



Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering

Muhammad Bilal¹ · Hafiz Adnan Habib² · Zahid Mehmood² · Tanzila Saba³ · Muhammad Rashid⁴

Received: 24 June 2019 / Accepted: 6 November 2019 / Published online: 16 November 2019
© King Fahd University of Petroleum & Minerals 2019

Abstract

Due to the advancements in digital image processing and multimedia devices, the digital image can be easily tampered and presented as evidence in judicial courts, print media, social media, and for insurance claims. The most commonly used image tampering technique is the copy-move forgery (CMF) technique, where the region from the original image is copied and pasted in some other part of the same image to manipulate the original image content. The CMFD techniques may not provide robust performance after various post-processing attacks and multiple forged regions within the images. This article introduces a robust CMF detection technique to mitigate the aforementioned problems. The proposed CMF detection technique utilizes a fusion of speeded up robust features (SURF) and binary robust invariant scalable keypoints (BRISK) descriptors for CMF detection. The SURF features are robust against different post-processing attacks such as rotation, blurring, and additive noise. However, the BRISK features are considered as robust in the detection of the scale-invariant forged regions as well as poorly localized keypoints of the objects within the forged image. The fused features are matched using hamming distance and second nearest neighbor. The matched features grouped into clusters by applying density-based spatial clustering of applications with noise clustering algorithm. The random sample consensus technique is applied to the clusters to remove the remaining false matches. After some post-processing, the forged regions are detected and localized. The performance of the proposed CMFD technique is assessed using three standard datasets (i.e., CoMoFoD, MICC-F220, and MICC-F2000). The proposed technique surpasses the state-of-the-art techniques used for CMF detection in terms of true and false detection rates.

Keywords Forgery detection · SURF features · BRISK features · DBSCAN clustering

1 Introduction

In this age of information, the use of digital images and videos as personal memories and social awareness is increasing rapidly. A large number of individuals and organizations are

using easily available and simple digital image modification tools for image modifications. There are commonly three motives where image manipulation tools are used, i.e., the image stenography, the image digital watermarking, and the image forgery. In the image stenography, sensitive information is hidden in the image [1–4]. In the image digital watermarking, the authentication data or copyright information is hidden into the image, to identify the authorization and ownership of the digital image and restrict the digital image from being tampered or from unauthorized distribution [5, 6]. In the image, forgery is used to manipulate and hide the original content of the image and used the forged image in unlawful and unethical purposes [7]. The examples for illegal use of image forgery are; presenting the forged images in a courtroom as evidence, spreading the forged images as propaganda to initiate chaos in the society, to blackmail an individual with forged images, broadcasting the false

✉ Zahid Mehmood
zahid.mehmood@uettaxila.edu.pk

¹ Department of Software Engineering, University of Engineering and Technology, Taxila, Pakistan
² Department of Computer Engineering, University of Engineering and Technology, Taxila, Pakistan
³ College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia
⁴ Department of Computer Engineering, Umm Al-Qura University, Mecca, Saudi Arabia

information by using forged images for particular person or organization gain.

In literature, there are two types of forgery detection techniques, active (non-blind) and passive (blind) technique. In the active technique, the data are embedded in the original image, which is later used to check the authenticity of the image by extracting and matching the embedded data [8]. However, the major drawback of the active technique for its usage in the forensic application is that it requires the prior knowledge of the embedded data [9].

To cope with the forensic application, the passive technique is used widely in forensic application [9]. The passive technique does not require any additional information to detect the CMF in the forged image; it uses the information present in a tampered image to identify the forged regions. It is widely acknowledged that there are two types of image forgery, one is CMF and the other is image splicing. In CMF one or more regions from the original image are counterfeit on some other region of the same image to hide or manipulate the original image content [11]. While in image splicing, the regions from one or more images are imitated on some other image. The example of CMF is shown in Fig. 1, where it is very difficult with the naked eye to identify the forgery. The result of image forgery detection can be categorized as; (1) an input image either forged or not forged without localization of forged region and other (2) where a forged region in a digital image is localized within the same image if detected as forged image [12].

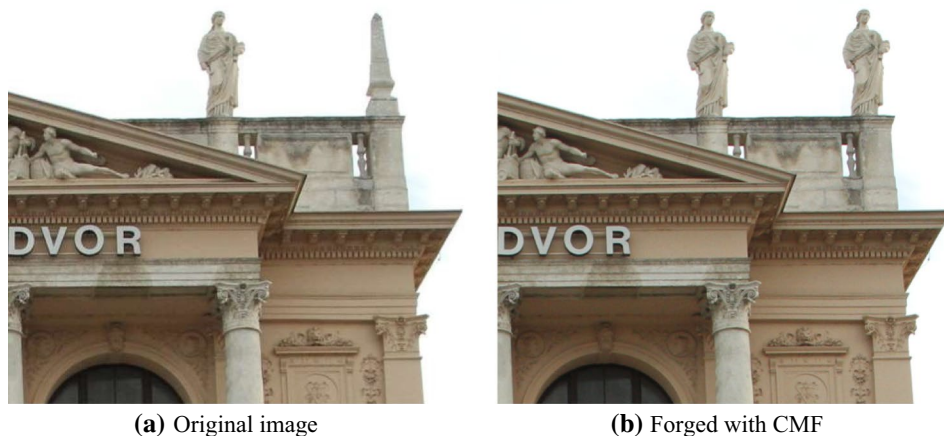
The proposed CMFD technique of this article uses a passive technique for CMFD, with the ability to localize the tampered regions in the image. To make the proposed technique fast, robust, and accurate, the discrete wavelet transform (DWT), SURF technique and BRISK technique have been utilized. The aim of using DWT in the proposed technique is to get only the most robust and appropriate features from DWT approximate sub-band to reduce the

computational cost [13]. Using SURF and BRISK, only the worthy and effective keypoints are detected, and features are extracted due to the refinement from DWT. The SURF [14] features allow detecting the forged regions even after post-processing attacks like rotation, blurring, color reduction, contrast adjustment, JPEG compression, additive noise, and brightness change of the forged region [15, 16]. The BRISK is generally robust against all possible transformation especially post-processing attacks like scaling and can detect most unique features from forged regions in CMF [17]. The features from SURF and BRISK are fused vertically with a descriptor length of $64 \times N$ each. These fuse features are then matched using Hamming distance and 2NN; Hamming distance is used because of the fact that BRISK can utilize the Hamming greatly [17]. Using density-based spatial clustering of application with noise (DBSCAN), the match features are group together into clusters, which aid in mitigating some false matches [18]. After that, the random sample consensus (RANSAC) technique is used to remove the residual false matches from the matched features in the previous step. The RANSAC estimates the parameters of a model from data provide with outliers (i.e., false matches) and inliers (i.e., true matches) to remove the outliers. The proposed CMFD technique shows better results compare with state-of-the-art CMFD technique.

The main achievements of the proposed CMFD technique are as follows:

- (1) The fusion of sparse features based on the SURF and BRISK descriptors to achieve a complementary effect in CMF detection.
- (2) Ability to detect single and multiple forged regions in a digital image.
- (3) Capacity to detect the forged regions even after post-processing attacks like scaling, rotation, blurring, color

Fig. 1 Example of CMF [10]



reduction, contrast adjustment, JPEG compression, additive noise, and brightness change.

- (4) Mitigate the computational cost for forgery detection by plummeting the feature vector size and narrowing down the matching area.

2 Related Work

The CMF is the most common image forgery technique due to its simple nature. Therefore, researchers have proposed many CMF detections over the past few years [19–23]. Fridrich et al. [24] propose the very first technique in CMF detection. The technique divides the image in small overlapped block and extracts feature based on the discrete cosine transform (DCT) coefficient. The extracted features then lexicographically sorted and matched for the detection of the forged regions. A block-based technique is presented by Lin et al. [25], which divides the input image the equal-sized overlapping blocks followed by feature extraction and storing them as an integer. The extracted features are then rearrange using radix sort and match using by comparing the accumulated numbers of each block feature vector. Ardizzone et al. [26] compare the features in a triangle rather than in the fixed-size block to detect forged regions. These triangles are matched according to their shape, content in the triangle, and local features. The drawback of this technique is unable to identify the forged region with affine transformation. A medley of DCT and DWT by Hayat et al. [13] is proposed in which DCT is used to extract features and then reduce them using DWT, respectively. Finally, the correlation coefficient between all row vectors is calculated to detect duplicated blocks. However, it does not perform well in the presence of occlusion and multiple forged regions.

A block-based technique is proposed by Alkawaz et al. [27], which uses discrete cosine transform (DCT) which can accurately detect the forged regions in the image. The image features are created by rearranging 2D-DCT coefficient. The forged regions are detected by calculating and comparing Euclidean distance between blocks. The performance of the CMFD technique greatly depends on the size of the block, wrongly chosen block size leads to a decrease in accuracy of the CMFD technique. Silva et al. [18] present a technique for CMFD which uses keypoint-based descriptor called SURF for feature extraction. To reduce the complexity of the technique, the author uses the clustering technique to reduce the area under the observation. This technique underperforms in JPEG compression post-processing attack. Another keypoint-based CMFD technique is proposed by Li et al. [28], which segmented the input forged image into the patches followed by keypoint extraction, which are compared with each other using affine transform matrix and expectation–maximization-based algorithm to detect CMF in the input image.

However, due to the complex matching process, the computational cost of the proposed technique has increased.

In [29], a review on different keypoint-based CMFD techniques is performed, which uses different keypoint-based descriptors like scale-invariant feature transform (SIFT) and SURF for feature extraction. The study shows that the SURF-based technique performs better than a SIFT-based technique for CMFD in terms of accuracy and computational cost. Another review by Farid H. [30] has discussed different passive forgery detection techniques, i.e., pixel-based, format-based, camera-based, physical-based, and geometric-based techniques. The study shows that above-mentioned passive forgery detection techniques work well by exploiting the information present in the forged image to detect forgeries. However, with the advancement in digital image processing, forgery detection becoming more and more difficult. Manu et al. [31] propose a dense field technique, which uses a fast approximation nearest neighbor search algorithm and patch match technique. The technique relies on polar cosine transform (PCT), Fourier–Mellin transforms (FMT), and Zernike Moments (ZM). The technique performs well rotational invariant post-processing, but computational cost is high and low accuracy.

A multi-level dense descriptor (MLDD) proposed by Bi et al. [32] is used to extract features and perform geometric invariant moments-based matching. This technique requires less computational cost. Yuan et al. [33] propose a deep learning-based technique for image forgery detection which uses a convolutional neural network (CNN). The CNN is used to learn hierarchical representation from an RGB color image. To detect the forged regions, it extracts the features from the image provided in test images where CNN plays the role of patch descriptor. The accuracy of this technique is high but it requires a high computational cost. A novel keypoint-based technique for CMFD is proposed by Zandi et al. [34] to detect a forgery in the image by utilizing the advantages of block-based and traditional keypoint-based descriptors. The technique iterates to adjust the density of the keypoint descriptor based on the achieved information. The technique performs well as compared with state-of-the-art CMFD techniques for various post-processing attacks like rotation invariance, additive white noise, JPEG compression, and blurring; however, its performance decreases if scaling is applied to forged regions of the image.

A hybrid CMFD technique is proposed by Yang et al. [35]. This technique combines the features based on the KAZE and SIFT feature descriptors. The hybrid features are matched, and affine transformation estimation is applied to remove false matches. This technique produces good results even if extreme geometrical transformation is applied in the forged regions of the image. Another technique based on the hybrid features (i.e., SIFT, SURF, and HOG feature descriptors) is proposed by Pandey et al. [36] to detect CMF in the

image. This technique produces better performance; however, it requires a high computational cost. Yu et al. [37] propose a technique that uses MROGH and hue histogram (HH) descriptor. The proposed technique performs well when compared to the SIFT and SURF-based techniques for CMF detection. This technique produces a satisfactory result in various post-processing attacks e.g., rotation and JPEG compression, but underperforms if forged regions subjected to scaling and additive noise.

