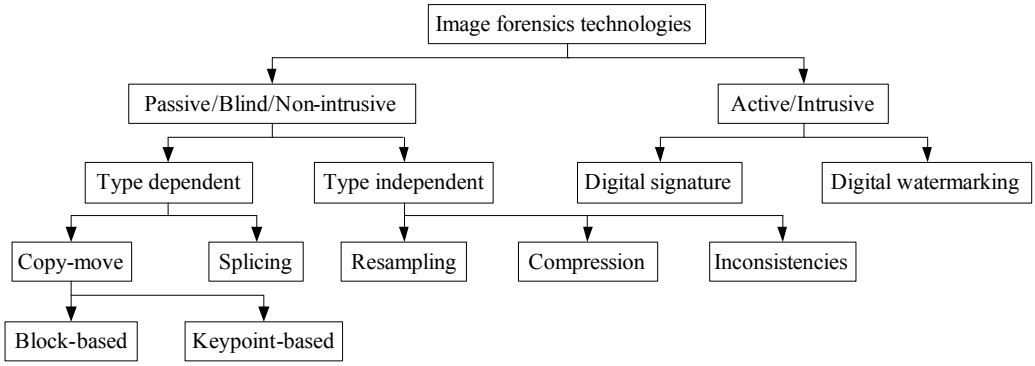


Fig. 2. Image forensics technologies classification.

The rest of this survey is organized as follows. Section 2 starts with a brief review of two models of copy-move forgery, and then two frameworks of CMFD methods are described. Block-based CMFD technologies are presented in Section 3, and Section 4 shows keypoint-based CMFD technologies. In Section 5, datasets consisting of forged images with copy-move and performance evaluation criterions are collected to evaluate the performance of CMFD technologies. Section 6 gives finally the future directions of CMFD and conclusion.

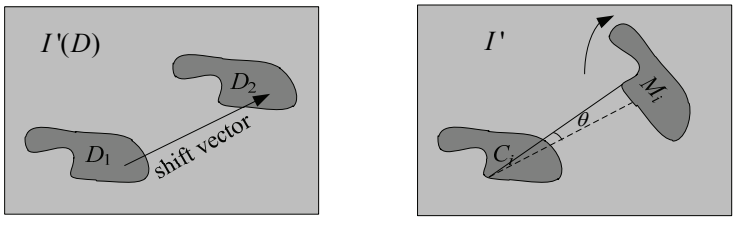
2. Models of Copy-Move Forgery and Frameworks of CMFD

In this section, two models of copy-move forgery are reviewed. Two frameworks accordant with the diverse CMFD technologies are also presented, and most of CMFD schemes are based on these models.

2.1 Models of Copy-Move Forgery

In [10], after analyzing 100 natural images, the authors found that it is impossible that a single image has two similar areas larger than 0.85% of the image area. The goal is looking for two similar large areas in suspicious image, as shown in Fig. 3(a). They made a deduction as below:

Given an image I, the forged image I', must subordinate to: $\exists$ areas D_1 and D_2 are subsets of D and a shift vector $d=(dx,dy)$, (they assumed that $|D_1|=|D_2|>|D|*0.85\%$ and $|d|>L$), $I'(x,y)=I(x,y)$ if $(x,y)\notin D_2$ and $I'(x,y)=I(x-dx,y-dy)$ if $(x,y)\in D_2$, where D_1 is the source region and D_2 is the pasted region, $D_2=D_1+d$. Nevertheless, Luo's model cannot describe the forgery way that a copied region is pasted to two or more places, and the copied region is rotated before being pasted. Plain copy-move forgery is shown in Fig. 3(a).



(a) (b)

Fig. 3. Two models of copy-move forgery: (a) Luo's model and (b) Liu's model.

To remedy the defect of Luo's model, Liu et al. [11] presented a more comprehensive copy-move forgery model, as shown in Fig. 3(b). They assumed that the shift vector threshold is $\boldsymbol{V}_T=[V_{tx},V_{ty}]$, and copied region threshold (the ratio of the copy area and the whole image area) is A_T. An image I is forged to I' via copy-move manipulation, if

1) The copied region $C_i, i\in\{1,2,\cdots,n\}$ is single-connected and has no hole inside, and its area is greater than $A_T a(I)$, where $a(I)$ denotes the area of I.

2) Supposing the pasted region of copied region C_i is M_i, there might be many duplicated region

pairs $\{C_1 \| M_1, C_1 \| M_2, \cdots, C_n \| M_n\}$, $C_i, M_i \in I'$, which satisfy $C_i \neq C_j$, $\forall i \neq j$, $i, j \in \{1,2,\cdots,n\}$ and $C_i \cap C_j = \phi$. For any pair $C_i \| M_i$, defining the origin of the reference system as the center of rotation, the copy-move forgery can be considered as translation after rotation, described by

$$\begin{cases} \forall (x,y) \in C_i, f(x,y) = f'(x',y'), \\ x' = x\cos\theta - y\sin\theta + \Delta_x, \\ y' = x\sin\theta + y\cos\theta + \Delta_y, \\ \sqrt{\Delta_x^2 + \Delta_y^2} \geq |\boldsymbol{V}_{\mathrm{T}}|, \\ a(C_i) > A_{\mathrm{T}} \cdot a(I), \end{cases} \tag{1}$$

where f denotes the pixel value at the position (x,y); Δ_x and Δ_y is the shift distance along x and y axis, respectively; and θ is the rotation angle. However, the pasted region may be altered by other operations, like scaling that changes one-to-one mapping. Therefore, a more generalized copy-move model needs to be proposed. A good CMFD scheme can detect the duplicated regions even if the pasted region is distorted by blurring, rotation, noise contamination, scaling, or JPEG compression.

2.2 Frameworks of CMFD

In this subsection, two frameworks of CMFD methods are presented, and most of CMFD schemes adhere to the two frameworks.

Block-based and keypoint-based CMFD methods always follow the framework as shown in Fig. 4(a).

1) *Pre-processing*: The suspicious image is processed by a series of operations. For example, adopt Wiener filter [12] or dyadic wavelet transform (DyWT) [13] for de-noise; convert RGB (red, green, blue) color space into grayscale space [14,15], YCrCb color space [16], HSV (hue, saturation, and value) space [17], or color local binary pattern (LBP) space [18]; perform discrete wavelet transform (DWT) [19] or Gaussian pyramid decomposition [11] to obtain the dimension reduction presentation of the image.

2) *Feature extraction*: Image segmentation is used for feature extraction in block-based CMFD methods. The image is divided into overlapping square image blocks [20], non-overlapping square image blocks [21], or overlapping circle image blocks [22]. Besides, simple linear iterative clustering (SLIC) method [23] is also used for image segmentation [24]. A great deal of features are extracted for CMFD, such as discrete cosine transform (DCT) [14], Fourier-Mellin transform (FMT) [25], 2D-Fourier transform [26], polar harmonic transform (PHT) [27], singular value decomposition (SVD) [28], LBP [22], Zernike moment [29], Hu moment [11], scale-invariant feature transform (SIFT) [15], speeded up robust features (SURF) [30], Harris corner features [31], DAISY [32], etc.

3) *Feature matching*: Feature matching is the procedure of finding similar feature vectors. To narrow the range of similar feature vectors, sorting algorithm causes similar features to be adjacent, such as lexicographic sorting [19] and radix sorting [33]. Besides, k-d tree [18] or locality-sensitive hashing (LSH) [34] speeds up the process of finding similar feature vectors a lot. In addition, there are many methods to evaluate the similarity between the feature vectors, such as Euclidean distance and Manhattan distance, which are corresponding with Eq. (2) and Eq. (3), respectively.

$$d_{\text{Euclidean}} = \sqrt{\sum_{i=1}^{n}[v_1(i) - v_2(i)]^2}\ , \tag{2}$$

$$d_{\text{Manhattan}} = \sum_{i=1}^{n}|\, v_1(i) - v_2(i)\,|\,, \tag{3}$$

where v_1 and v_2 are n-dimensional feature vectors.

4) *Localization and post-processing*: If the regions determined by the process of feature matching are shown in the map, there will be many isolated points, and morphologic operations [35], filtering [33] or random sample consensus (RANSAC) algorithm [36] is usually used to refine detected regions.

Another model is based on machine learning, as shown in Fig. 4(b). The classifier is trained by trained image set with labels and the trained classifier will determine whether the test image has been tampered or not, like support vector machine (SVM) classifier [16]. However, CMFD methods based machine learning only decide whether the test image has been forged or not. It is still a challenging problem for this type of methods to locate tampered region.

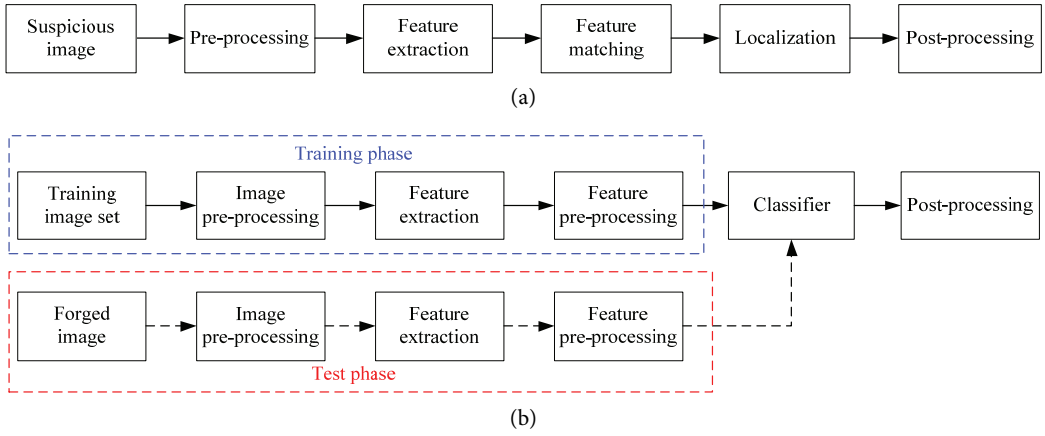


Fig. 4. Two frameworks of CMFD methods: (a) framework of block-based CMFD and keypoint-based CMFD and (b) framework of CMFD based on machine learning. Adapted from G. K. Birajdar and V. H. Mankar. Digital image forgery detection using passive techniques: a survey. Digital Investigation 2013;10(3):226-245, with the permission of Elsevier [37].

