Hindawi
Journal of Sensors
Volume 2022, Article ID 6580508, 16 pages
https://doi.org/10.1155/2022/6580508

Research Article

Passive Framework of Sparse Region Duplication Detection from Digital Images

Zahid Mehmood,[1] **Hassan Nazeer Chaudhry**,[2] **Rizwan Ali Naqvi**,[3] **Farzana Kulsoom**,[4] **Asmaa Munshi**,[5] **and Muhammad Bilal**[6]

[1]*Department of Computer Engineering, University of Engineering and Technology, Taxila 47050, Pakistan*
[2]*Department of Electronics, Information and Bioengineering, Politecnico di Milano, Milano 20125, Italy*
[3]*Department of Unmanned Vehicle Engineering, Sejong University, Seoul 05006, Republic of Korea*
[4]*Department of Telecommunication Engineering, University of Engineering and Technology, Taxila 47050, Pakistan*
[5]*College of Computer Science and Engineering, University of Jeddah, Jeddah 21577, Saudi Arabia*
[6]*Department of Computer Science, Capital University of Science and Technology, Islamabad 44000, Pakistan*

Correspondence should be addressed to Zahid Mehmood; zahid.mehmood@uettaxila.edu.pk
and Rizwan Ali Naqvi; rizwanali@sejong.ac.kr

Received 13 January 2022; Revised 22 May 2022; Accepted 30 May 2022; Published 22 June 2022

Academic Editor: Bin Gao

Currently, digital images are widely communicated by media using social media applications. The general public captures the digital images for preserving the family and personal memories and to share with their friends and family. Digital images have been used extensively in forensic science to present the digital images as proof in the court and law enforcement agencies, which present a loophole for the culprits to forge the digital image and change the proofs and evidence. Copy-move forgery (CMF) is among the most widely employed image manipulation methods. In this method, the area of the image is duplicated to some other part to modify its content by applying different postprocessing operations on images like blurring, color reduction, and scaling which is a challenging research problem in copy-move forgery detection (CMFD). In this paper, an efficient and effective CMFD method is presented to identify the single and multiple altered areas in an image in the presence of postprocessing operations. The proposed CMFD method divides the image into circular blocks. It computes a rotation-invariant feature vector from each circular block of the image by applying local intensity order pattern (LIOP) features. The computed feature vectors are then compared using Euclidean distance to locate the suspected image's forged areas. The experimental results of the proposed CMFD method are reported on three standard datasets of the CMF, namely, CoMoFoD, KLTCI, and MICC-F220. The experimental analysis of the proposed CMFD method on these datasets indicates that it produces robust performance (detection accuracies of 97.29% on the CoMoFoD dataset, 98.53% on the KLTCI dataset, and 97.57% on the MICC-F220 dataset) as compared with state-of-the-art CMFD methods in terms of the standard performance evaluation parameters of the CMF.

1. Introduction

In the digital revolution age, digital samples are a common means of information. The availability of powerful imaging tools like Photoshop and Corel Draw has enabled modifying the image content much easier without compromising quality. On a negative note, it paved the way for forgeries. The abusive use of image tampering has brought major security challenges. Thus, it is of utmost importance to verify the authenticity of the images. Therefore, it is a challenging task to verify an image's originality accurately. Image validation is required in information sensitive departments like the military, media, court, medical appliances, banking, and news agencies. In CMF, a portion from the same image is taken and pasted to another location; significant characteristics, i.e., chrominance information, noise, light, and brightness variations, remain the same which makes the identification procedure a difficult task [1]. Different approaches like pixel, camera, format physical, and geometry-based are applied to identify image alteration. Because of the multidimensional behavior of image forgery problems, some methods can show better detection results. In contrast, others can no longer be useful, and it depends upon the forgery attack to which an image is subjected [1]. In [2], Zernike moments of circular blocks were utilized to analyze tempered images for locating copy-move regions. The Zernike moment-based features do not produce robust performance in the case of applying scaling operation on the blocks of the forged image during copy-move operation. There are also high computational costs associated with moment-based techniques. To reduce the dimensions of the feature vectors, principal component analysis (PCA) was applied to small-sized image blocks. However, it is not able to identify the transformations of rotation or scaling [3].

Keypoint-based approaches work to calculate features only for associated keypoints and improve computational efficiency as well as the effectiveness of CMF like keypoint-based methodologies, namely, scale-invariant feature transform (SIFT) and speeded-up robust features (SURF) [4]. These frameworks may not be successful in detecting flat duplicate regions. Figure 1 presents an example of CMF and splicing forgery attacks. A 9-dimensional vector was previously introduced to find the fixed angle rotation to detect image forgery [5]. However, this technique could not detect small copied regions in a forged image. Furthermore, a technique was proposed to detect the image features using a local binary pattern (LBP) [6], which exhibits robustness against blurring, flipping, and rotation. Still, its performance degraded while detecting the areas having general angles. A CMFD technique was proposed to identify duplicated regions using a special ordering of the wavelet coefficients from lower to higher frequency subbands. However, this technique was inefficient to defect forgery in compressed and noisy areas of an image [7]. Another technique was proposed to detect corresponding blocks' similarity in a forged image using kernel PCA. However, this technique does not consider some geometric operations like scaling and shearing. Moreover, a technique was proposed to detect signal resampling using the expectation/maximization (EM) algorithm, which was helpful in image forgery detection. However, this technique limits evidence with the uncompressed and high-resolution format [8].