3 The Methodology of the Proposed CMFD Technique

The foundation of the proposed CMFD technique is based on DWT, hybrid features (i.e., SURF and BRISK), clustering based on the DBSCAN, and RANSAC. The block diagram of the proposed CMFD technique is shown in Fig. 2, and the detail description of each step is provided in the following subsequent sections.

3.1 Pre-processing

In the first step of the proposed technique, the input forged image is converted into the grayscale using Eq. (1).

$$Y = (2.99)R + (0.587)G + (0.114)B \quad (1)$$

where Y denotes the luminance and R , G , and B denotes the red, green, and blue pixels values of the color image. The

grayscale conversion of the input forged image reduces the computational cost of the proposed CMFD technique.

3.2 Discrete Wavelet Transform (DWT)

In this step, the DWT is applied to the grayscale input forged image. The DWT divides the forged image into four sub-bands, i.e., approximation (LL), horizontal (LH), vertical (HL), and diagonal (HH). In the proposed CMFD technique, the level-2 approximation sub-band is chosen since most energetic information of the image lies in this sub-band [38], hence reduce the computational cost of the proposed CMFD technique. The level-2 approximation coefficients of the DWT can be obtained by Eq. (2).

$$y'_{\text{low}} = (((Y * g) \downarrow 2) * g) \downarrow 2 \quad (2)$$

where Y is the input grayscale forged image passed through the filter g , and y'_{low} denotes the approximation coefficients of the level-2 DWT, which can also be illustrated in Fig. 3.

The filtration through level-2 approximation coefficients enables the pre-processing forged image to extract only the most energy-rich features by SURF and BRISK descriptor in the next step.

3.3 Features Extraction Using SURF and BRISK

After applying DWT to the input image, the SURF and BRISK descriptors are used to extract features. The detail

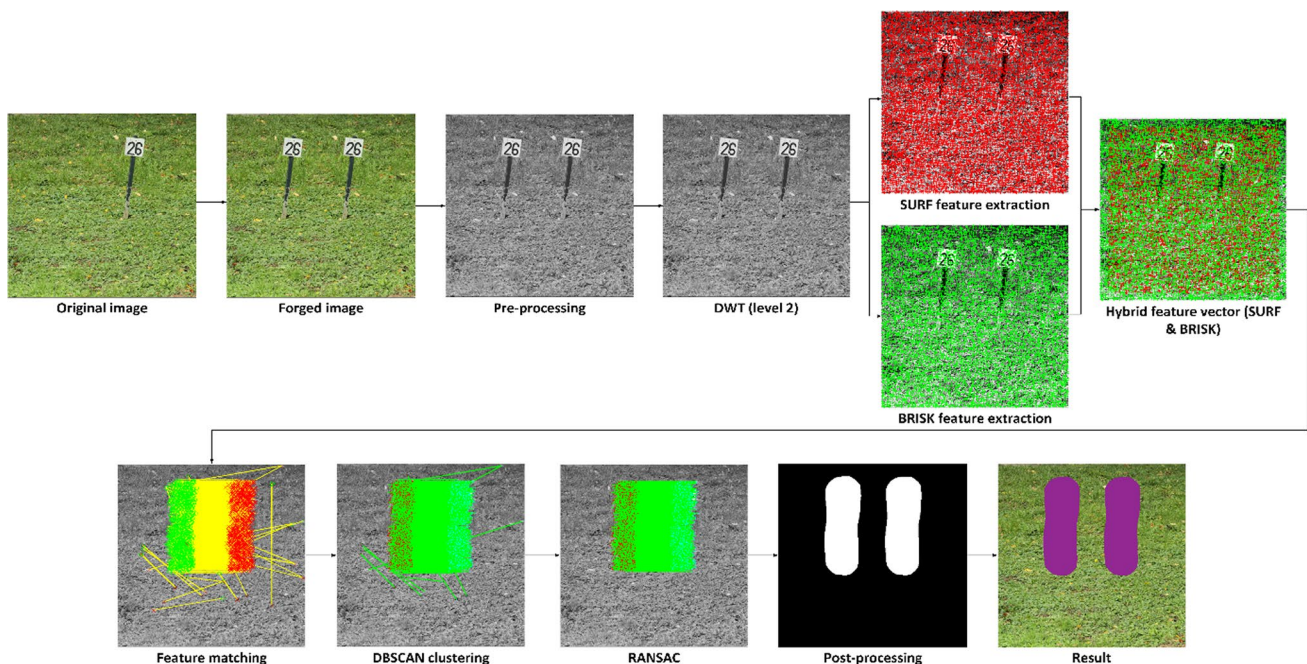


Fig. 2 Block diagram of the proposed CMF detection technique based on the sparse features and DBSCAN clustering applied on the forged image of the CoMoFoD dataset [10]



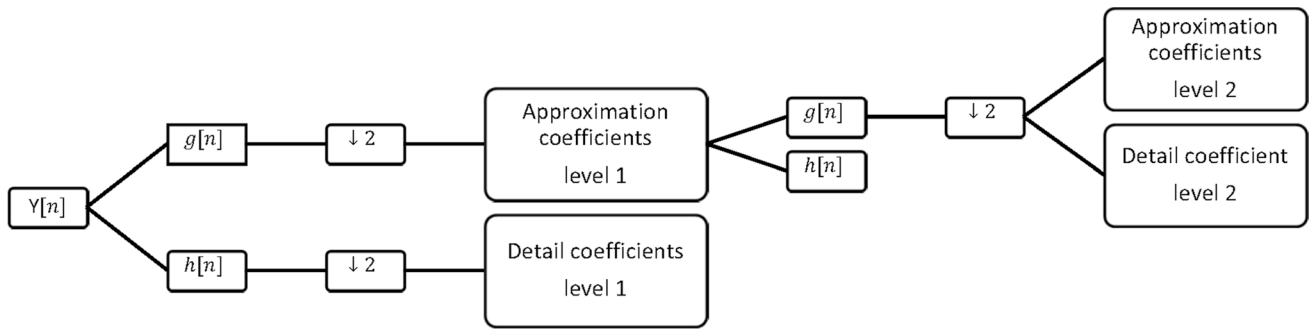


Fig. 3 Level-2 filter analysis of DWT

sub-sections about SURF and BRISK descriptor are as follow:

3.3.1 Features Extraction Using a SURF Descriptor

The SURF descriptor is not only fast but also robust against translation and affine transformation even in the presence of the noise [39]. The SURF descriptors are considered to be better than the other descriptors in terms of speed and robustness [40]. The SURF uses Hessian matrix determinant to select the keypoint [14] as expressed in Eq. (3)

$$H(i, \sigma) = \begin{bmatrix} L_{xx}(i, \sigma) & L_{xy}(i, \sigma) \\ L_{yx}(i, \sigma) & L_{yy}(i, \sigma) \end{bmatrix} \quad (3)$$

where $H(i, \sigma)$ is Hessian matrix at point $i = (x, y)$ in the y'_{low} with scale σ , $L_{xx}(i, \sigma)$, $L_{xy}(i, \sigma)$, $L_{yx}(i, \sigma)$, and $L_{yy}(i, \sigma)$ are the convolution of the second order of Gaussian with $m(x, y)$ at point i [14].

The Hessian matrix uses a box filter to take approximation by taking second-order Gaussian derivatives to reduce computational cost as they can be efficiently computed using the independent size of integral images. The selected box filter in the Hessian matrix is of 9×9 with $\sigma = 1.2$ for Gaussian second-order approximation coefficients [14]. Now consider these approximation coefficients (i.e., A_{xx} , A_{yy} , and A_{xy}), the Hessian matrix uses Eq. (4) for fast and accurate approximation calculation for the Hessian determinant.

$$|H_{approx}| = A_{xx} * A_{yy} - (0.9A_{xy})^2 \quad (4)$$

where $\left| \frac{L_{xy}(1.2)_F |A_{xx}(9)_F| / L_{xx}(1.2)_F |A_{xy}(9)_F|}{L_{xx}(1.2)_F |A_{xy}(9)_F|} = 0.9 \right|$ is relative weight to balancing the Hessian determinant and $|x|_F$ is Frobenius norm.

The next step is the extraction of the feature descriptors from DoG approximation. This process consists of two steps, in the first step, an orientation-based assignment around the detected interest point is conducted. The calculation for orientation uses Haar wavelet response with Gaussian at interest

point with $\sigma = 2.5$ s. Subsequently, the horizontal and vertical wavelet responses are sum up with rotating edge to calculate the dominant orientation. This dominant orientation is taken as interest point descriptor.

In the second step of the extraction of the feature descriptors, the filter region is divided into small sub-regions. From each sub-regions, the d_x the horizontal and d_y the vertical wavelet responses are then sum up for each sub-region to produce the set of features. For polarity information of intensities, the absolute values of responses $|d_x|$ and $|d_y|$ are also calculated [14]. This gives four-dimensional descriptor vector V as expressed in Eq. (5).

$$V = \left(\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y| \right) \quad (5)$$

Concatenating the dimensions of each sub-region result give $64 \times N$ feature vector. The extracted features using the SURF descriptor are now ready to fuse with BRISK features extracted in the next sub-section.

3.3.2 Features Extraction Using a BRISK Descriptor

In this step, the features are extracted from the forged image by applying the BRISK descriptor. It is a binary feature description technique [17]. One of the main advantages of using BRISK is its robustness against scale invariance. For feature selection, BRISK uses a sampling pattern as shown in Fig. 4.

In Fig. 4, the blue dots indicate the location and the dashed lines in red color indicate the radius r_i , which is based on the Gaussian kernel to smooth the sampling-point intensity values to avoid aliasing at point n_i in the pattern; hence, the local gradient can be calculated by Eq. (6).

$$g(n_i, n_j) = (n_j - n_i) * \frac{(I(n_j, \sigma_j) - I(n_i, \sigma_i))}{\|n_j - n_i\|^2} \quad (6)$$

where $g(n_i, n_j)$ is a local gradient, (n_i, n_j) represent the sampling-point pairs, $I(n_i, \sigma_i)$ and $I(n_j, \sigma_j)$ are smoothed

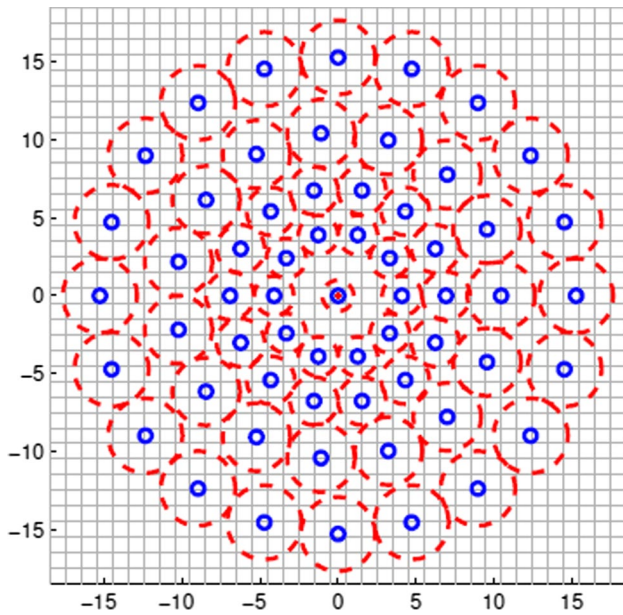


Fig. 4 Sampling pattern for BRISK with $P=60$ points [17]

intensities values. To identify the scale invariance in BRISK, it uses sampling pattern around keypoint k rotated by $\alpha = \arctan 2(g_x, g_y)$. The calculation of bit-vector d_k is performed by comparing all the short-distance sampling-point pairs $(n_i^\alpha, n_j^\alpha) \in S_s$, so that every bit b is either 1 or 0 as shown in Eq. (7). The length of bit-vector d_k is $64 \times N$ with keypoint in the range specified by $[\delta_{\text{minimum}} \delta_{\text{maximum}}]$.

$$b = \begin{cases} 1, & I(n_j^\alpha, \sigma_j) > I(n_i^\alpha, \sigma_i) \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

$$\forall (n_i^\alpha, n_j^\alpha) \in S_s$$

The features extracted using the BRISK descriptor are fuse with the features extracted in the previous sub-section using the SURF descriptor in Eq. (5), vertically as both features have the same dimension as shown in Fig. 5.