3. Block-Based CMFD Methods

Diverse CMFD methods are briefly described in this section, including DCT-based, wavelet transform-based, PHT-based, LBP-based, Zernike-based, SVM-based, etc. A table is given to compare the performance of CMFD methods from various aspects at the end of this section.

3.1 DCT Based Algorithms

Fridrich et al. [14] first proposed the DCT-based method for CMFD. The image is divided into fixed-size overlapping image blocks at raster-scan, and DCT is performed on each block. The quantization feature vector is obtained by performing zigzag scanning on the quantized DCT coefficient matrix. The feature matrix is lexicographically ordered and Euclidean distance is used for similarity judgment.

However, this method has high computation cost. To reduce computational complexity, Huang et al. [38] truncated the feature vector by using a constant to reduce the dimensionality of the feature and presented a scheme to judge similarity between feature vectors. Mahmood et al. [39] used Gaussian radial basis function (RBF) and kernel principal component analysis (KPCA) to reduce the dimensionality of the feature vector that ameliorated the efficiency in the feature matching process. Cao et al. [40] divided the inscribed circle of a square image block into four non-overlapping parts and extracted mean of each part coefficients as the feature to detect duplicated regions. Fadl and Semary [41] divided feature vectors into several groups by using fast k-means algorithms and searched duplication-region in each group. In [42], the authors divided the image into smooth and complex by using edge detection information, and if the image is smooth (complex), it is divided into big (small) blocks. DCT coefficients were set as 0 or 1 according to the rules in [43] for CMFD. Alkawaz et al. [44] studied the effects of different block size on the performance of CMFD method. In [45], package clustering algorithm is used to divide the DCT feature vectors and coordinates into different packages, and then find similar feature vectors in each package. Zhao and Guo [46] presented a scheme combining DCT and SVD for CMFD. Doyoddorj and Rhee [47] used quantized DCT coefficients obtained by performing DCT in Radon space of each image block and detected copy-move regions. Ustubioglu et al. [48] proposed a CMFD algorithm based on LBP and DCT.

3.2 Wavelet Transform Based Algorithms

In this subsection, different wavelet transform algorithms are collected. The image is decomposed into four parts by DWT, including approximate component sub-band LL, horizontal detail sub-band LH, vertical detail sub-band HL, and diagonal detail sub-band HH. In [19], LL is divided into overlapping image blocks and singular value vector is the feature vector obtained by performing SVD on each block. Kashyap and Joshi [49] extracted blur moment invariants from each block and performed PCA on blur moment invariants matrix to reduce the dimensionality. DyWT [50] is shift invariant and captures the structure in a better way than DWT. In [51,52], authors presented a CMFD scheme by using the fact that copied region and pasted region should exhibit similarity between them in LL, while copied region and pasted region in HH should exhibit high dissimilarity between them in noise pattern. A similar approach in [53] utilized singular value vectors obtained from overlapping blocks in LL and HH to detect duplicated regions. However, LL and HH are obtained by stationary wavelet transform (SWT) [54].

3.3 Other Transforms Based Algorithms

In [55], the authors offered a CMFD scheme that used image block feature mapped to log-polar coordinates and phase correlation to search duplicated region. Bravo-Solorio and Nandi [56] computed 1D descriptor invariant to rotation and reflection by summing a log-map along the log-radius axis to make the localization of duplication-region more precise. In [57], they proved the effectiveness of their scheme by various experiments and comparisons with other CMFD methods. However, interpolation from the Cartesian coordinates to a log-polar gridding reduces precision and results in considerable errors in low image resolution or small block-size. By using rotation and scale invariant features, Wu et al. [58] proposed a CMFD scheme to detect region-duplication in a forged image by using log-polar fast

Fourier transform (LPFFT), while Park et al. [59] presented a scheme to detect region-duplication by utilizing the feature extracted from the up-sampled log-polar Fourier (ULPF) descriptor. By introducing an adaptive phase correlation method in the log-polar coordinate system and utilizing the information extracted from the band limitation, Yuan et al. [60] presented a robust CMFD method which can handle with large scaling operation.

Yap et al. [61] proposed PHTs-based method against rotation, which included polar sine transform (PST), polar cosine transform (PCT), and polar complex exponential transform (PCET). PCET has relatively better performance than the other two transforms. In [27,62], the authors divided the image into overlapping circular blocks, and PST was performed on each circular block to extract feature. After filtering and morphological processing, the duplicated regions were found. Li [34] extracted PST coefficients of each block as the feature and searched duplicated region by approximate nearest searching and LSH to achieve CMFD. Ganty and Kousalya [63] realized spectral-hashing-based PCT image CMFD algorithm. In [64], the authors proposed a PCET-based CMFD scheme in which LSH was used for identifying the potential similar image blocks. Bi et al. [65] extracted color texture descriptor and invariant moment descriptor calculated from the PCET moments to solve the problem of searching duplicated regions. Wo et al. [66] presented a CMFD method based on multi-radius PCET that can detect the pasted region with large-scale scaling and rotation. In [67], the authors proposed an efficient discrete Radon polar complex exponential transform (DRPCET)-based scheme for extracting the scaling and rotational invariant features for CMFD. It is worth mentioning that they introduced an auxiliary circular template to construct invariant feature, as shown in Fig. 5. Zhong et al. [68] extracted the discrete radial harmonic Fourier moments (DRHFMs) from each circular block with the help of the circular template (Fig. 5).

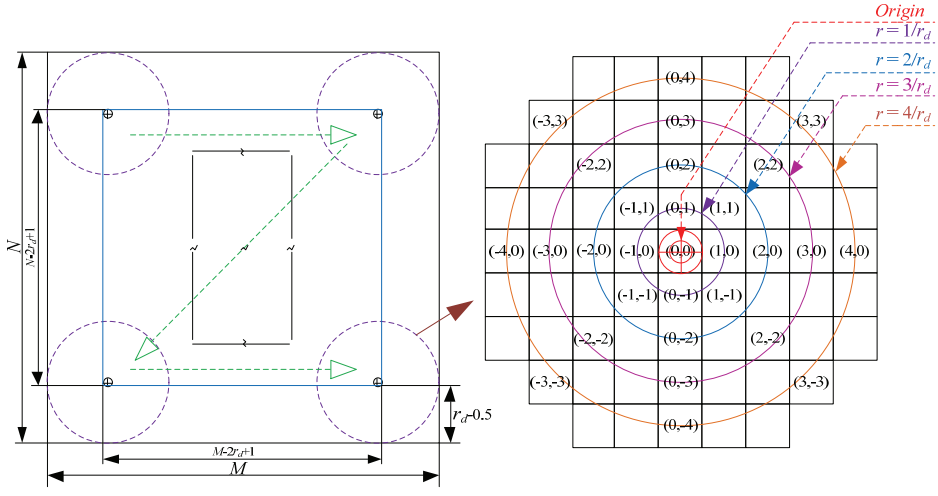


Fig. 5. A circular template in Cartesian space. Adapted from J. Zhong et al. A new block-based method for copy move forgery detection under image geometric transforms. Multimedia Tools and Applications 2017;76(13):14887-14903, with the permission of Springer [68].

In [25], the authors proposed FMT-based CMFD scheme in which counting bloom filters, rather than lexicographic sorting, were used to save computational time. Li and Yu [69] improved Bayram's scheme in which distance vectors are clustered by a vector erosion filter that is robust to rotation and scaling.

After introducing analytical Fourier-Mellin transform (AFMT), Zhong and Gan [70] proposed discrete analytical Fourier-Mellin transform (DAFMT)-based CMFD scheme. However, as pointed in [67], the defect of AFMT is too complicated, especially the construction of its invariant moment.

Ketenci and Ulutas [26] applied 2D-Fourier transform on each overlapping square block to extract feature for achieving CMFD algorithm. After performing the Fourier transform of the polar expansion on the overlapping windows pair and implementing an adaptive band limitation to construct a correlation matrix, Shao et al. [71] offered a CMFD scheme by estimating the rotation angle of the forged region and using search algorithm to locate the duplicated regions. In [72], the authors utilized four features extracted from Fourier transform coefficients of each circular block to achieve CMFD algorithm. After extracting electromagnetism-like (EMag) mechanism descriptor from each non-overlapping block, Dadkhah et al. [73] applied discrete Fourier transform (DFT) to EMag features to achieve CMFD. By using city block filter, horizontal filter, vertical filter, and frequency filter, Huang et al. [74] offered a threshold-free CMFD scheme by combining the features including fast Fourier transform (FFT), SVD, and PCA.