3.4 Feature Matching

In this step, the fused features from SURF and BRISK are matched. The Hamming distance is utilized for feature matching in the proposed technique, as it is beneficial for BRISK features matching. The set $D = \{d_1, d_2, \dots, d_{n-1}\}$ is the sorted Hamming distance correspondence to the other features. Now, the 2NN test is carried out by calculating the ratio of closest Hamming distance and second closest Hamming distance. This ratio is compared with a threshold T (which is set to 0.6) as defined in Eq. (8).

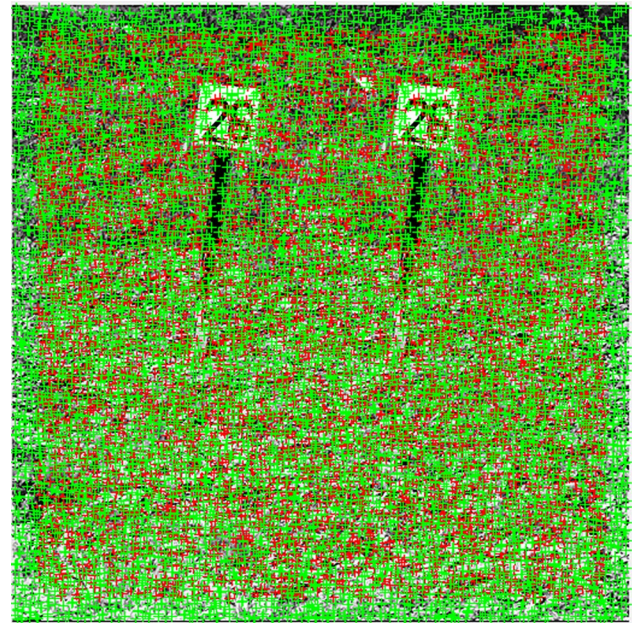


Fig. 5 Result of the fused features of SURF (red) and BRISK (green) descriptors

$$\frac{d_1}{d_2} \leq T, T \in (0, 1) \quad (8)$$

The 2NN is repeated on d_i and d_{i+1} until T is less than the ratio. Now, if the total repetitions are k then there are a total of k matches for the point under inspection.

The matched points are shown in Fig. 6. There are lots of false matches in the match features. The false matches are reduced by applying DBSCAN clustering in the next sub-section.

3.5 Clustering Using DBSCAN

It has been widely observed that the match keypoints in the input forged image are denser than the wrongly matched keypoints, as shown in Fig. 6. DBSCAN, a clustering technique, which produces excellent results in the field based on spatial clustering applications [41, 42]. This clustering technique also uses the information that the true match keypoints are denser than the false match keypoints in the cluster.

Firstly, the density of keypoints around each keypoint within the cluster is calculated in DBSCAN. This density calculation acts as an influence function of all keypoints present in the cluster on the particular keypoint present in the same cluster. This influence can be mathematically described as in Eq. (9).

$$I(a, b) = \sqrt{\sum_{d=1}^n (a_d - b_d)^2} \quad (9)$$

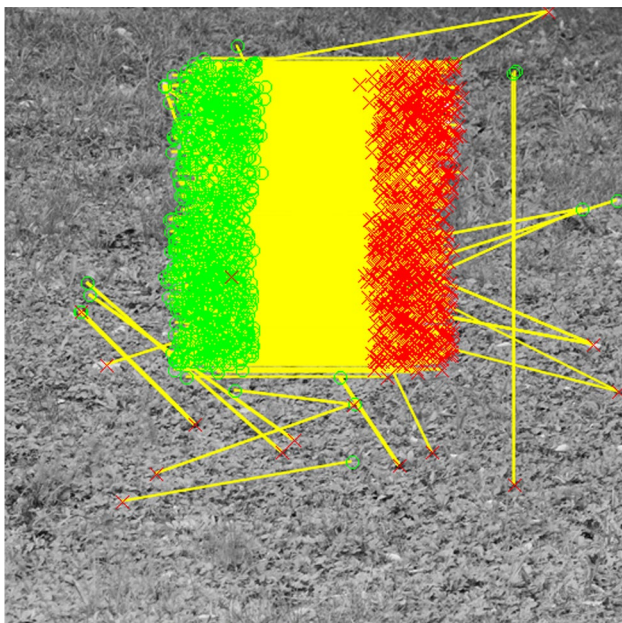


Fig. 6 SURF and BRISK features are matching with some false matches

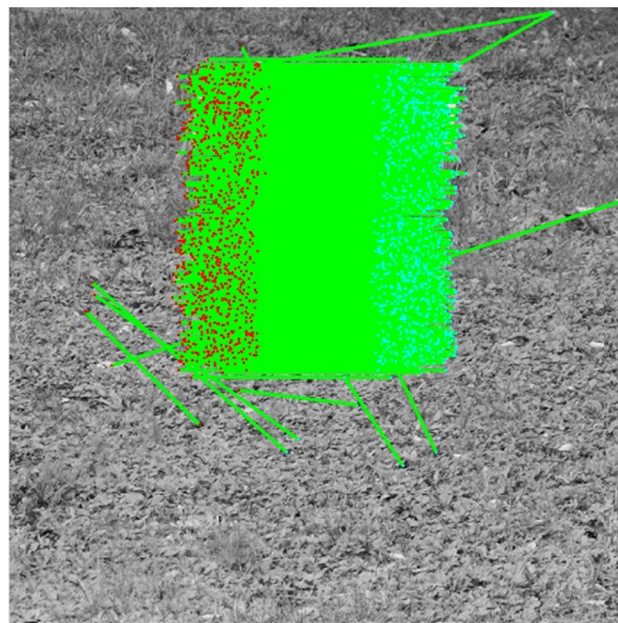


Fig. 7 Clustering and false match removal of match features

where the influence $I(a, b)$ of keypoint a on keypoint b is simply an Euclidean distance between both keypoints. The Euclidean distance and impact of keypoint a on to the keypoint b are inversely proportional to each other. As the distance increases, the impact of keypoint a on to the keypoint b decreases, and vice versa [41].

In the next step, the local density of keypoint a is calculated by summing all the influence of keypoint a with its m -nearest neighbors' distance. This summation can be described mathematically as in Eq. (10).

$$D(a, b_1, b_2, \dots, b_m) = \sum_{x=1}^m I(a, b_x) \tag{10}$$

where the m -nearest neighbors for keypoint a are calculated and rearrange it in ascending order using quick sort according to their distance to the keypoint a . By calculating the ratio of keypoint density a with a total number of m nearest neighbors, the clusters are generated.

The DBSCAN clustering technique removed some false match feature but some of the false matches are still present in the cluster-based result as shown in Fig. 7. The detail discussion on removing the remaining false match region from the forged image is mentioned in the next step.

3.6 False Match Region Removal Using RANSAC

The clustering in the previous step can remove some false matches, but not all of them. In this step, the residual false

matches in the cluster are removed. The proposed technique uses random sample consensus (RANSAC) technique for this purpose [43]. RANSAC estimates the parameters of a model from data provide with outliers (i.e., false matches) and inliers (i.e., true matches). The RANSAC uses a transformation matrix to estimate the outliers, as described in Eq. (11).

$$H \begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix} = \begin{pmatrix} a_j \\ b_j \\ 1 \end{pmatrix} \tag{11}$$

where H is a transformation matrix with scaling, rotation, and shearing. Also, $\begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix}$ and $\begin{pmatrix} a_j \\ b_j \\ 1 \end{pmatrix}$ are the location at i and j point. Now, based on the transformation matrix H , as in Fig. 8, all the false matches are eliminated that are not attuned with the H .

The RANSAC can remove the remaining false match features that are left from DBSCAN clustering. This step contributes well in improving the proposed CMFD technique accuracy.

3.7 Post-processing and Localization

In the final step, the morphological operation is applied to the resultant image from the previous sub-section. If the binary mask is all black, then no forged region is present

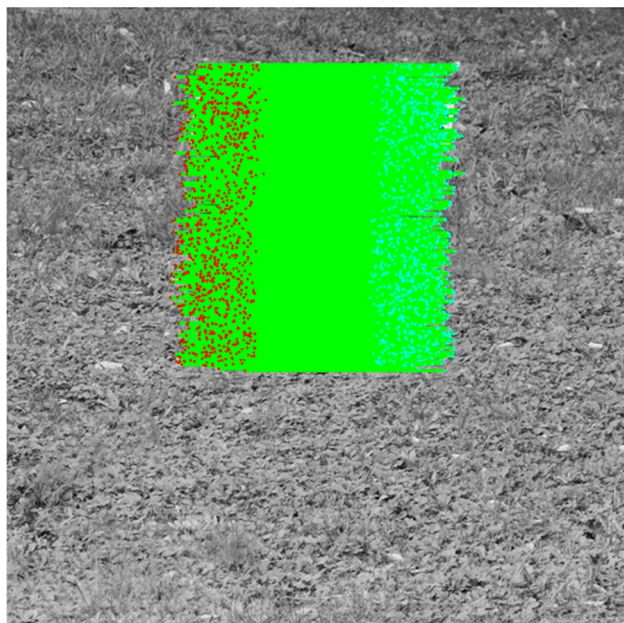
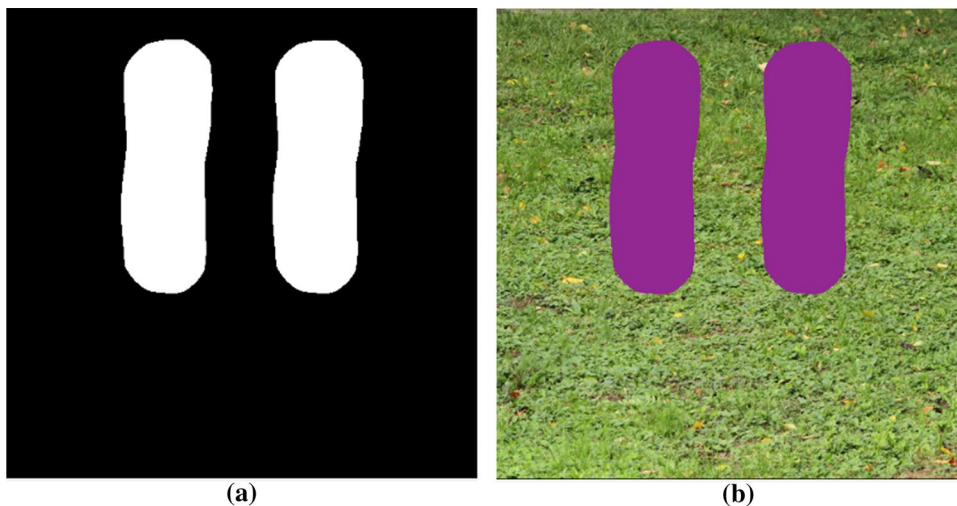


Fig. 8 False match removal using RANSAC from a cluster-based image

in the image; if any white area is present in the image, this concludes that the image is forged.