3.4 LBP and Moment Invariant Based Algorithms

Li et al. [22] divided the image into overlapping circular blocks and extracted features using rotation invariant uniform LBP to detect duplicated regions. Davarzani et al. [75] presented an efficient scheme for CMFD using multi-resolution LBP (MLBP), in which k-d tree is used to save time and RANSAC is used to remove the possible false matches. In [76], the object is detected by normalized cut segmentation, and then, with the help of Hessian method, local interest points are localized. Duplication-region is found by using center-symmetric LBP (CSLBP). Yang et al. [77] also used uniform LBP to detect duplicated region. What is different with [22] is that the authors used a shift-vector counter instead of the block matching. Tralic et al. [78] combined cellular automata (CA) and LBP to extract feature vectors for CMFD. In [79], the authors proposed a CMFD method using binary gradient contours (BGC), and they proved the performance of their schemes is superior to many LBP-based methods.

Ryu et al. [29] presented a CMFD algorithm by using the magnitude of Zernike moment invariant against rotation. In [80], the authors combined LSH and RANSAC to improve the accuracy and efficiency of CMFD scheme based on Zernike moment. Al-Qershi and Khoo [81] adopted a grouping method [82] for block matching to improve detection accuracy. Thuong et al. [83] extracted foreground of the image by morphological technology and performed the wavelet transform to the foreground to extract approximate component. Zernike moment is used for CMFD in [83]. Mahmoud and Abu-Alrukab [84] proposed pseudo-Zernike moment (PZM)-based scheme for CMFD and improved Zernike moment based method.

Mahdian and Saic [85] proposed a CMFD method based on blur invariant moment constructed by applying the algorithm [86]. Du et al. [87] combined the 1D moment, the 2D moment, and the Markov feature to present a CMFD algorithm based on multiple features, where 1D moment is the feature of 1D histogram and 2D moment is the feature of 2D histogram in the horizontal and vertical direction. Imamoglu et al. [88] extracted Krawtchouk moment to detect the duplicated region in the forged image. Liu et al. [11] extracted Hu moment for CMFD and Kushol et al. [89] combined Hu moment and Lab color space-based feature for CMFD.

3.5 Other Algorithms

Popescu and Farid [90] utilized PCA to reduce the dimensionality of block features and proposed a scheme to detect duplicated regions in forged images. Kakar and Sudha [91] extracted the features by using the MPEG-7 image signature tools and presented a novel technology for CMFD. Malviya and Ladhake [92] employed auto color correlogram (ACC), a feature used in image retrieval, to obtain feature vector and detected duplicated regions successfully. In [93], the authors presented a CMFD method against scaling operation. Vladimirovich and Valerievich [94] proposed a plain CMFD algorithm using structure pattern and 2D Rabin-Karp rolling hash, which achieves zero false negative error and fast execution speed for the images with high resolution. On the basis of the method in [94], Kuznetsov and Myasnikov [95] presented a CMFD scheme by using a hash value calculation in a sliding window mode. Kashyap et al. [96] combined SVD and cuckoo search algorithm that can automatically generate suitable parameter value for each image.

PatchMatch [97] is a fast approximate nearest-neighbor search algorithm for block matching [98-100]. In [98], the authors modified the basic PatchMatch algorithm and proved its efficiency by using CMFD based on Zernike moment and CMFD based on RGB value, respectively. They presented two detectors in [99] that can detect forged regions in the spliced image and copy-move image, respectively. By utilizing the invariant features and a suitably modified version of PatchMatch, Cozzolino et al. [100] achieved a CMFD scheme that has a good robustness to various types of geometrical distortion.

In [16], the authors extracted multi-resolution Weber law descriptors (WLD) as the feature and trained a model by SVM in which the accuracy of their method can reach up to 91%. After training models by SVM with MLBP and multi-resolution WLD, respectively, Hussain et al. [101] found that multi-resolution WLD performs better than multi-resolution LBP in detecting splicing and copy-move forgeries. In [102], steerable pyramid transform (SPM) is performed on the chrominance channels Cr and Cb to obtain some multi-scale and multi-oriented sub-bands. The feature vector is produced by concatenating the histograms from each sub-band and SVM uses the feature vectors to classify images into forged or authentic. Rao and Ni [103] presented a CMFD scheme based on the deep learning technology including SVM and convolutional neural network (CNN). A 10-layer CNN is used to automatically learn hierarchical representations from the RGB images. Dense features extracted from the test image are obtained by using the pre-trained CNN, and a feature fusion technology is designed to obtain the discriminative features for SVM classification.

State-of-the-art block-based CMFD algorithms and some of the classical schemes are described in Table 1. Table 1 describes the methods from several aspects including pre-processing, feature extraction, method for searching similar blocks, post-processing, performance, and dataset.

In Table 1, several aspects need to be explained. The collected data are the basis of the corresponding literature, and the detail information can be found in literature. In 'Feature extraction' column, GLCM is the abbreviation of gray-level co-occurrence matrix; CLD is the abbreviation of color layout descriptors; CHT is the abbreviation of circular harmonic transforms; and feature1 is three averages of the red, blue, and green color of the pixels and entropy. In 'Performance', single/multiple means the method can detect the number of the forged region. AWGN means additive white Gaussian noise; [max_value,min_value] means the range of relevant processing with maximum value and minimum value; and min_value:step:max_value means the value ranges from maximum value and minimum value with the step. The parameters in 'Performance' need to be distinguished by readers to read

relevant literature because of the difference of researchers' comprehension. In 'Dataset', datasets for CMFD will be listed in Section 5.2, and basic datasets used by researchers to create their own datasets for CMFD are also listed in this survey, such as UCID [104], National Geographic [105], ImageNet [106], Kodak [107], DOCR [108], PIMPRCG [109], USC-SIPI [110], KSU [51], and Caltech-256 [111].

Table 1. Block-based CMFD methods comparison

Ref	Year	Pre-processing	Feature extraction	Method for searching similar blocks	Post-processing	Performance	Dataset
Liu et al. [11]	2011	Gaussian pyramid decomposition; Circular block	Hu moment	Sorting; Euclidean distance	Morphologic operations	Multiple; AWGN (15:10:15); JPEG compression (45:20:85); Rotation (-20°, 12°, 90°); Gaussian blurring (5, 1:1:3); Flipping (horizontal)	Internet
Zhu et al. [18]	2017	Convert RGB into color LBP; Square block	GLCM	K-d tree; Euclidean distance	Morphologic operations	Single; Gaussian noise (40,80); Gaussian blurring ((3,1), (5,2)); JPEG compression (60, 90)	GRIP
Ustubioglu et al. [20]	2016	Square block	Color moments; CLD	Clustering; Sorting; Euclidean distance	Morphologic operations	Multiple; AWGN ((5, 0.5:0.5:3.0), (3, 0.5:0.5:1.0)); Gaussian blurring (15:5:35); JPEG compression (40:10:90)	CoMoFoD
Li et al. [22]	2013	Convert RGB into gray; Low-pass filtering; Circular block	LBP	Sorting; Euclidean distance	Filtering; Morphologic operations	Single; Rotation (90°:90°:270°); Flipping (horizontal, vertical); JPEG compression (50:10:90); AWGN (15:5:35); Gaussian blurring (5, 1:1:5)	UCID; Internet
Li et al. [27]	2012	Convert RGB into gray; Circular block	PHT	Sorting; Euclidean distance	Morphologic operations	Single; Rotation (15°, 30°, 90°, 180°); AWGN ([15, 40]); JPEG compression (>50); Mixture operations	Internet
Kang and Wei [28]	2018	Square block	SVD	Sorting; Euclidean distance		Single; JPEG compression (50:10:100); Gaussian blurring (0:0.4:2.0); AWGN (25:5:50)	Internet
Ryu et al. [29]	2010	Square block	Zernike moment	Sorting; Euclidean distance		Single; Rotation (0°:10°:90°); JPEG compression (40:10:100); AWGN (0.001:0.002:0.009); Gaussian blurring (0.5:0.5:3.0); Mixture operations	Internet; National Geographic
Li [34]	2013	Circular block	PCT	LSH	Morphologic operations	Single; Gaussian blurring (0.5:0.5:3.0); Gaussian noise (0.001:0.002:0.009); JPEG compression (20:10:90); Rotation (10°:10°:90°)	ImageNet; Kodak; DOCR
Huang et al. [38]	2011	Convert RGB into gray; Square block	DCT	Sorting; Euclidean distance	Morphologic operations	Single; Gaussian blurring ((3, 0.5:0.5:1.0), (5, 0.5:0.5:1.0)); AWGN (1, 2, 4); JPEG compression (50, 70:10:90)	DVMM
Mahmood et al. [39]	2016	Convert RGB into gray; Square block	KPCA; DCT	Sorting; Euclidean distance	Morphologic operations	Multiple; JPEG compression (70:5:90); AWGN (20:5:40); Gaussian blurring (5, 0.5:0.5:3.0)	DVMM; Internet
Cao et al. [40]	2012	Convert RGB into gray; Circular block	DCT	Sorting; Euclidean distance	Morphologic operations	Multiple; AWGN (10:5:35); Gaussian blurring (5, 0.5:0.5:3.0)	DVMM; Kodak; Internet
Wang et al. [45]	2017	Convert RGB into gray; Square block	DCT	Package clustering; Euclidean distance	-	Multiple; AWGN (10:10:50); Gaussian blurring (2, 0.5:1.0:2.5); Mixture operations	MICC-F; DVMM; PIMPRCG

Table 1. (Continued)