This morphological result as a binary mask is shown in Fig. 9a. The final localization of the forged region in the image using the binary mask from the previous step is in Fig. 9b. This step produces the final image with localization if any forgery is detected from the previous step.

Fig. 9 a Binary mask and b localization of forged region in the original image



4 Experimental Results, Performance Evaluation Criteria, and Discussions

The experimental results of the proposed technique are carried out on three state-of-the-art datasets, namely CoMoFoD [10], MICC-F220, and MICC-F2000 [44]. The CoMoFoD dataset is a collection of 200 tampered images, each of size 512×512 . MICC-F220 and MICC-F2000 datasets consist of 220 and 2000 tampered images, respectively.

4.1 Performance Evaluation Criteria

The performance of the proposed technique is evaluated in terms of precision (P), recall (R), and F-measure. The performance evaluation criteria are based on the total number of true positive (T_p —correctly detected forged region), false positive (F_p —an authentic region that is mistakenly detected as a forged region) and false negative (F_N —the forged regions that are mistakenly missed). Two most commonly used criteria for CMFD are precision P and recall R , which are mathematically expressed in Eq. (12) and Eq. (13), respectively.

$$P = \frac{T_p}{T_p + F_p} \quad (12)$$

$$R = \frac{T_p}{T_p + F_N} \quad (13)$$

Using P and R , dice similarity coefficient (DSC) aka F_{measure} the score is calculated, which is mathematically defined by Eq. (14).

$$F_{\text{measure}} = 2 * \left(\frac{P * R}{P + R} \right) \quad (14)$$

The following are the tests to establish the expediency of the proposed CMFD technique.

4.2 Accuracy and Effectiveness

Three separate tests for consistent, inconsistent, and multiple forged regions are performed to evaluate the accuracy and effectiveness of the proposed CMFD technique. For these experiments, the images are selected from the CoMoFoD dataset. In Figs. 10a, 11a, and 12a, the authentic images are shown with no forged region in the images.

Using CMF, the image is forged as shown in Figs. 10b, 11b, and 12b with consistent, inconsistent, and multiple forged regions, respectively. The proposed CMFD technique can detect the forgery even in the presence of the inconsistent and multiple forged regions as shown in Figs. 10c, 11c, and 12c. The precision, recall, and F-measure in the case of Fig. 11c are $P = 0.9855$, $R = 0.9185$, and $F_{\text{measure}} = 0.9508$. In Fig. 12c, $P = 0.8394$, $R = 0.9213$, and $F_{\text{measure}} = 0.8784$. For the multiple forged image using CMF in Fig. 12c, the image with multiple forged rocks, the $P = 0.9268$, $R = 0.9402$, and $F_{\text{measure}} = 0.9335$, the image with multiple forged windows, the $P = 0.9061$, $R = 0.9645$, and $F_{\text{measure}} = 0.9344$, the image with multiple forged tree leaves, the $P = 0.9256$, $R = 0.8977$, and $F_{\text{measure}} = 0.9115$, and the image with multiple forged car,

the $P = 0.9080$, $R = 0.8684$, and $F_{\text{measure}} = 0.9335$. The binary mask for comparison is shown in Figs. 10d, 11d, and 12d.

4.3 Robustness

To mitigate the accuracy of CMFD techniques, the culprits apply the post-processing attacks on forged regions. In the robustness test, the most commonly used post-processing attacks are tested to estimate the robustness of the proposed technique. These post-processing attacks are rotational invariance, scale invariance, blurring, color reduction, contrast adjustment, JPEG compression, additive noise, and brightness change (Fig. 13).

The proposed CMFD technique performs outstandingly against various attacks as presented in Table 1 and Fig. 14, respectively. The following sub-sections discussed the experimental results of the proposed CMFD technique on each post-processing attack after CMF in the images of the CoMoFoD dataset.

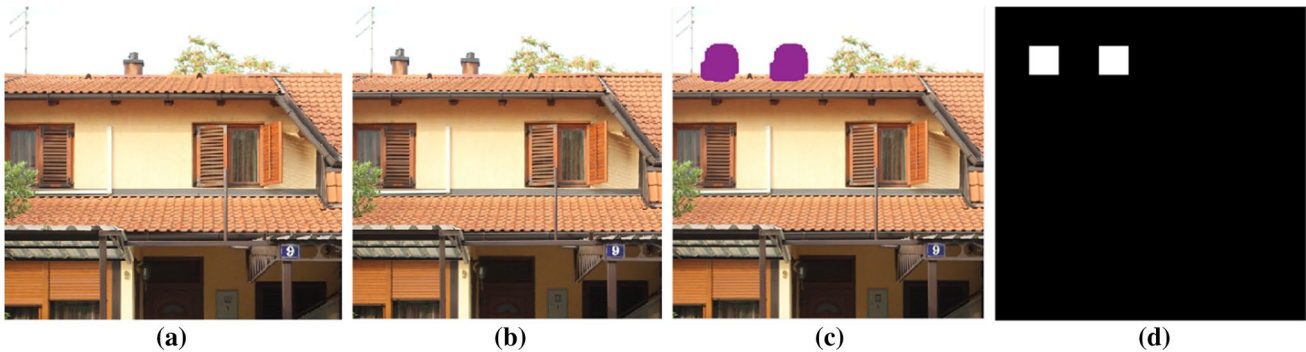


Fig. 10 **a** Without forgery image, **b** forgery with consistent shape, **c** localization of forged image, and **d** binary mask from the dataset for comparison

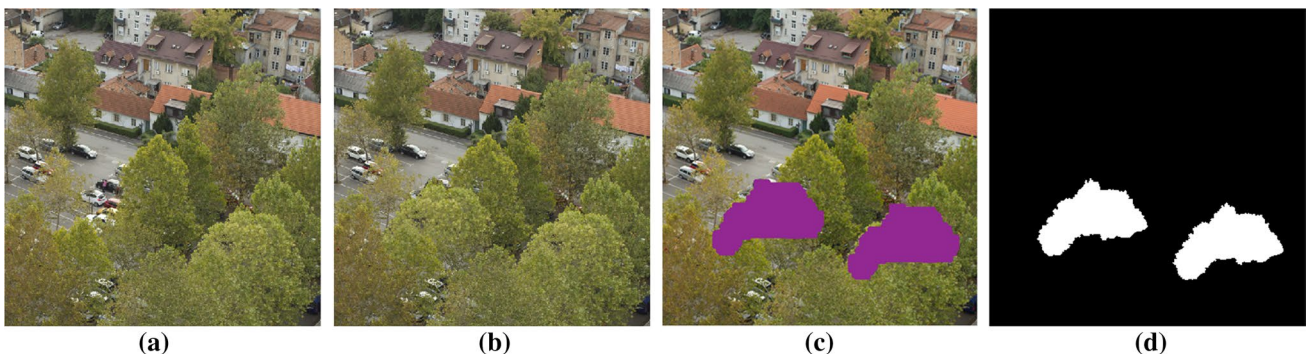


Fig. 11 **a** Without forgery image, **b** forgery with inconsistent shape, **c** localization of forged image, and **d** binary mask from the dataset for comparison

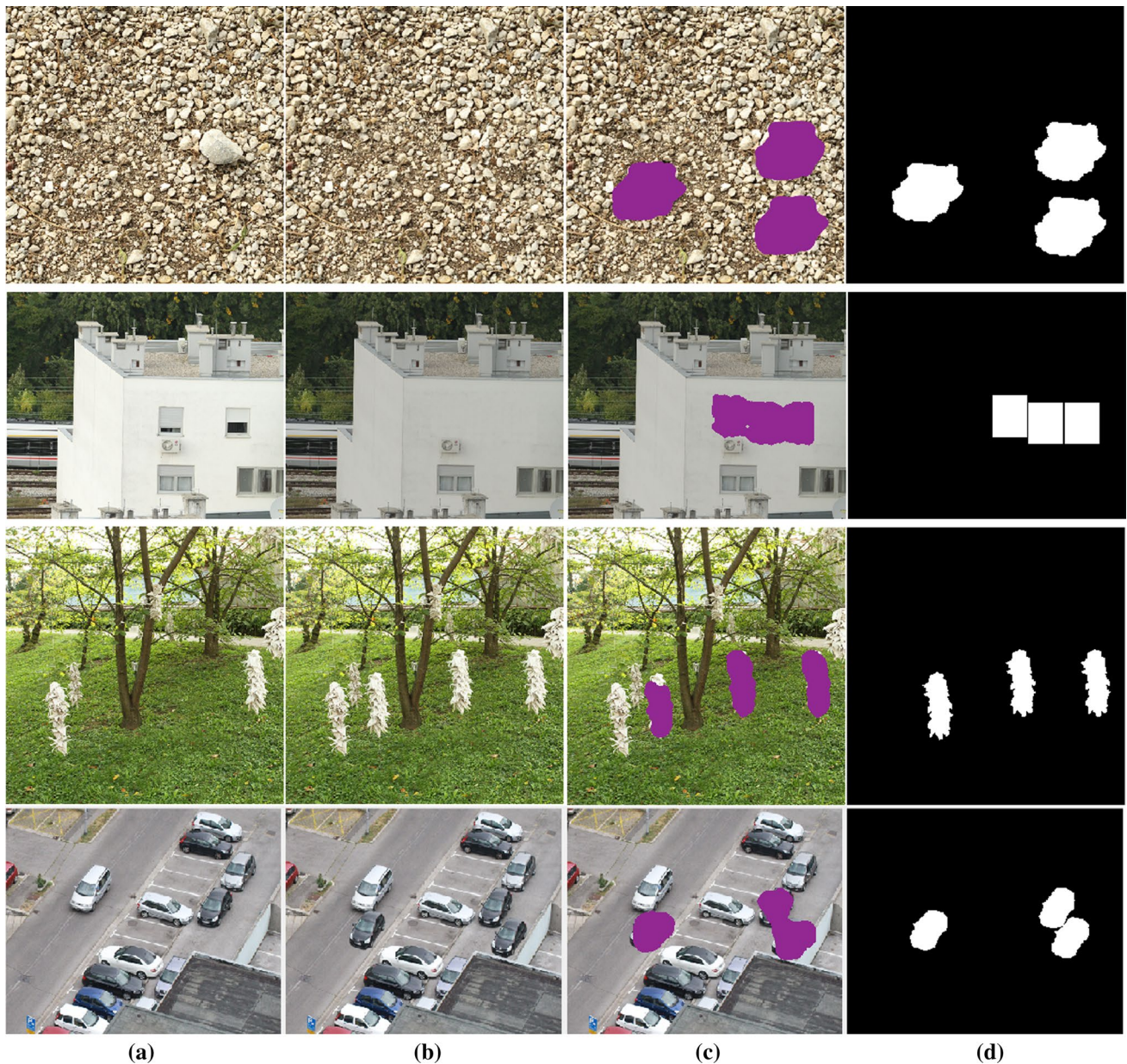


Fig. 12 **a** Without forgery image, **b** multiple copy-move forgeries, **c** localization of forged image, and **d** binary mask from the dataset for comparison

a) Rotational invariance

The forged region of the image in rotational invariant conducted on three different images, the images with rotational invariant of 60-degrees, 90-degrees, and 180-degrees, respectively, as shown in Fig. 13b, and original image without tampering are shown in Fig. 13a. The detected forged region is shown in Fig. 13c, which is compared with a binary mask of the CoMoFoD dataset is shown in Fig. 13d for visual reference.

(b) Scale invariance

The original image from the CoMoFoD dataset, as shown in Fig. 15a, is forged by a scale-invariant attack by reducing the size of the forged region to 15% as shown in Fig. 15b. The detected forged region using proposed CMFD technique and binary mask for comparison is shown in Fig. 15c and d, respectively.

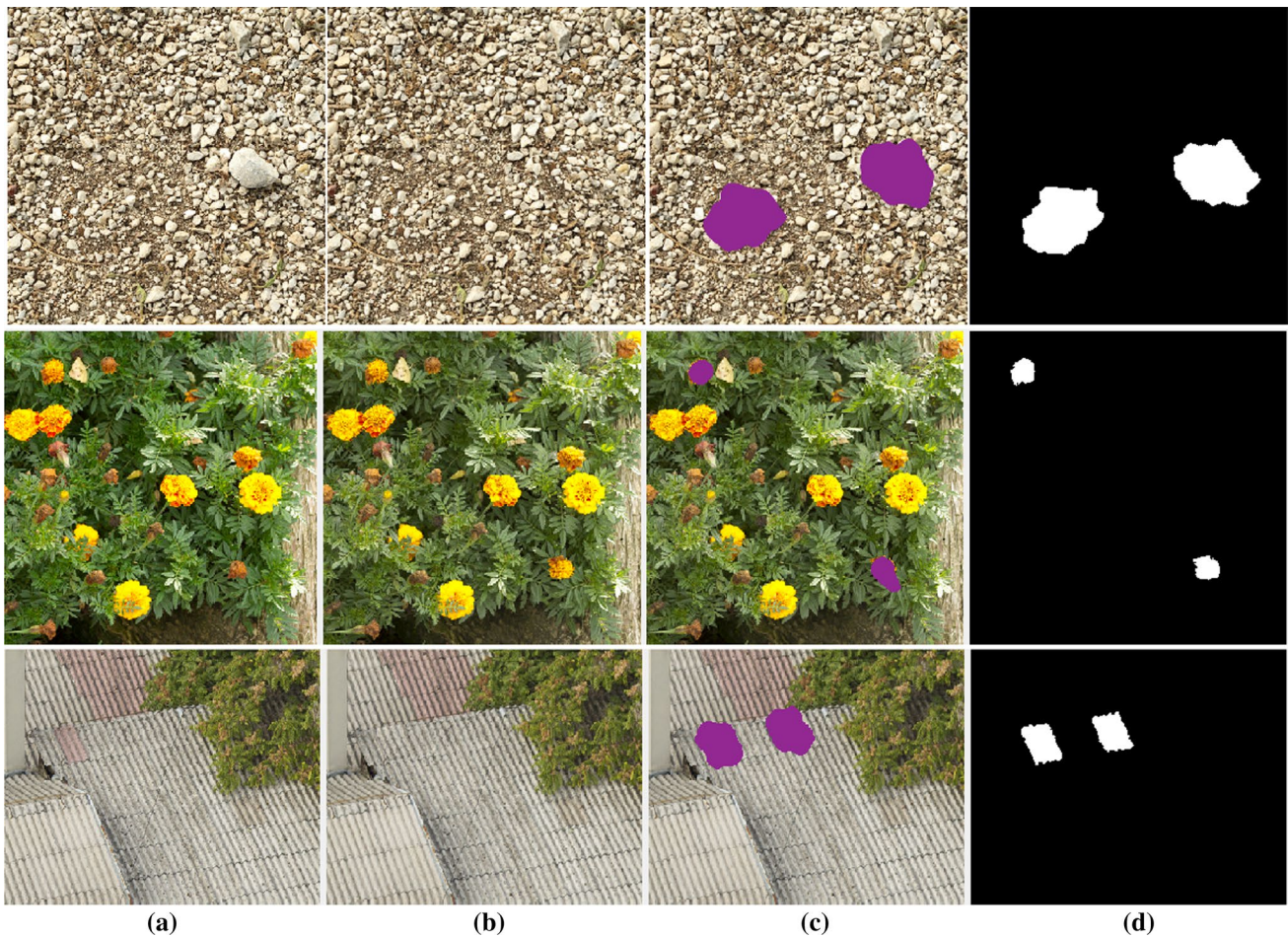


Fig. 13 **a** Without forgery image, **b** forgery with rotational invariance of 60-degree, 90-degree, and 180-degree, respectively, **c** localization of forged image and **d** binary mask from the dataset for comparison

Table 1 Performance analysis of the proposed CMFD technique in terms of *P* and *R* for different post-processing attacks

| Post-processing type | | Precision | Recall |
|----------------------------|-------------|-----------|--------|
| Rotational invariance (RI) | 60° | 0.9824 | 0.8917 |
| | 90° | 0.9130 | 0.8720 |
| | 180° | 0.9980 | 0.6954 |
| Scale invariance (SI) | | 0.8980 | 0.9935 |
| Blurring (B) | | 0.9362 | 0.8747 |
| Color reduction (CR) | | 0.9796 | 0.8784 |
| Contrast adjustment (CA) | | 0.8745 | 0.9754 |
| JPEG compression (JPEG-C) | | 0.8213 | 0.9332 |
| Additive noise (AN) | PSNR = 33.1 | 0.9333 | 0.9552 |
| | PSNR = 23.2 | 0.8839 | 0.9128 |
| | PSNR = 20.6 | 0.9382 | 0.8118 |
| Brightness change (BC) | | 0.9841 | 0.9447 |

c) Blurring

The CoMoFoD dataset consists of tampered images that are blurred by applying an averaging filter of mask size 3 × 3, 5 × 5, and 7 × 7. For blurring test, the proposed technique uses an averaging filter with a mask size of 7 × 7 as shown in Fig. 16.

d) Color reduction

For the color reduction test, the colors of the forged image are reduced by calculating the uniform quantization of intensity values of the original image. The colors of the forged image are reduced to 128 intensity levels for each color channel of the RGB image, as shown in Fig. 17.

e) Contrast adjustment

For contrast adjustment test, the intensity range of a sample forged image of the CoMoFoD dataset is mapped

Fig. 14 Performance analysis of the proposed CMFD technique in terms of $F_{measure}$ for post-processing attacks

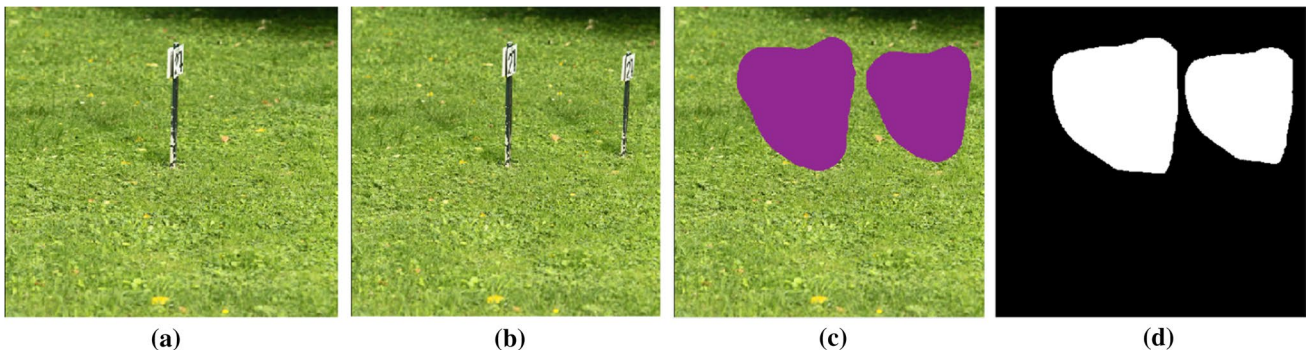
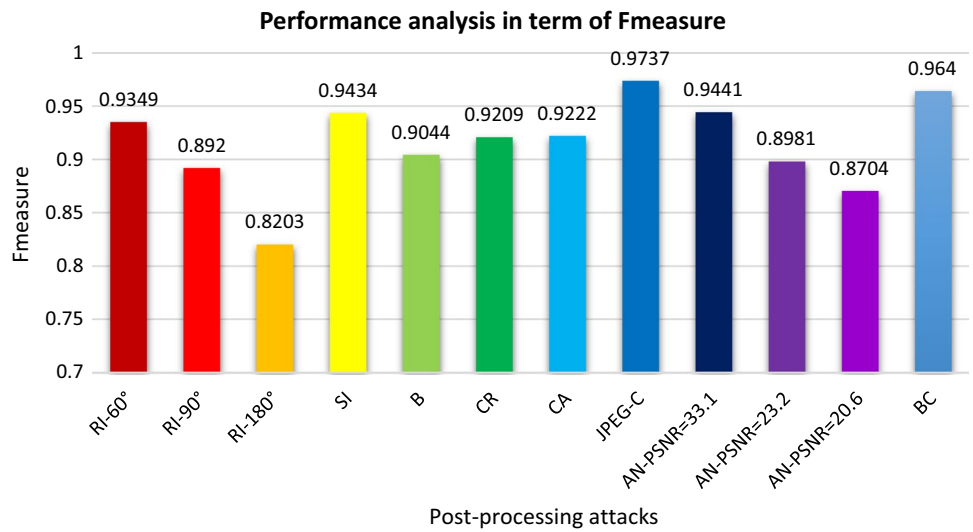


Fig. 15 **a** Without forgery image, **b** forgery with scale invariance, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison

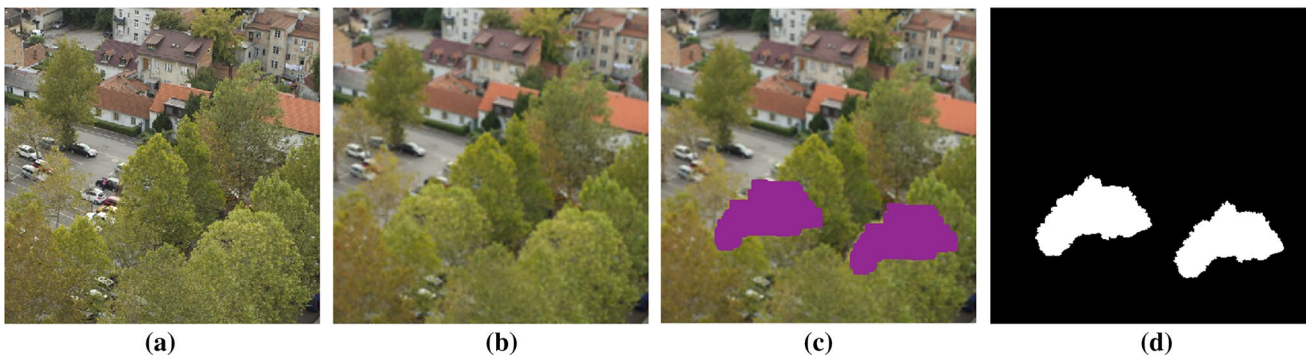


Fig. 16 **a** Without forgery image, **b** forgery with blurring, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison from CoMoFoD dataset [10]

to one of the three new lower and upper intervals bound i.e., (0.01, 0.95), (0.01, 0.9), and (0.01, 0.8). In the proposed CMFD technique, new lower and upper interval bound, i.e., (0.01, 0.8), are used, which generate a darker forged image as shown in Fig. 18.

f) JPEG compression

The JPEG compression of a sample forged image in the CoMoFoD dataset is achieved by varying the JPEG quality factor. In this test, the original image from the CoMoFoD

dataset is compressed by the JPEG quality factor of 50, which reduces image quality and produces blocks-type effects on a forged image as shown in Fig. 19.

g) Additive noise

For additive noise test, the CoMoFoD dataset uses white Gaussian noise with three different values of variance,

i.e., 0.009, 0.005, and 0.0005, with peak signal to noise ratio (PSNR) 20.6, 23.2 and 33.1, respectively. The mean is set to zero for all variations. The performance of the proposed CMFD technique is evaluated on the PSNR values as mentioned earlier and experimental results are shown in Fig. 20.