Ref	Year	Pre-processing	Feature extraction	Method for searching similar blocks	Post-processing	Performance	Dataset
Zhao and Guo [46]	2013	Convert RGB into gray; Square block	DCT; SVD	Sorting; Euclidean distance	Morphologic operations	Multiple; Gaussian blurring ((5, 0.5:0.5:3.0), (3, 0.5:0.5:1.0)); AWGN (20:5:45); JPEG compression (65:5:95); Mixture operations	USC-SIPI; Kodak; Internet
Doyoddorj and Rhee [47]	2014	Square block	Radon transform; DCT	Sorting; Euclidean distance	Filtering	Multiple; AWGN (5:5:40); Gaussian blurring (5, 1:1:7); Mixture operations (JPEG compression+Rotation, JPEG compression+Scaling, Rotation+AWGN, Rotation+Scaling, etc.)	FAU
Muhammad et al. [51]	2012	DyWT; Square block	LL; HH	Sorting; Euclidean distance	-	Multiple; JPEG compression (60, 80, 90); Rotation (<20°)	CASIA TIDE v1.0; KSU
Dixit et al. [53]	2017	Convert RGB into gray; SWT; Square block	LL; HH; SVD	Sorting; Euclidean distance	-	Single; Blurring	Internet
Bravo-Solorio and Nandi [57]	2011	Square block	Feature1	Sorting; Bravo	-	Multiple; JPEG compression (60:10:100); Rotation; Scaling (0.95:0.01:1.05); Flipping (horizontal); Mixture operations	Caltech-256
Li et al. [62]	2014	Convert RGB into gray; Gaussian low-pass filtering; Circular block	PST	Sorting; Euclidean distance	Filtering; Morphologic operations	Multiple; Scaling (0.1:0.2:1.1); Rotation (15°, 30°, 90°); Flipping (horizontal, vertical); AWGN (20:10:40); JPEG compression (40:20:80); Gaussian blurring (3,1:2:5); Mixture operations	Internet
Granty and Kousalya [63]	2016	Circular block	PCT; Spectral hashing; PCA	Sorting; Hamming distance; Euclidean distance	Filtering; Morphologic operations	Single; Blurring (0.5:0.5:3.0); Noise (1:2:9); JPEG compression (20:30:90); Rotation (20°:10°:90°)	FAU
Emam et al. [64]	2016	Circular block	PCET	LSH	Morphologic operations	Multiple; JPEG compression (0:20:80); Gaussian noise (0.002:0.002:0.006); Rotation (0°, 2°, 10°, 60°, 180°); Scaling (0.93:0.04:1.09)	FAU
Wo et al. [66]	2016	Circular block	Multi-radius PCET	Sorting	Morphologic operations	Multiple; JPEG compression (20:20:100); Gaussian blurring ((3, 0.5), (5, 0.5)); Gaussian noise (0, 0.0004:0.0002:0.001); Rotation (0°:30°:360°); Scaling (0.5:0.1:2.0)	FAU; Kodak
Zhong et al. [67]	2017	Convert RGB into gray; Circular block	DRPCET	Sorting; Person correlation coefficient	-	Single; Rotation (0°:20°:180°); Gaussian noise; Scaling; Mixture operations (Rotation+Scaling, Rotation+Gaussian noise)	MICC-F2000; Internet
Zhong et al. [68]	2017	Convert RGB into gray; Gaussian filtering; Circular block	DRHFM	Sorting; Euclidean distance	-	Multiple; Rotation; Gaussian noise; Scaling; JPEG compression; Mixture operations (Rotation+Scaling, Rotation+JPEG compression, etc.)	MICC
Zhong and Gan [70]	2016	Convert RGB into gray; Circular block	DAFMT	Sorting; Spearman rank correlation coefficient	-	Single; Rotation ([0°, 180°]); Scaling ([0.4,1.4]); Gaussian noise; Mixture operations (Rotation+Scaling+Noise adding, etc.)	Internet

Table 1. (Continued)

Ref	Year	Pre-processing	Feature extraction	Method for searching similar blocks	Post-processing	Performance	Dataset
Huang et al. [74]	2017	Convert RGB into gray; Square block;	FFT; SVD; PCA	Matchers	City filtering; Horizontal filtering; Vertical filtering; Frequency filtering	Multiple; JPEG compression (20, 50, 80, 90); Gaussian blurring (3:4:7, 1); Gaussian noise (0, 5:5:20)	Internet; CASIA TIDE v1.0
Davarzani et al. [75]	2013	Convert RGB into gray; Circular block; Low-pass filtering;	MLBP	Sorting; K-d tree	RANSAC	Multiple; Rotation; Scaling; JPEG compression; Gaussian blurring; Gaussian noise; Mixture operations	Internet; PIMPR CG
Kuznetsov and Myasnikov [79]	2016	Square block	BGC; LBP	K-d tree	Filtering	Single; Contrast enhancement; Gaussian noise; JPEG compression (40:10:90)	Internet
Ryu et al. [80]	2013	Square block	Zernike moment	LSH	RANSAC	Multiple; Rotation(0^o:10^o:90^o); JPEG compression (40:20:100); AWGN (2:2:8); Linear filtering (0.5:0.5:2.5); Scaling	FAU
Mahmoud and Abu-Alrukab [84]	2016	Square block	Zernike moment; PZM	Sorting; Euclidean distance; Physical distance	-	Multiple; Color reduction; Additive noise; Contrast adjustment; Blurring; Brightness change; Rotation; Scaling	CoMoFoD
Malviya and Ladhake [92]	2016	Square block	ACC	Manhattan distance	-	Multiple	CoMoFoD
Cozzolino et al. [100]	2015	Circular block	CHT	PatchMatch	Linear filtering	Multiple; JPEG compression (20:10:100); Scaling; Rotation; Noise	GRIP; FAU

4. Keypoint-Based CMFD Methods

Typical keypoint-based CMFD methods selected from many keypoint-based methods are presented in this section, such as SIFT, dense scale-invariant feature transform (DSIFT), affine-scale-invariant feature transform (ASIFT), SURF, Harris corner feature, DAISY, mirror reflection invariant feature transform (MIFT) [112], multi-support region order-based gradient histogram (MROGH) [113,114].

In [115], the authors extracted SIFT descriptor as the feature, and best-bin-first (BBF) search method is used to match the similar feature. Pan and Lyu [15] estimated the geometric transform between matched SIFT keypoints and found the duplicated regions. Amerini et al. [116-118] proposed SIFT-based CMFD methods. In [116], maximum likelihood estimation (MLE) of the homograph and RANSAC algorithm are used for geometric transformation estimation. Amerini et al. [117] proposed a generalized 2NN test for multiple duplicated regions localization and agglomerative hierarchical clustering is used to identify the possible cloned region. In [118], they introduced J-Linkage algorithm to improve their works. Jin and Wan [119] used non-maximum value suppression and optimized J-Linkage to ameliorate the performance of SIFT-based CMFD methods. In [120], the authors proposed a SIFT-based CMFD scheme by using the SIFT keypoints extracted from actual part obtained by

performing DyWT to the image. Different with the manner of converting the color image into the gray image in pre-processing, Gong and Guo [121] extracted the color gradient from the suspicious image and took the gradient as the only input for SIFT extraction. In [122], the authors converted the color image into HSV. To solve value setting, Zhao and his colleagues [123,124] proposed a CMFD method based on SIFT with particle swarm optimization (PSO). ASIFT [125] and DSIFT [126] are also used in CMFD, respectively. In [127], the authors used expectation maximization (EM) algorithm to estimate the transform matrix. Warif et al. [128] presented a CMFD method that combined SIFT-based CMFD scheme with symmetry-based matching.

Shivakumar and Baboo [129] proposed a CMFD scheme based on SURF and k-d tree was used for feature matching. Mishra et al. [130] combined SURF and hierarchical agglomerative clustering (HAC) and presented a CMFD method. After multi-scale analysis and voting processes, Silva et al. [131] presented a CMFD scheme by using SURF as the feature. By combining adaptive minimal-maximal suppression (AMMS) and SURF, Yang et al. [132] presented a CMFD method to solve the problem of insufficient keypoints in the uniform area. SLIC was used for image segmentation, and SURF was used as the feature to find the duplicated region in [24].

Chen et al. [133] proposed a CMFD scheme based on Harris corner points and step sector statistics, in which BBF algorithm was used to find duplicated region. By combining Harris corner points and LBP, Zhao and Zhao [134] presented a scheme to detect region duplication in images. Wang et al. [135] used the statistical features of the Harris corner keypoints neighborhoods as forensics feature, and a new feature matching method was used for the improvement of detected accuracy. Combining the angular radial partitioning and Harris keypoints, Uliyan et al. [136] presented a CMFD scheme.

In recent several years, many CMFD schemes based on hybrid keypoints have been proposed and implemented, such as SIFT, SURF, and Harris corner [137], SURF and SIFT [138], SURF and binary robust invariant scalable keypoints (BRISK) [139], Harris corner points and BRISK [140], SURF, SIFT, and histogram oriented gradient (HOG) [141,142], MROGH and Harris corner points [143], and KAZE and SIFT [144].

State-of-the-art keypoint-based CMFD algorithms and some of the classical schemes are described in Table 2. Table 2 describes the methods from the below aspects: feature, performance, and dataset. In 'Performance', the second item is the visualization form. In 'Dataset', SATA-130 is included in FAU.

Table 2. Keypoint-based CMFD methods comparison

Ref.	Year	Feature	Performance	Dataset
Jaberi et al. [112]	2014	MIFT	Single; Closed region; Scaling; Rotation; Deformation; Mixture operations (Scaling+Blurring, Scaling+Rotation+Blurring, Rotation+Blurring, Scaling+Deformation, etc.)	CASIA TIDE v2.0
Yu et al. [113]	2016	MROGH	Multiple; Closed region; JPEG compression (20:10:100); Rotation (2^o:2^o:10^o, 20^o, 60^o, 180^o); Scaling ([0.5, 2.0]); AWGN (0.02:0.02:0.10); Mixture operation (Rotation+Scaling)	FAU; MICC-F2000
Amerini et al. [117]	2011	SIFT	Multiple; Lines; Rotation; Scaling; Mixture operation (Rotation+Scaling)	MICC-F2000; MICC-F220
Amerini et al. [118]	2013	SIFT	Multiple; Lines; Rotation; Scaling; Mixture operation (Rotation+Scaling)	MICC-F2000; SATA-130; MICC-F600
Karsh et al. [125]	2016	ASIFT	Single; Points and lines	CoMoFoD

Table 2. (Continued)

Ref.	Year	Feature	Performance	Dataset
Li et al. [127]	2015	DSIFT	Multiple; Closed region; Noise (20:20:100); JPEG compression (20:10:100); Rotation (2^o:2^o:10^o); Scaling (0.91:0.02:1.09)	FAU; MICC-F600
Mishra et al. [130]	2013	SURF	Single; Points and lines; JPEG compression (20:20:80); AWGN(20:10:50); Gaussian blurring ((5, 0.5:0.5:1.0), (7,0.5:0.5:1.0)); Gamma correction (1.2:0.2:1.8); Scaling; Rotation	MICC-F220
Chen et al. [133]	2013	Harris corner points	Single; Circulars and lines; Rotation; Scaling (0.8, 0.9, 1.1, 1.2, 1.3); Mixture operation (Rotation+Scaling); Flipping (horizontal); JPEG compression (50:10:90); AWGN (20:5:40)	Kodak; CASIA TIDE v2.0
Zhao and Zhao [134]	2013	Harris corner points; LBP	Multiple; Lines; Rotation; Gaussian blurring; Flipping (horizontal, vertical); JPEG compression; AWGN; Mixture operations (Rotation+Gaussian blurring, Flipping+Gaussian blurring, etc.)	Kodak; Internet; CASIA TIDE v2.0
Ardizzone et al. [137]	2015	SIFT; SURF; Harris corner points	Single; Closed region; Rotation; Scaling	CVIP
Pandey et al. [138]	2015	SURF; SIFT	Single; -; Rotation; Scaling; Mixture operation (Rotation+Scaling)	MICC-F220
Kumar et al. [139]	2015	SURF; BRISK	Multiple; Points; JPEG compression (40:10:100); Gaussian noise (0:0.02:0.10)	FAU; CoMoFoD
Isaac and Wilscy [140]	2015	Harris corner points; BRISK	Single; Lines; Noise adding; Brightness change; Color reduction; Blurring	CoMoFoD; MICC-F220
Prasad and Ramkumar [142]	2016	SIFT; HOG; SURF	Single; Lines	MICC-F220
Yang et al. [144]	2017	KAZE; SIFT	Multiple; Closed region; Rotation (2^o:2^o:10^o); Scaling (0.91:0.02:1.09); Gaussian noise (0, 0.02:0.02:0.10); JPEG compression (20:10:100)	FAU

5. Performance Evaluation Criterions and Datasets

5.1 Performance Evaluation Criterions

The performance of CMFD methods is usually evaluated from two aspects: the image level and the pixel level. The most frequently used performance evaluations are Precision p, Recall r, and F_1 score [145], which are shown in Eqs. (4)–(6), respectively.

$$p = \frac{T_P}{T_P + F_P}, \tag{4}$$

$$r = \frac{T_P}{T_P + F_N}, \tag{5}$$

$$F_1 = 2 \cdot \frac{p \cdot r}{p + r}, \tag{6}$$

where T_P denotes the number of doctored images correctly detected as doctored images; F_P denotes the number of authentic images erroneously detected as doctored images; and F_N denotes the number of doctored images falsely detected as authentic images, at image level. At pixel level, T_P denotes the number of correctly detected as doctored pixels; F_P denotes the number of falsely detected as doctored pixels; and F_N denotes the number of falsely detected as authentic pixels. The larger the p, r, and F_1 are, the higher the accuracy of the CMFD scheme is.

Zhao and Guo [46] presented another evaluation criterion at pixel level, the detection accuracy rate R_{DA} and the false positive rate R_{FP}, which are shown in Eqs. (7) and (8), respectively.

$$R_{DA} = \frac{|\psi_C \cap \tilde{\psi}_{DC}| + |\psi_P \cap \tilde{\psi}_{DP}|}{|\psi_C| + |\psi_P|}, \tag{7}$$

$$R_{FP} = \frac{|\tilde{\psi}_{DC} - \psi_C| + |\tilde{\psi}_{DP} - \psi_P|}{|\tilde{\psi}_{DC}| + |\tilde{\psi}_{DP}|}, \tag{8}$$

where $|\ |$ denotes the area of the copied region or pasted region, $\cap$ denotes the intersection of two regions, $-$ denotes the difference between two regions, ψ_C denotes the pixels of the copied region, ψ_P denotes the pixels of the pasted region, $\tilde{\psi}_{DC}$ denotes the pixels of detected copied region, and $\tilde{\psi}_{DP}$ denotes the pixels of detected pasted region. The closer R_{FP} is to 0 and R_{DA} is to 1, the higher the accuracy of the CMFD method is.

5.2 Datasets

Diverse datasets for CMFD are listed in this sub-section. A good dataset for CMFD should have the original images, the forged images, the distorted forged images, and their corresponding ground truth maps, as shown in Fig. 6, which are from the CoMoFoD dataset [146]. Some commonly used datasets for the evaluation of CMFD methods are collected in Table 3, and their corresponding links are shown in References.

Besides these datasets mentioned above, many methods created their own datasets by using images from the Internet and other datasets that are also collected in this survey [104-111,151].

(a) (b) (c) (d)

Fig. 6. Example of the CoMoFoD dataset: (a) original image, (b) forged image, (c) forged image with image blurring, and (d) ground truth map.

Table 3. Dataset comparison

Dataset	Content	Content detail	Ground truth map	Format (size)
GRIP [100]	80 tampered color images 80 authentic color images	80 single plain tampered images	Yes	PNG (1024×768; 768×1024)
CVIP [137]	1,060 tampered color images 50 authentic color images	680 single tampered images (rotation) 380 single tampered images (scaling)	Yes	BMP 1000×700 or 700×1000
MICC-F8multi [147]	8 tampered color images	8 multiple tampered images	No	JPG (2048×1536, 800×532, 947×683)
MICC-F220 [147]	110 tampered color images 110 authentic color images	110 single tampered images (rotation, scaling)	No	JPG (from 722×480 to 800×600)
MICC-F2000 [147]	700 tampered color images 1,300 authentic color images	700 single tampered images (rotation, scaling)	No	JPG (2048×1536)
MICC-F600 [147]	152 tampered color images 448 authentic color images	38 single plain tampered images; 38 multiple plain tampered images; 38 images in which the copied region is rotated by 30°; 38 images in which the copied region is rotated by 30° and scaled by 120%	Yes	PNG, JPG (from 722×480 to 800×600)
FAU [145]	48 color image sets (1632×1224) 48 color image sets (3039×2014)	Single or multiple tampered images (translation, rotation, scaling, distortion, combination)	Yes	PNG, JPG (1632×1224; 3039×2014)
CoMoFoD [146]	200 color image sets (512×512) 60 color image sets (3000×2000)	Single or multiple tampered images (translation, rotation, scaling, distortion, combination)	Yes	PNG, JPG (512×512; 3000×2000)
CASIA TIDE v1.0 [148]	921 tampered color images 800 authentic images	480 tampered images within same images 451 tampered images from different images (rotation, deformation, resize)	No	JPG (384×256)
CASIA TIDE v2.0 [148]	5,123 tampered color images 7,491 authentic color images	5,123 tampered color images (rotation, deformation, resize)	No	TIF, JPG (from 240×160 to 900×600)
COVERAGE [149]	100 tampered color images 100 authentic color images	100 single tampered color images (translation, scaling, rotation, free-form, illumination, combination)	Yes	TIF (400×486)
DVMM [150]	912 tampered gray images 933 authentic gray images	180 single plain tampered images	No	BMP (128×128)

6. Future Direction and Conclusion

6.1 Future Direction

On the basis of the existing problems in current research status, several future directions for CMFD research are provided in this subsection based on the existing problems.

- *Benchmark dataset*. A dataset is indispensable to evaluate the performance of CMFD method. Dataset for CMFD evaluation should include original images and corresponding forged images

with different resolution, diverse forged images with regions (smooth or texture) which have different size in various geometric transformation (rotation, scaling, etc.), the forged region saved individually as images, the distorted images with post-processing methods (JPEG compression, AWGN, noise contamination, blurring, etc.). Besides, the corresponding ground truth maps and post-processing methods with open-source code (MATLAB, OpenCV) also should be included in dataset.

- *Effectiveness and robustness*. CMFD methods should be effective to detect the forged regions in distorted doctored images as mentioned in *benchmark dataset*. It is worth exploring efficient local invariant feature and descriptors extraction, high-speed method of feature matching, and accurate localization method.
- *Deep learning*. It is relatively few CMFD methods based on deep learning. The application of deep learning is only used in the classification of authentic images and forged images, and it is hard to determinate the accurate forged regions. It is also a difficult problem that these CMFD methods based on deep learning are hard repeatable and used for comparison because of the difference of the training set and testing set or the complex experiments. The researchers study this topic by using deep learning technologies in the future, such as deep Boltzmann machines [152] and CNN [153].