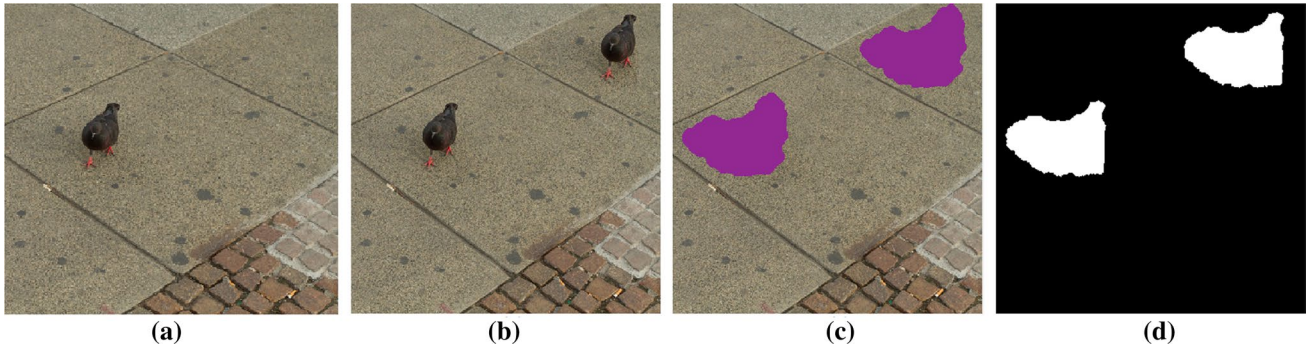


Fig. 17 **a** Without forgery image, **b** forgery with color reduction, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison

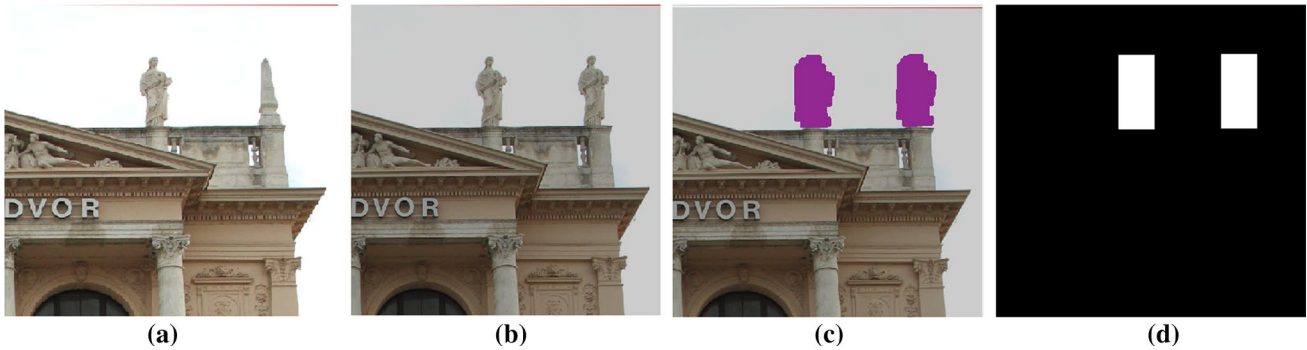


Fig. 18 **a** Without forgery image, **b** forgery with contrast adjustment, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison

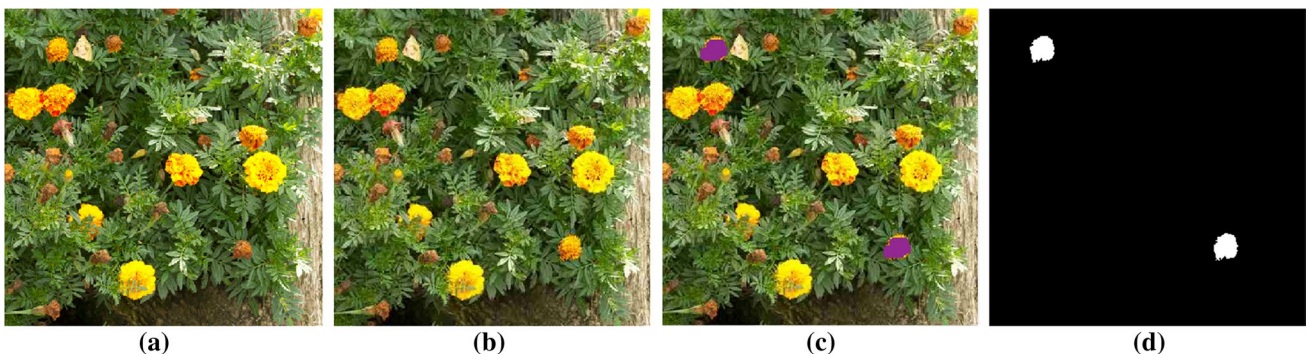


Fig. 19 **a** Without forgery image, **b** forgery with JPEG compression, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison

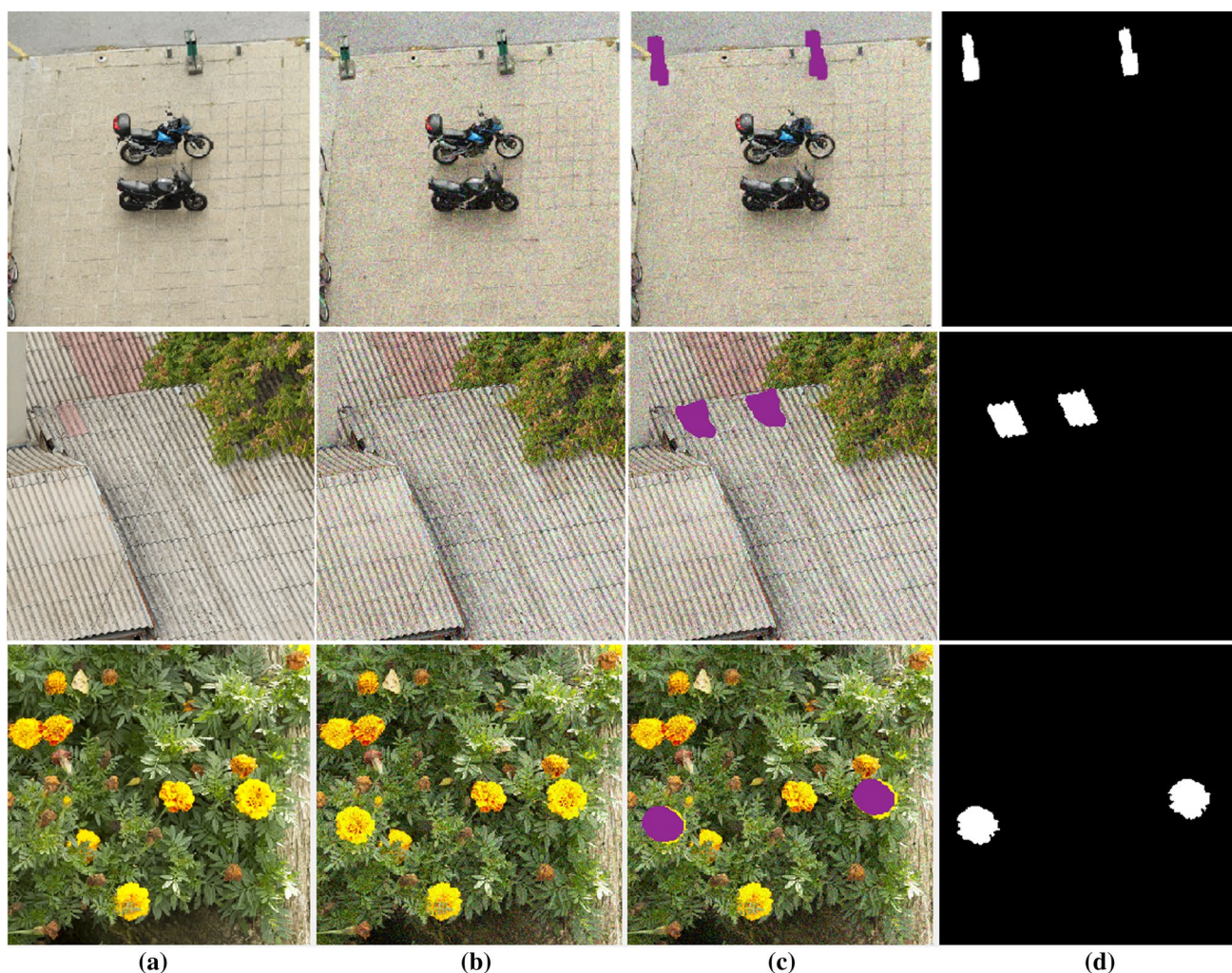


Fig. 20 **a** Without forgery image, **b** forgery with additive noise with PSNR at 33.1, 23.2, and 20.6, respectively, **c** localization of forged image and **d** binary mask from the CoMoFoD dataset for comparison

h) Brightness change

For the brightness change test, the CoMoFoD dataset uses the same approach as used for the contrast adjustment. The lower and upper bound of forged image intensity range is mapped to one of the three new lower and upper intervals bound (0.01, 0.95), (0.01, 0.9) and (0.01, 0.8). For this test, the (0.01, 0.8) range is used for brightness change as shown in Fig. 21, which produces a visually brighter forged image.

4.4 Comparison Test

The proposed technique is tested on MICC-F220, MICC-F2000, and CoMoFoD datasets. The results from above-mentioned datasets compared with the following state-of-the-art CMFD techniques. Manu et al. (cluster keypoint-based technique) [31], Amerini et al. (SIFT-based technique) [44], Cozzolino et al. (FMT, ZM-Polar,

ZM-Cart, PCT-Polar and PCT-Cart) [45], the SURF-based technique for CMFD proposed by Thampi et al. [46], Chen et al. (SIFT-based technique) [47], Abdel-Basset et al. (2-level clustering technique for CMFD) [48] and Soni et al. (hybrid feature-based technique for CMFD) [49].