6.2 Conclusion

Passive forensics technology of digital image is one of the rapidly growing fields of research. Our brief review of image CMFD technologies indicates that the research is still in the phase of vigorous development and has a huge potential for the future research and development applications. Two classical models of copy-move forgery and two frameworks of CMFD technologies are presented at first. Then, block-based and keypoint-based CMFD methods are reviewed from different aspects, respectively, including the classical CMFD technologies and the state-of-the-art algorithms for CMFD in recent several years. The performance evaluation criterions and frequently used datasets for evaluating the performance of the CMFD schemes are collected. The future directions of this topic are given at last. With the help of the advanced technologies, some CMFD schemes with high performance are expected to become standard tools in the future. We also hope that this survey will provide related information to scientists, researchers, and relevant research communities in this field. The investigation on image forensics is still a continual, sustainable process and it will continue to explore forensics technologies with high accuracy and robustness.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61702303, No. 61201371); the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004); and the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022). The authors thank Surong Zhang, Xiuhong Wei, and Chi Wang for their kind help and valuable suggestions in revising this paper.

References

[1] Photo Tampering throughout History [Online]. Available: http://pth.izitru.com/2008_07_01.html.

[2] D. Vaishnavi and T. S. Subashini, "A passive technique for image forgery detection using contrast context histogram features," *International Journal of Electronic Security and Digital Forensics*, vol. 7, no. 3, pp. 278-289, 2015.

[3] H. Yao, S. Wang, X. Zhang, C. Qin, and J. Wang, "Detecting image splicing based on noise level inconsistency," *Multimedia Tools and Applications*, vol. 76, no. 10, pp. 12457-12479, 2017.

[4] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, New Orleans, LA, USA, 2017, pp. 2152-2156.

[5] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1849-1853, 2015.

[6] A. Taimori, F. Razzazi, A. Behrad, A. Ahmadi, and M. Babaie-Zadeh, "Quantization-unaware double JPEG compression detection," *Journal of Mathematical Imaging and Vision*, vol. 54, no. 3, pp. 269-286, 2016.

[7] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences*, vol. 49, no. 3, pp. 281-307, 2017.

[8] D. M. Uliyan and M. A. F. Al-Husainy, "Detection of scaled region duplication image forgery using color based segmentation with LSB signature," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, pp. 126-132, 2017.

[9] H. Zhang, C. Wang, and X. Zhou, "Fragile watermarking based on LBP for blind tamper detection in images," *Journal of Information Processing Systems*, vol. 13, no. 2, pp. 385-399, 2017.

[10] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Proceedings of the 18th International Conference on Pattern Recognition*, Hong Kong, China, 2006, pp. 746-749.

[11] G. Liu, J. Wang, S. Lian, and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, vol. 34, no. 5, pp. 1557-1565, 2011.

[12] F. Peng, Y. Y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features," *Forensic Science International*, vol. 212, no. 1-3, pp. e21-e25, 2011.

[13] M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform," *AASRI Procedia*, vol. 9, pp. 84-91, 2014.

[14] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, Cleveland, OH, USA, 2003, pp. 55-61.

[15] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 857-867, 2010.

[16] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, "Copy-move image forgery detection using multi-resolution weber descriptors," in *Proceedings of the 8th International Conference on Signal Image Technology and Internet Based Systems*, Naples, Italy, 2012, pp. 395-401.

[17] A. V. Malviya and S. A. Ladhake, "Region duplication detection using color histogram and moments in digital image," in *Proceedings of the International Conference on Inventive Computation Technologies*, Coimbatore, India, 2016, pp. 1-4.

[18] Y. Zhu, X. J. Shen, and H. P. Chen, "Covert copy-move forgery detection based on color LBP," *Acta Automatica Sinica*, vol. 43, no. 3, pp. 390-397, 2017.

[19] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, Beijing, China, 2007, pp. 1750-1753.

[20] B. Ustubioglu, G, Ulutas, M. Ulutas, and V. V. Nabiyev, "Improved copy-move forgery detection based on the CLDs and colour moments," *The Imaging Science Journal*, vol. 64, no. 4, pp. 215-225, 2016.

[21] J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images," in *Proceedings of the 11th IEEE Singapore International Conference on Communication Systems*, Guangzhou, China, 2008, pp. 362-366.

[22] L. Li, S. Li, H. Zhu, S. C. Chu, J. F. Roddick, and J. S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 46-56, 2013.

[23] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 11, pp. 2274-2282, 2012.

[24] M. P. Bhavya Bhanu and M. N. Arun Kumar, "Copy-move forgery detection using segmentation," in *Proceedings of the 11th International Conference on Intelligent Systems and Control*, Coimbatore, India, 2017, pp. 224-228.

[25] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Taipei, Taiwan, 2009, pp. 1053-1056.

[26] S. Ketenci and G. Ulutas, "Copy-move forgery detection in images via 2D-Fourier transform," in *Proceedings of the 36th International Conference on Telecommunications and Signal Processing*, Rome, Italy, 2013, pp. 813-816.

[27] L. Li, S. Li, and J. Wang, "Copy-move forgery detection based on PHT," in *Proceedings of the World Congress on Information and Communication Technologies*, Trivandrum, India, 2012, pp. 1061-1065.

[28] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proceedings of the International Conference on Computer Science and Software Engineering*, Wuhan, China, 2008, pp. 926-930.

[29] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Proceedings of the 12th International Conference on Information Hiding*, Calgary, AB, Canada, 2010, pp. 51-65.

[30] B. Xu, J. Wang, G. Liu, and Y. Dai, "Image copy-move forgery detection based on SURF," in *Proceedings of the International Conference on Multimedia Information Networking and Security*, Nanjing, China, 2010, pp. 889-892.

[31] J. Zhao and J. Guo, "Passive forensics for region duplication image forgery using Harris feature points and annular average representation," *Journal of Data Acquisition and Processing*, vol. 30, no. 1, pp. 164-174, 2015.

[32] J. M. Guo, Y. F. Liu, and Z. J. Wu, "Duplication forgery detection using improved DAISY descriptor," *Expert Systems with Applications*, vol. 40, no. 2, pp. 707-714, 2013.

[33] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188-197, 2009.

[34] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," *Forensic Science International*, vol. 224, no. 1-3, pp. 59-67, 2013.

[35] R. C. Gonzalez and R. E. Woods, "Morphological image processing," in *Digital Image Processing (3rd ed.)*. Beijing, China: Publishing House of Electronics Industry, 2010, pp. 649-701.

[36] M. A. Fischler and R. C. Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381-395, 1981.

[37] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: a survey," *Digital Investigation*, vol. 10, no. 3, pp. 226-245, 2013.

[38] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1-3, pp. 178-184, 2011.

[39] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, "Copy-move forgery detection technique for forensic analysis in digital images," *Mathematical Problems in Engineering*, vol. 2016, article no. 8713202, 2016.

[40] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Science International*, vol. 214, no. 1-3, pp. 33-43, 2012.

[41] S. M. Fadl and N. A. Semary, "A proposed accelerated image copy-move forgery detection," in *Proceedings of the IEEE Visual Communications and Image Processing Conference*, Valletta, Malta, 2014, pp. 253-257.

[42] E. Mohebbian and M. Hariri, "Increase the efficiency of DCT method for detection of copy-move forgery in complex and smooth images," in *Proceedings of the 2nd International Conference on Knowledge-Based Engineering and Innovation*, Tehran, Iran, 2015, pp. 436-440.

[43] S. Kumar, J. V. Desai, and S. Mukherjee, "Copy move forgery detection in contrast variant environment using binary DCT vectors," *International Journal of Image, Graphics and Signal Processing*, vol. 7, no. 6, pp. 38-44, 2015.

[44] M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Computing and Applications*, 2016. https://doi.org/10.1007/s00521-016-2663-3

[45] H. Wang, H. X. Wang, X. M. Sun, and Q. Qian, "A passive authentication scheme for copy-move forgery based on package clustering algorithm," *Multimedia Tools and Applications*, vol. 76, no. 10, pp. 12627-12644, 2017.

[46] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1-3, pp. 158-166, 2013.

[47] M. Doyoddorj and K. H. Rhee, "Robust copy-move forgery detection based on dual-transform," in *Proceedings of the 5th International Conference on Digital Forensics and Cyber Crime*, Moscow, Russia, 2013, pp. 3-16.

[48] B. Ustubioglu, G. Ulutas, M. Ulutas, V. Nabiyev, and A. Ustubioglu, "LBP-DCT based copy move forgery detection algorithm," in *Proceedings of the 30th International Symposium on Computer and Information Sciences*, London, UK, 2015, pp. 127-136.

[49] A. Kashyap and S. D. Joshi, "Detection of copy-move forgery using wavelet decomposition," in *Proceedings of the International Conference on Signal Processing and Communication*, Noida, India, 2013, pp. 396-400.

[50] S. Mallat and S. Zhong, "Characterization of signals from multiscale edges," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 14, no. 7, pp. 710-732, 1992.

[51] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation*, vol. 9, no. 1, pp. 49-57, 2012.

[52] C. S. Prakash and S. Maheshkar, "Copy-move forgery detection using DyWT," *International Journal of Multimedia Data Engineering and Management*, vol. 8, no. 2, pp. 1-9, 2017.

[53] R. Dixit, R. Naskar, and S. Mishra, "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD," *IET Image Processing*, vol. 11, no. 5, pp. 301-309, 2017.

[54] G. P. Nason and B. W. Silverman, "The stationary wavelet transform and some statistical applications," in *Wavelets and Statistics*. New York, NY: Springer, 1995, pp. 281-299.

[55] A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping," in *Proceedings of the International Conference on Computational Intelligence and Multimedia Applications*, Sivakasi, India, 2007, pp. 371-377.

[56] S. Bravo-Solorio and A. K. Nandi, "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling," in *Proceedings of the 17th European Signal Processing Conference*, Glasgow, UK, 2009, pp. 824-828.

[57] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," *Signal Processing*, vol. 91, no. 8, pp. 1759-1770, 2011.