The experimental details presented in Table 2 and Fig. 22 show that the proposed CMFD technique outperforms the state-of-the-art CMFD techniques in terms of precision (P), recall (R), and F_{measure} . The proposed CMFD technique outperforms state-of-the-art CMFD techniques because it uses a complementary features-based vector that contains robust features of SURF and BRISK descriptors. Furthermore, the proposed CMFD technique uses DBSCAN-based clustering technique as compared to the k-mean clustering technique, which does not require prior information about the total numbers of clusters in the forged image, which help in detecting single and multiple forged regions. Lastly, the proposed CMFD technique uses

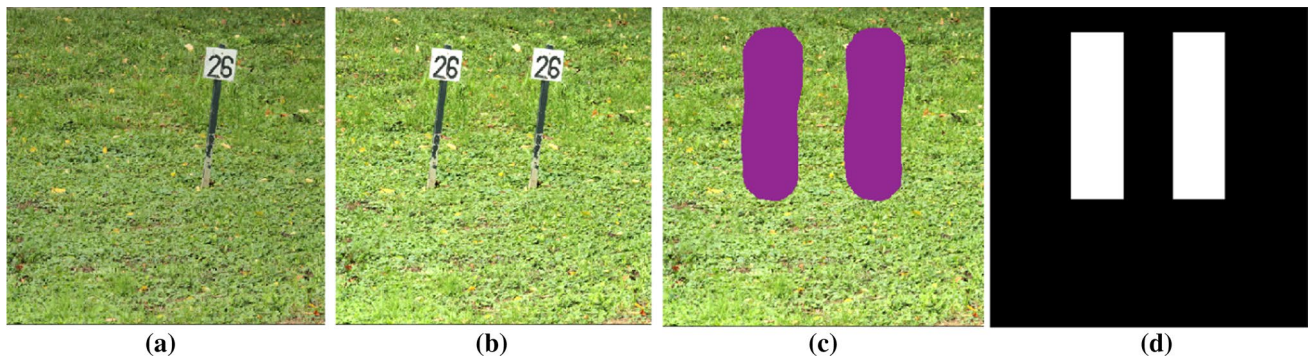


Fig. 21 **a** Without forgery image, **b** forgery with brightness change, **c** localization of forged image, and **d** binary mask from the CoMoFoD dataset for comparison

Table 2 Performance comparison of the proposed CMFD technique with state-of-the-art CMFD techniques on the MICC-F220, MICC-2000, and CoMoFoD datasets (bold values indicate best performances)

| Dataset | Technique name | <i>P</i> | <i>R</i> |
|---------------------|--------------------------|------------------|---------------|
| MICC-F220 | Manu et al. [31] | 0.9050 | 0.9550 |
| | FMT [45] | 1.0000 | 0.5940 |
| | ZM-Polar [45] | 1.0000 | 0.4910 |
| | ZM-Cart [45] | 0.9820 | 0.4910 |
| | PCT-Polar [45] | 0.9650 | 0.5000 |
| | PCT-Cart [45] | 0.9630 | 0.4730 |
| | SURF [46] | 0.8160 | 0.9273 |
| | Abdel-Basset et al. [48] | – | – |
| | Soni et al. [49] | – | – |
| | Proposed technique | 0.9564 | 0.9630 |
| MICC-F2000 | Manu et al. [31] | 0.7260 | 0.9560 |
| | FMT [45] | 0.7920 | 0.7000 |
| | ZM-Polar [45] | 0.8250 | 0.5870 |
| | ZM-Cart [45] | 0.8070 | 0.5800 |
| | PCT-Polar [45] | 0.8550 | 0.6000 |
| | PCT-Cart [45] | 0.8190 | 0.5740 |
| | SURF [46] | 0.6780 | 0.9460 |
| | Abdel-Basset et al. [48] | – | – |
| | Proposed technique | 0.9990 | 0.8935 |
| | CoMoFoD | Manu et al. [31] | 0.7980 |
| Amerini et al. [44] | | 0.7000 | 0.8750 |
| FMT [45] | | 0.8290 | 0.5220 |
| ZM-Polar [45] | | 0.8700 | 0.4890 |
| ZM-Cart [45] | | 0.8480 | 0.5090 |
| PCT-Polar [45] | | 0.8770 | 0.4910 |
| PCT-Cart [45] | | 0.8480 | 0.4940 |
| SURF [46] | | 0.6160 | 0.7098 |
| Chen et al. [47] | | 0.7019 | 0.8461 |
| Proposed technique | | 0.9598 | 0.9124 |

RANSAC technique for robust estimation of true and false matches in the forged image.

4.5 Time Efficiency

To analyze the performance analysis in terms of the computational cost of the proposed CMFD technique, the images from MICC-F220, MICC-F2000, and CoMoFoD datasets are used. The 100 images are taken from the MICC-F220 dataset and computational cost (time in seconds) is compared with following state-of-the-art CMFD techniques; Fridrich et al. [24], Yang et al. [35], Yang et al. [50], Popescu et al. [51], and Soni et al. [52] as shown in Table 3. The reason for selecting 100 images from MICC-F220 is that the state-of-the-art CMFD technique also uses 100 images of the MICC-F220 dataset to report the computational cost. The whole images from dataset MICC-F2000 are used to evaluate the time performance of proposed CMFD technique and compared with Li J. et al. [53], Yang et al. [50], Zhong et al. [54], Amerini et al. [44], Amerini et al. [55], and Soni et al. [56], as presented in Table 4. The whole images are used to conduct a time evaluation experiment from CoMoFoD dataset and compared with Amerini et al. [44], and Muzaffer et al. [57], as shown in Table 5. The hardware and software resources (i.e., Intel(R) Core(TM) i7-4600U CPU @ 2.10 GHz, 8 GB RAM, HDD 500 GB, MATLAB 2017b, and Windows 10 64-bit OS) are same for all the above experiments. The performance of the proposed CMFD technique is better than state-of-the-art CMFD techniques in terms of true-positive rate (TPR), false-positive rate (FPR), and time efficiency (CPU time in seconds) as detailed mentioned in Tables 3, 4, and 5. The robust TPR performance and low computational cost of the proposed CMFD technique are achieved: by the refinement of forged image by applying DWT and extracting only energy-rich features, by using the fast feature extraction techniques of SURF and BRISK as compared to SIFT descriptor, and plummeting the search space using DBSCAN clustering.

Fig. 22 Performance comparison of proposed CMFD technique with state-of-the-art techniques in terms of $F_{measure}$

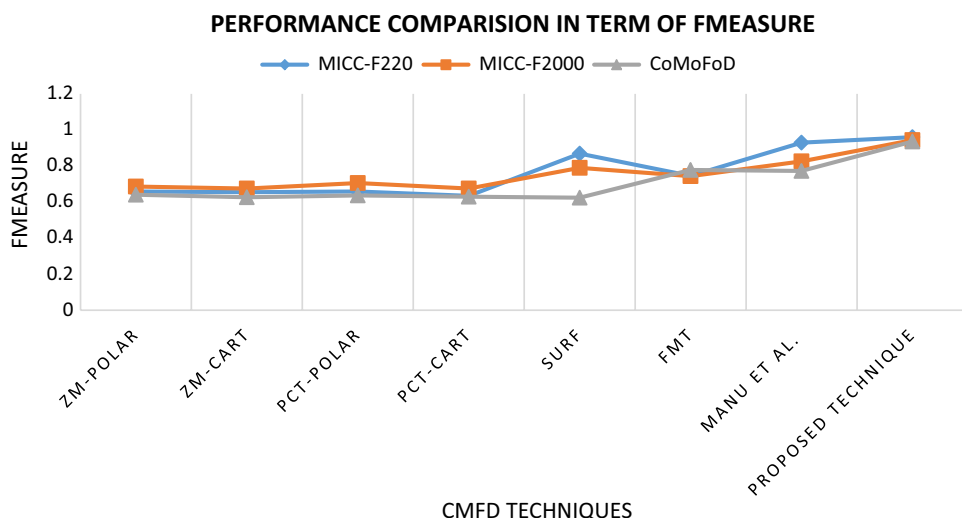


Table 3 Performance comparison of the proposed CMFD technique on the MICC-F220 dataset with state-of-the-art CMFD techniques in terms of FPR, TPR, and CPU time (time in seconds)

| Techniques | False-positive rate (%) | True-positive rate (%) | CPU time (S) |
|----------------------|-------------------------|------------------------|--------------|
| Fridrich et al. [24] | 84.00 | 89.00 | 294.69 |
| Yang et al. [35] | 10.42 | 95.45 | 12.40 |
| Yang et al. [50] | 9.02 | 95.88 | 10.20 |
| Popescu et al. [51] | 86.00 | 87.00 | 70.97 |
| Soni et al. [52] | 8.60 | 97.40 | 9.20 |
| Proposed technique | 7.31 | 98.05 | 8.35 |

Bold values indicate the best performances

Table 4 Performance comparison of the proposed CMFD technique on the MICC-F2000 dataset with state-of-the-art CMFD techniques in terms of FPR, TPR, and CPU time (time in seconds)

| Techniques | False-positive rate (%) | True-positive rate (%) | CPU time (S) |
|------------------------|-------------------------|------------------------|--------------|
| Li J. et al. [53] | 11.80 | 91.55 | 24.45 |
| Yang et al. [50] | 12.02 | 92.78 | 25.20 |
| Zhong et al. [54] | 14.82 | 93.75 | 22.40 |
| Amerini I. et al. [44] | 11.61 | 93.42 | 20.94 |
| Amerini et al. [55] | 9.15 | 94.86 | 19.20 |
| Soni et al. [56] | 6.80 | 98.50 | 18.60 |
| Proposed technique | 5.22 | 98.84 | 12.72 |

Bold values indicate the best performances

5 Conclusions

The proposed CMFD technique uses level-2 DWT to select energy-rich features from the forged image. The features from SURF and BRISK descriptors are fused together to get the complementary effect for CMF detection in the

Table 5 Performance comparison of the proposed CMFD technique with state-of-the-art CMFD techniques in terms of FPR, TPR, and CPU time (time in seconds) on the CoMoFoD dataset

| Techniques | False-positive rate (%) | True-positive rate (%) | CPU time (S) |
|----------------------|-------------------------|------------------------|--------------|
| Amerini [44] et al. | 92.00 | 94.00 | 1340.38 |
| Muzaffer [57] et al. | 89.00 | 91.00 | 146.7 |
| Proposed technique | 9.82 | 96.68 | 58.9 |

Bold values indicate the best performances

proposed CMFD technique to aid in the detection of the single and multiple forged regions in the image. The fused feature set also assists robust CMF detection in the presence of post-processing attacks like scale invariance, rotation invariance, blurring, color reduction, contrast adjustment, JPEG compression, additive noise, and brightness change. The DBSCAN clustering and RANSAC are used to reduce search space, mitigate false matches, and reduce the computational cost of the proposed technique. The proposed technique provides an accurate and robust result for single and multiple forged regions even in the presence of post-processing attacks with less computational cost compared to state-of-the-art techniques. The experiment results show that the proposed CMFD technique outperforms the state-of-the-art CMFD techniques in term of precision, recall, and $F_{measure}$. Therefore, the proposed technique can perform a vigorous part in the forensic application. Nevertheless, image forgery uses more complicated post-processing attacks, e.g., excessive scaling, smoothening, and brightness change in the forged regions. Therefore, we are in the process of refining the proposed technique that handles these concerns more efficiently.

Authors' Contributions MB, HAH, ZM, TS, MR have authors contributed equally to this work.

Availability of Data and Material Please contact the authors for data requests.

Compliance with Ethical Standards

Conflict of interest All the authors declare no conflict of interest.