[58] Q. Wu, S. Wang, and X. Zhang, "Log-polar based scheme for revealing duplicated regions in digital images," *IEEE Signal Processing Letters*, vol. 18, no. 10, pp. 559-562, 2011.

[59] C. S. Park, C. Kim, J. Lee, and G. R. Kwon, "Rotation and scale invariant upsampled log-polar Fourier descriptor for copy-move forgery detection," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16577-16595, 2016.

[60] Y. Yuan, Y. Zhang, S. Chen, and H. Wang, "Robust region duplication detection on log-polar domain using band limitation," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 559-565, 2017.

[61] P. T. Yap, X. Jiang, and A. C. Kot, "Two-dimensional polar harmonic transforms for invariant image representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 7, pp. 1259-1270, 2010.

[62] L. Li, S. Li, H. Zhu, and X. Wu, "Detecting copy-move forgery under affine transforms for image forensics," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1951-1962, 2014.

[63] R. E. J. Granty and G. Kousalya, "Spectral-hashing-based image retrieval and copy-move forgery detection," *Australian Journal of Forensic Sciences*, vol. 48, no. 6, pp. 643-658, 2016.

[64] M. Emam, Q. Han, and X. Niu, "PCET based copy-move forgery detection in images under geometric transforms," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11513-11527, 2016.

[65] X. Bi, C. M. Pun, and X. C. Yuan, "Multi-level dense descriptor and hierarchical feature matching for copy–move forgery detection," *Information Sciences*, vol. 345, pp. 226-242, 2016.

[66] Y. Wo, K. Yang, G. Han, H. Chen, and W. Wu, "Copy–move forgery detection based on multi-radius PCET," *IET Image Processing*, vol. 11, no. 2, pp. 99-108, 2017.

[67] J. Zhong, Y. Gan, J. Young, and P. Lin, "Copy move forgery image detection via discrete Radon and polar complex exponential transform-based moment invariant features," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 31, no. 2, article no. 1754005, 2017.

[68] J. Zhong, Y. Gan, J. Young, L. Huang, and P. Lin, "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools and Applications*, vol. 76, no. 13, pp. 14887-14903, 2017.

[69] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in *Proceedings of the IEEE International Conference on Image Processing*, Hong Kong, China, 2010, pp. 2113-2116.

[70] J. Zhong and Y. Gan, "Detection of copy–move forgery using discrete analytical Fourier–Mellin transform," *Nonlinear Dynamics*, vol. 84, no. 1, pp. 189-202, 2016.

[71] H. Shao, T. Yu, M. Xu, and W. Cui, "Image region duplication detection based on circular window expansion and phase correlation," *Forensic Science International*, vol. 222, no. 1-3, pp. 71-82, 2012.

[72] F. Yavuz, A. Bal, and H. Cukur, "An effective detection algorithm for region duplication forgery in digital images," in *Proceedings of the Conference on Optical Pattern Recognition XXVII*, Baltimore, MD, USA, 2016, pp. 1-7.

[73] S. Dadkhah, M. Koppen, H. A. Jalab, S. Sadeghi, A. A. Manaf, and D. M. Uliyan, "Electromagnetismlike mechanism descriptor with Fourier transform for a passive copy-move forgery detection in digital image forensics," in *Proceedings of the 6th International Conference on Pattern Recognition Applications and Methods*, Porto, Portugal, 2017, pp. 612-619.

[74] D. Y. Huang, C. N. Huang, W. C. Hu, and C. H. Chou, "Robustness of copy-move forgery detection under high JPEG compression artifacts," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1509-1530, 2017.

[75] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," *Forensic Science International*, vol. 231, no. 1-3, pp. 61-72, 2013.

[76] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," in *Proceedings of the IEEE Conference on Open Systems*, Melaka, Malaysia, 2015, pp. 7-11.

[77] P. Yang, G. Yang, and D. Zhang, "Rotation invariant local binary pattern for blind detection of copy-move forgery with affine transform," in *Proceedings of the 2nd International Conference on Cloud Computing and Security*, Nanjing, China, 2016, pp. 404-416.

[78] D. Tralic, S. Grgic, X. Sun, and P. L. Rosin, "Combining cellular automata and local binary patterns for copy-move forgery detection," *Multimedia Tools and Applications*, vol. 75, no. 24, pp. 16681-16903, 2016.

[79] A. Kuznetsov and V. Myasnikov, "A copy-move detection algorithm using binary gradient contours," in *Proceedings of the 13th International Conference on Image Analysis and Recognition*, Povoa de Varzim, Portugal, 2016, pp. 349-357.

[80] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1355-1370, 2013.

[81] O. M. Al-Qershi and B. E. Khoo, "Enhanced matching method for copy-move forgery detection by means of Zernike moments," in *Proceedings of the 13th International Workshop on Digital-Forensics and Watermarking*, Taipei, Taiwan, 2014, pp. 485-497.

[82] G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," *Information Sciences*, vol. 239, pp. 253-265, 2013.

[83] L. T. Thuong, M. Luong, H. K. Tu, P. C. H. Long, and T. H. An, "Block based technique for detecting copy-move digital image forgeries: wavelet transform and Zernike moments," in *Proceedings of the 2nd International Conference on Electrical and Electronic Engineering, Telecommunication Engineering, and Mechatronics*, Las Pinas, Philippines, 2016, pp. 26-33.

[84] K. Mahmoud and A. Abu-Alrukab, "Copy-move forgery detection using Zernike and Pseudo Zernike moments," *The International Arab Journal of Information Technology*, vol. 13, no. 6A, pp. 930-937, 2016.

[85] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 171, no. 2-3, pp. 180-189, 2007.

[86] J. Flusser and T. Suk, "Degraded image analysis: an invariant approach," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 6, pp. 590-603, 1998.

[87] Z. L. Du, X. L. Li, L. X. Jiao, and K. Shen, "Region duplication blind detection based on multiple feature combination," in *Proceedings of the International Conference on Machine Learning and Cybernetics*, Xi'an, China, 2012, pp. 17-21.

[88] M. B. Imamoglu, G. Ulutas, and M. Ulutas, "Detection of copy-move forgery using Krawtchouk moment," in *Proceedings of the 8th International Conference on Electrical and Electronics Engineering*, Bursa, Turkey, 2013, pp. 311-314.

[89] R. Kushol, M. S. Salekin, M. H. Kabir, and A. A. Khan, "Copy-move forgery detection using color space and moment invariants-based features," in *Proceedings of the International Conference on Digital Image Computing: Techniques and Applications*, Gold Coast, QLD, Australia, 2016, pp. 1-6.

[90] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Department of Computer Science, Dartmouth College, Hanover, NH, *Technical Report TR2004-515*, 2004.

[91] P. Kakar and N. Sudha, "Exposing postprocessed copy–paste forgeries through transform-invariant features," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1018-1028, 2012.

[92] A. V. Malviya and S. A. Ladhake, "Pixel based image forensic technique for copy-move forgery detection using Auto Color Correlogram," in *Proceedings of the 7th International Conference on Communication, Computing and Virtualization*, Mumbai, India, 2016, pp. 383-390.

[93] A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A scaling robust copy-paste tampering detection for digital image forensics," in *Proceedings of the 7th International Conference on Communication, Computing and Virtualization*, Mumbai, India, 2016, pp. 458-465.

[94] K. A. Vladimirovich and M. V. Valerievich, "A fast plain copy-move detection algorithm based on structural pattern and 2D Rabin-Karp rolling hash," in *Proceedings of the 11th International Conference on Image Analysis and Recognition*, Vilamoura, Portugal, 2014, pp. 461-468.

[95] A. Kuznetsov and V. Myasnikov, "Using efficient linear local features in the copy-move forgery detection task," in *Proceedings of the International Conference on Analysis of Images, Social Networks and Texts*, Yekaterinburg, Russia, 2016, pp. 305-313.

[96] A. Kashyap, M. Agarwal, and H. Gupta, "Detection of copy-move image forgery using SVD and cuckoo search algorithm," Apr. 3, 2017 [Online]. Available: https://arxiv.org/abs/1704.00631.

[97] C. Barnes, E. Shechtman, A. Finkelstein, and D. B. Goldman, "PatchMatch: a randomized correspondence algorithm for structural image editing," *ACM Transactions on Graphics*, vol. 28, no. 3, article no. 24, 2009.

[98] D. Cozzolino, G. Poggi, and L. Verdoliva, "Copy-move forgery detection based on PatchMatch," in *Proceedings of the IEEE International Conference on Image Processing*, Paris, France, 2014, pp. 5312-5316.

[99] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching," in *Proceedings of the IEEE International Conference on Image Processing*, Paris, France, 2014, pp. 5297-5301.

[100] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy–move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284-2297, 2015.

[101] M. Hussain, S. Q. Saleh, H. Aboalsamh, G. Muhammad, and G. Bebis, "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection," in *Proceedings of the IEEE International Symposium on Innovations in Intelligent Systems and Applications*, Alberobello, Italy, 2014, pp. 197-204.

[102] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, vol. 25, no. 4, pp. 985-995, 2014.

[103] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *Proceedings of the IEEE International Workshop on Information Forensics and Security*, Abu Dhabi, United Arab Emirates, 2016, pp. 1-6.

[104] G. Schaefer and M. Stich, "UCID: an uncompressed colour image database," in *Proceedings of the Conference on Storage and Retrieval Methods and Applications for Multimedia*, San Jose, CA, USA, 2004, pp. 472-480.

[105] National Geographic [Online]. Available: http://www.nationalgeographic.com/photography/.

[106] J. Deng, W. Dong, R. Socher, L. J. Li, K. Li, and F. F. Li, "ImageNet: a large-scale hierarchical image database," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Miami, FL, USA, 2009, pp. 248-255.

[107] Kodak Lossless True Color Image Suite [Online]. Available: http://r0k.us/graphics/kodak/.

[108] Database for object and concept recognition [Online]. Available: http://www.cs.washington.edu/research/imagedatabase/groundtruth/.

[109] T. T. Ng, S. F. Chang, J. Hsu, and M. Pepeljugoski, "Columbia photographic images and photorealistic computer graphics dataset," Columbia University, New York, NY, *ADVENT Technical Report #205-2004-5*, 2005.

[110] The USC-SIPI Image Database [Online]. Available: http://sipi.usc.edu/database/.

[111] G. Griffin, A. Holub, and P. Perona, "Caltech-256 object category dataset," California Institute of Technology, Los Angeles, CA, USA, *Technical Report 7694*, 2007.

[112] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery," *Machine Vision and Applications*, vol. 25, no. 2, pp. 451-475, 2014.

[113] L. Yu, Q. Han, and X. Niu, "Feature point-based copy-move forgery detection: covering the non-textured areas," *Multimedia Tools and Applications*, vol. 75, no. 2, pp. 1159-1176, 2016.

[114] M. Emam, Q. Han, L. Yu, and H. Zhang, "A keypoint-based region duplication forgery detection algorithm," *IEICE Transactions on Information and Systems*, vol. E99-D, no. 9, pp. 2413-2416, 2016.

[115] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Proceedings of the IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Wuhan, China, 2008, pp. 272-276.

[116] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Dallas, TX, USA, 2010, pp. 1702-1705.

[117] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[118] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 659-669, 2013.

[119] G. Jin and X. Wan, "An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage," *Signal Processing: Image Communication*, vol. 57, pp. 113-125, 2017.

[120] V. Anand, M. F. Hashmi, and A. G. Keskar, "A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and SIFT methods," in *Proceedings of the 6th Asian Conference on Intelligent Information and Database Systems*, Bangkok, Thailand, 2014, pp. 530-542.

[121] J. Gong and J. Guo, "Exposing region duplication through local geometrical color invariant features," *Journal of Electronic Imaging*, vol. 24, no. 3, article no. 033010, 2015.

[122] P. P. Panzade, C. S. Prakash, and S. Maheshkar, "Copy-move forgery detection by using HSV preprocessing and keypoint extraction," in *Proceedings of the 4th International Conference on Parallel, Distributed and Grid Computing*, Waknaghat, India, 2016, pp. 264-269.

[123] F. Zhao, W. Shi, B. Qin, and B. Liang, "Analysis of SIFT method based on swarm intelligent algorithms for copy-move forgery detection," in *Proceedings of the 9th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, China, 2016, pp. 478-490.

[124] W. Shi, F. Zhao, B. Qin, and B. Liang, "Improving image copy-move forgery detection with particle swarm optimization techniques," *China Communications*, vol. 13, no. 1, pp. 139-149, 2016.

[125] R. K. Karsh, A. Das, G. L. Swetha, A. Medhi, R. H. Laskar, U. Arya, and R. K. Agarwal, "Copy-move forgery detection using ASIFT," in *Proceedings of the 1st India International Conference on Information Processing*, Delhi, India, 2016, pp. 1-5.

[126] A. R. H. Khayeat, X. Sun, and P. L. Rosin, "Improved DSIFT descriptor based copy-rotate-move forgery detection," in *Proceedings of the 7th Pacific-Rim Symposium on Image and Video Technology*, Auckland, New Zealand, 2015, pp. 642-655.

[127] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015.

[128] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Salleh, and F. Othman, "SIFT-symmetry: a robust detection method for copy-move forgery with reflection attack," *Journal of Visual Communication and Image Representation*, vol. 46, pp. 219-232, 2017.

[129] B. L. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *International Journal of Computer Science Issues*, vol. 8, no. 4, pp. 199-205, 2011.

[130] P. Mishra, N. Mishra, S. Sharma, and R. Patel, "Region duplication forgery detection technique based on SURF and HAC," *The Scientific World Journal*, vol. 2013, article no. 267691, 2013.

[131] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *Journal of Visual Communication and Image Representation*, vol. 29, pp. 16-32, 2015.

[132] B. Yang, X. Sun, X. Xin, W. Hu, and Y. Wu, "Image copy–move forgery detection based on sped-up robust features descriptor and adaptive minimal–maximal suppression," *Journal of Electronic Imaging*, vol. 24, no. 6, article no. 063016, 2015.

[133] L. Chen, W. Lu, J. Ni, W. Sun, and J. Huang, "Region duplication detection based on Harris corner points and step sector statistics," *Journal of Visual Communication and Image Representation*, vol. 24, no. 3, pp. 244-254, 2013.

[134] J. Zhao and W. Zhao, "Passive forensics for region duplication image forgery based on Harris feature points and local binary patterns," *Mathematical Problems in Engineering*, vol. 2013, article no. 619564, 2013.

[135] X. Wang, G. He, C. Tang, Y. Han, and S. Wang, "Keypoints-based image passive forensics method for copy-move attacks," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 3, article no. 1655008, 2016.

[136] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, and S. Sadeghi, "Image region duplication forgery detection based on angular radial partitioning and Harris key-points," *Symmetry*, vol. 8, no. 7, article no. 62, 2016.

[137] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy–move forgery detection by matching triangles of keypoints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2084-2094, 2015.

[138] R. C. Pandey, S. K. Singh, K. K. Shukla, and R. Agrawal, "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," in *Proceedings of the 9th International Conference on Industrial and Information Systems*, Gwalior, India, 2014, pp. 1-6.

[139] S. Kumar, J. V. Desai, and S. Mukherjee, "A fast keypoint based hybrid method for copy move forgery detection," *International Journal of Computing and Digital Systems*, vol. 4, no. 2, pp. 91-99, 2015.

[140] M. M. Isaac and M. Wilscy, "Copy-move forgery detection based on Harris corner points and BRISK," in *Proceedings of the 3rd International Symposium on Women in Computing and Informatics*, Kochi, India, 2015, pp. 394-399.

[141] R. C. Pandey, R. Agrawal, S. K. Singh, and K. K. Shukla, "Passive copy move forgery detection using SURF, HOG and SIFT features," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications*, Bhubaneswar, India, 2014, pp. 659-666.

[142] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," in *Proceedings of the IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, Bangalore, India, 2016, pp. 706-710.

[143] M. Emam, Q. Han, and H. Zhang, "Two-stage keypoint detection scheme for region duplication forgery detection in digital images," *Journal of Forensic Sciences*, vol. 63, no. 1, pp. 102-111, 2018.

[144] F. Yang, J. Li, W. Lu, and J. Weng, "Copy-move forgery detection based on hybrid features," *Engineering Applications of Artificial Intelligence*, vol. 59, pp. 73-83, 2017.

[145] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841-1854, 2012.

[146] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—new database for copy-move forgery detection," in *Proceedings of the 55th International Symposium on ELMAR*, Zadar, Croatia, 2013, pp. 49-54.

[147] G. Serra, "MICC-F600, MICC-F220, MICC-F2000, and MICC-F8multi," [Online]. Available: http://giuseppeserra.com/content/sift-based-forensic-method-copy-move-detection.

[148] National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, "CASIA image tampering detection evaluation database (CASIA TIDE) v1.0, v2.0," [Online]. Available: http://forensics.idealtest.org.

[149] B. Wen, Y. Zhu, R. Subramanian, T. T. Ng, X. Shen, and S. Winkler, "COVERAGE–a novel database for copy-move forgery detection," in *Proceedings of the IEEE International Conference on Image Processing*, Phoenix, AZ, USA, 2016, pp. 161-165.

[150] T. T. Ng and S. F. Chang, "A data set of authentic and spliced image blocks," Columbia University, New York, NY, *ADVENT Technical Report #203-2004-3*, 2004.

[151] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics," in *Proceedings of the 8th IEEE International Conference on Computer Vision*, Vancouver, Canada, 2001, pp. 416-423.

[152] R. Salakhutdinov and G. Hinton, "Deep Boltzmann machines," in *Proceedings of the 12th International Conference on Artificial Intelligence and Statistics*, Clearwater, FL, USA, 2009, pp. 448-455.

[153] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proceedings of the 26th Annual Conference on Neural Information Processing Systems*, Lake Tahoe, NV, USA, 2012, pp. 1097-1105.

Zhi Zhang https://orcid.org/0000-0002-1476-6790

He was born in Shandong province, China, in 1992. He received his B.E. degree in electronic information engineering from Shandong University of Science and Technology, China, in 2016. He is currently pursuing his M.E. degree in information and communication engineering at Shandong University, China. His current research interests include image watermarking, forgery detection, and computer vision.

Chengyou Wang https://orcid.org/0000-0002-0901-2492

He was born in Shandong province, China, in 1979. He received his M.E. and Ph.D. degrees in signal and information processing from Tianjin University, China, in 2007 and 2010, respectively. He is currently an associate professor and supervisor of postgraduate students at Shandong University, Weihai, China. His current research interests include image/video processing and analysis, computer vision, and wireless communication technology.

Xiao Zhou https://orcid.org/0000-0002-1331-7379

She was born in Shandong province, China, in 1982. She received her M.E. degree in information and communication engineering from Inha University, Korea, in 2005; and her Ph.D. degree in information and communication engineering from Tsinghua University, China, in 2013. She is currently a lecturer and supervisor of postgraduate students at Shandong University, Weihai, China. Her current research interests include wireless communication technology, digital image processing, and computer vision.