References

- Kessler, G.C.: An overview of steganography for the computer forensics examiner. *Forensic Sci. Commun.* **6**(3), 1–27 (2004)
- Nilizadeh, A.; Nilchi, A.R.N.: A novel steganography method based on matrix pattern and LSB algorithms in RGB images. In: 2016 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC), Bam, Iran 2016, pp. 154–159. IEEE (2016)
- Nilizadeh, A.; Mazurczyk, W.; Zou, C.; Leavens, G.T.: Information hiding in RGB images using an improved matrix pattern approach. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA 2017, pp. 1407–1415. IEEE (2017)
- Rehman, A.; Saba, T.; Mahmood, T.; Mehmood, Z.; Shah, M.; Anjum, A.: Data hiding technique in steganography for information security using number theory. *J. Inf. Sci.* (2018). <https://doi.org/10.1177/0165551518816303>
- Cox, I.J.; Miller, M.L.; Bloom, J.A.; Honsinger, C.: *Digital Watermarking*, vol. 53. Springer, Berlin (2002)
- Nikolaidis, N.; Pitas, I.: Digital image watermarking: an overview. In: *Proceedings IEEE International Conference on Multimedia Computing and Systems*, Florence, Italy 1999, pp. 1–6. IEEE (1999)
- Belk, R.W.: Extended self in a digital world. *J. Consum. Res.* **40**(3), 477–500 (2013). <https://doi.org/10.1086/671052>
- Qureshi, M.A.: A bibliography of pixel-based blind image forgery detection techniques. *Sig. Process. Image Commun.* **39**, 46–74 (2015)
- Asghar, K.; Habib, Z.; Hussain, M.: Copy-move and splicing image forgery detection and localization. *Aust. J. Forensic Sci.* **49**, 281–307 (2017)
- Tralic, D.; Zupancic, I.; Grgic, S.; Grgic, M.: CoMoFoD—new database for copy-move forgery detection. In: *ELMAR, 2013 55th international symposium*, Zadar, Croatia 2013, pp. 49–54. IEEE (2013)
- Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. *Inf. Forensics Secur. IEEE Trans.* **7**, 1841–1854 (2012)
- Muhammad, G.; Al-Hammadi, M.H.; Hussain, M.; Bebis, G.: Image forgery detection using steerable pyramid transform and local binary pattern. *Mach. Vis. Appl.* **25**, 985–995 (2014)
- Hayat, K.; Qazia, T.: Forgery detection in digital images via discrete wavelet and discrete cosine transforms. *Comput. Electr. Eng.* **62**, 448–458 (2017)
- Bay, H.; Ess, A.; Tuytelaars, T.; Gool, L.: Speeded-up robust features (SURF). *Comput. Vis. Image Underst.* **110**(3), 346–359 (2008)
- Bo, X.; Junwen, W.; Guangjie, L.; Yuewei, D.: Image copy-move forgery detection based on SURF. In: 2010 International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, China 2010, pp. 889–892. IEEE (2010)
- Pandey, R.C.; Singh, S.K.; Shukla, K.; Agrawal, R.: Fast and robust passive copy-move forgery detection using SURF and SIFT image features. In: 2014 9th International conference on industrial and information systems (ICIIS), Gwalior, India 2014, pp. 1–6. IEEE (2014)
- Leutenegger, S.; Chli, M.; Siegwart, R.Y.: BRISK: Binary robust invariant scalable keypoints. In: *IEEE International Conference on Computer Vision (ICCV)*, 2011, pp. 2548–2555. IEEE (2011)
- 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**(5), 16–32 (2015). <https://doi.org/10.1016/j.jvcir.2015.01.016>
- Mahmood, T.; Mehmood, Z.; Shah, M.; Khan, Z.: An efficient forensic technique for exposing region duplication forgery in digital images. *Appl. Intell.* **48**(7), 1791–1801 (2018). <https://doi.org/10.1007/s10489-017-1038-5>
- Mahmood, T.; Mehmood, Z.; Shah, M.; Saba, T.: A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. *J. Vis. Commun. Image Represent.* **53**(5), 202–214 (2018). <https://doi.org/10.1016/j.jvcir.2018.03.015>
- Mahmood, T.; Irtaza, A.; Mehmood, Z.; Mahmood, M.T.: Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images. *Forensic Sci. Int.* **279**(10), 8–21 (2017). <https://doi.org/10.1016/j.forsciint.2017.07.037>
- Mahmood, T.; Nawaz, T.; Mehmood, Z.; Khan, Z.; Shah, M.; Ashraf, R.: Forensic analysis of copy-move forgery in digital images using the stationary wavelets. In: 2016 6th International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland 2016, pp. 578–583. IEEE (2016)
- Mahmood, T.; Nawaz, T.; Ashraf, R.; Shah, M.; Khan, Z.; Irtaza, A.; Mehmood, Z.: A survey on block based copy move image forgery detection techniques. In: 2015 International Conference on Emerging Technologies (ICET), Peshawar, Pakistan 2015, pp. 1–6. IEEE (2015)
- Fridrich, A.J.; Soukal, B.D.; Lukáš, A.J.: Detection of copy-move forgery in digital images. In: *in Proceedings of Digital Forensic Research Workshop 2003*. Citeseer (2003)
- Lin, H.-J.; Wang, C.-W.; Kao, Y.-T.: Fast copy-move forgery detection. *WSEAS Trans. Signal Process.* **5**(5), 188–197 (2009)
- Ardizzone, E.; Bruno, A.; Mazzola, G.: Copy-move forgery detection by matching triangles of keypoints. *IEEE Trans. Inf. Forensics Secur.* **10**(10), 2084–2094 (2015). <https://doi.org/10.1109/TIFS.2015.2445742>
- Alkawaz, M.H.; Sulong, G.; Saba, T.; Rehman, A.: Detection of copy-move image forgery based on discrete cosine transform. *Neural Comput. Appl.* **30**(1), 183–192 (2018). <https://doi.org/10.1007/s00521-016-2663-3>
- Li, J.; Li, X.; Yang, B.; Sun, X.: Segmentation-based image copy-move forgery detection scheme. *IEEE Trans. Inf. Forensics Secur.* **10**(3), 507–518 (2014). <https://doi.org/10.1109/TIFS.2014.2381872>
- Warbhe, A.D.; Dharaskar, R.; Thakare, V.: A survey on keypoint based copy-paste forgery detection techniques. *Procedia Comput. Sci.* **78**, 61–67 (2016). <https://doi.org/10.1016/j.procs.2016.02.011>
- Farid, H.: Image forgery detection. *IEEE Signal Process. Magazine* **26**(2), 16–25 (2009). <https://doi.org/10.1109/MSP.2008.931079>
- Manu, V.; Mehtre, B.M.: Copy-move tampering detection using affine transformation property preservation on clustered keypoints. *Signal Image Video Process.* **12**(3), 549–556 (2018). <https://doi.org/10.1007/s11760-017-1191-7>



32. Bi, X.; Pun, C.-M.; Yuan, X.-C.: Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. *Inf. Sci.* **345**, 226–242 (2016). <https://doi.org/10.1016/j.ins.2016.01.061>
33. Yuan, Y.; Zhang, Y.; Chen, S.; Wang, H.: Robust region duplication detection on log-polar domain using band limitation. *Arab. J. Sci. Eng.* **42**(2), 559–565 (2017). <https://doi.org/10.1007/s13369-016-2268-2>
34. Zandi, M.; Mahmoudi-Aznavah, A.; Talebpour, A.: Iterative copy-move forgery detection based on a new interest point detector. *IEEE Trans. Inf. Forensics Secur.* **11**(11), 2499–2512 (2016). <https://doi.org/10.1109/TIFS.2016.2585118>
35. Yang, F.; Li, J.; Lu, W.; Weng, J.: Copy-move forgery detection based on hybrid features. *Eng. Appl. Artif. Intell.* **59**(3), 73–83 (2017). <https://doi.org/10.1016/j.engappai.2016.12.022>
36. Pandey, R.C.; Agrawal, R.; Singh, S.K.; Shukla, K.K.: 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 (FICTA) 2014 2015*, pp. 659–666. Springer (2015)
37. Yu, L.; Han, Q.; Niu, X.: Feature point-based copy-move forgery detection: covering the non-textured areas. *Multimed. Tools Appl.* **75**(2), 1159–1176 (2016). <https://doi.org/10.1007/s11042-014-2362-y>
38. Bin, Y.; Xingming, S.; Xianyi, C.; Zhang, J.; Xu, L.: An efficient forensic method for copy-move forgery detection based on DWT-FWHT. *Radioengineering* **22**(4), 1098–1105 (2013)
39. Mikolajczyk, K.; Schmid, C.: A performance evaluation of local descriptors. *IEEE Trans. Pattern Anal. Mach. Intell.* **27**(10), 1615–1630 (2005). <https://doi.org/10.1109/TPAMI.2005.188>
40. Juan, L.; Gwun, O.: A comparison of sift, pca-sift and surf. *Int. J. Image Process.* (IJIP) **3**(4), 143–152 (2009)
41. Fahim, A.; Saake, G.; Salem, A.; Torkey, F.; Ramadan, M.: Improved DBSCAN for spatial databases with noise and different densities. *Comput. Sci. Telecommun.* **3**, 53–60 (2009)
42. Ester, M.; Kriegel, H.-P.; Sander, J.; Xu, X.: A density-based algorithm for discovering clusters in large spatial databases with noise. In: *Kdd 1996*, vol. 34, pp. 226–231 (1996)
43. Fischler, M.A.; Bolles, R.C.: Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Commun. ACM* **24**(6), 381–395 (1981). <https://doi.org/10.1145/358669.358692>
44. Amerini, I.; Ballan, L.; Caldelli, R.; Del Bimbo, A.; Serra, G.: A sift-based forensic method for copy-move attack detection and transformation recovery. *IEEE Trans. Inf. Forensics Secur.* **6**(3), 1099–1110 (2011). <https://doi.org/10.1109/TIFS.2011.2129512>
45. Cozzolino, D.; Poggi, G.; Verdoliva, L.: Efficient dense-field copy-move forgery detection. *IEEE Trans. Inf. Forensics Secur.* **10**(11), 2284–2297 (2015). <https://doi.org/10.1109/TIFS.2015.2455334>
46. Thampi, S.M.; Gelbukh, A.; Mukhopadhyay, J.: *Advances in Signal Processing and Intelligent Recognition Systems*. Springer, Berlin (2014)
47. Chen, C.-C.; Lu, W.-Y.; Chou, C.-H.: Rotational copy-move forgery detection using SIFT and region growing strategies. *Multimed. Tools Appl.* (2019). <https://doi.org/10.1007/s11042-019-7165-8>
48. Abdel-Basset, M.; Manogaran, G.; Fakhry, A.E.; El-Henawy, I.: 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. *Multimed. Tools Appl.* **1**, 1–19 (2018). <https://doi.org/10.1007/s11042-018-6266-0>
49. Soni, B.; Das, P.K.; Thounaojam, D.M.: Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. *J. Inf. Secur. Appl.* **45**, 44–51 (2019). <https://doi.org/10.1016/j.jisa.2019.01.007>
50. Yang, B.; Sun, X.; Guo, H.; Xia, Z.; Chen, X.: A copy-move forgery detection method based on CMFD-SIFT. *Multimed. Tools Appl.* **77**(1), 837–855 (2018). <https://doi.org/10.1007/s11042-016-4289-y>
51. Popescu, A.C.; Farid, H.: Exposing digital forgeries by detecting traces of resampling. *IEEE Trans. Signal Process.* **53**(2), 758–767 (2005). <https://doi.org/10.1109/TSP.2004.839932>
52. Soni, B.; Das, P.K.; Thounaojam, D.M.: Improved block-based technique using SURF and FAST keypoints matching for copy-move attack detection. In: *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India 2018, pp. 197–202. IEEE (2018)
53. Li, J.; Li, X.; Yang, B.; Sun, X.: Segmentation-based image copy-move forgery detection scheme. *IEEE Trans. Inf. Forensics Secur.* **10**(3), 507–518 (2015). <https://doi.org/10.1109/TIFS.2014.2381872>
54. Zhong, J.; Gan, Y.; Young, J.; Huang, L.; Lin, P.: A new block-based method for copy move forgery detection under image geometric transforms. *Multimed. Tools Appl.* **76**(13), 14887–14903 (2017). <https://doi.org/10.1007/s11042-016-4201-9>
55. 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. *Sig. Process. Image Commun.* **28**(6), 659–669 (2013). <https://doi.org/10.1016/j.image.2013.03.006>
56. Soni, B.; Das, P.K.; Thounaojam, D.M.: multiCMFD: fast and efficient system for multiple copy-move forgeries detection in image. In: *Proceedings of the 2018 International Conference on Image and Graphics Processing 2018*, pp. 53–58. ACM (2018)
57. Muzaffer, G.; Ulutas, G.: A fast and effective digital image copy move forgery detection with binarized SIFT. In: *2017 40th International Conference on Telecommunications and Signal Processing (TSP)*, Barcelona, Spain 2017, pp. 595–598. IEEE (2017)