As a consequence of incredible image handling instruments, the forgeries in digital images effectively become a genuine social issue. This is done with the intent of highlighting a certain object or hiding or removing an object from the image and by applying different postprocessing attacks like blurring, color reduction, scaling, and rotation on images. By and large, a counterfeiter uses some relative changes to roll out the improvements outwardly flawless. Most existing copy-move recognition strategies are not compelling when duplicated locales are under mathematical twists. Unlike block-based approaches, which extract features from every block, the keypoint-based approach takes descriptors from selected places on the image. As a result of the reduced number of descriptors, a faster CMF detection approach based on keypoints can be designed. SIFT, SURF, binary robust invariant scalable keypoints (BRISK), and other feature descriptor methods are among the options. When a tampering operation is performed on an image, the actual pattern of the image is destroyed because it loses/changes the main meaning of the information carried within an image. Two detection methods have been defined; the active method and the passive method for CMF. In the active method, previous knowledge, idea, or concept of images is required to insert the information/image into the original image. For example, digital signs and the image watermark are used to identify duplicated areas of the image. The passive method is the simple method, it does not require any previous or basic information. The tampered or copied areas do not leave any real-time signs but it becomes very essential to know about the basic statistics of authentic images and resolve the inconsistent pattern in the image.

The following are the main contributions of the proposed CMFD method.

It computes LIOP features over circular blocks (instead of standard square blocks used by traditional CMFD methods) to generate the rotation-invariant feature vector. LIOP features present the more detailed image information by employing the direction-based relation of the central pixel to its neighborhoods. Therefore, it helps identify those features that are robust to postprocessing attacks of CMF (like scaling and rotation changes) and assist in effectively detecting the CMF.

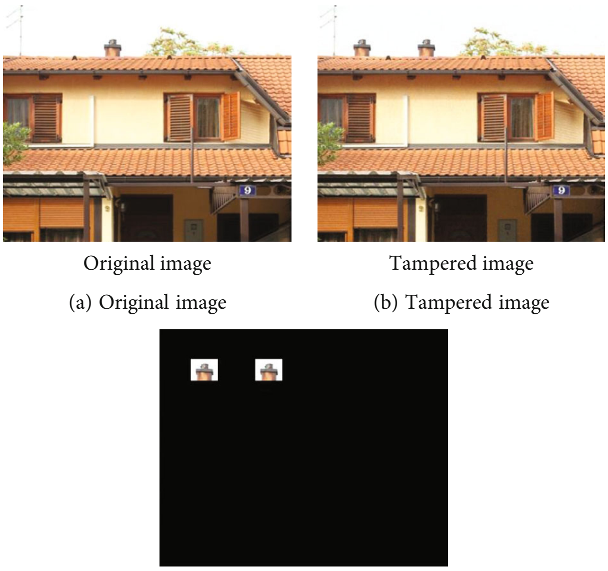
It is proficient in identifying single and multiple CMF from digital images.

It also minimized the feature vector's size for block representation which reduces the computational complexity for CMFD without utilizing any clustering and machine learning methods.

The remaining sections of this paper are structured as follows: state-of-the-art CMFD methods are reviewed in Section 2. In Section 3, the methodology of the proposed CMFD method is presented in detail. The experimental results are presented in Section 4. Finally, the conclusion along with future work directions is presented in Section 5.

2. Related Works

The section presents details of the active and passive image region duplication detection techniques. Alkawaz et al. [9] applied discrete cosine transform with 8×8 overlaying blocks to detect forgery regions in digital images. They also applied lexicographic sort for feature sorting. Bilal et al. [10] employed a fusion of speed-up robust features and binary robust invariant scalable keypoint features for image forgery areas detection. Huang et al. [11] extracted SIFT descriptors of an image. They achieved good detection results for many types of postprocessing, i.e., JPEG compression, size, and angle variations, and under the presence of noise attacks. But the method is not efficient to the low signal-to-noise ratio (SNR) and small-sized tampered areas. Bayram et al. [12] used counting bloom filters (CBF) and fluorescence molecular tomography (FMT) for CMFD. They



Original image

(a) Original image

Tampered image

(b) Tampered image

Detected result

(c) Detected result

Figure 1: A visual example of copy-move forgery (CMF).

used counting bloom filters (CBF) as an alternate to lexicographic sorting. They proposed FMT features for rotated, scaled, and highly compressed images. They achieved time efficiency by using CBF. However, robustness is reduced in that effort. Pan and Lyu [13] used a technique based on SIFT features of the image invariant to traditional sample transform like geometrical and illumination distortions. They used efficient approximation to achieve the correct representative set of features matching and transforming among copied areas. As their performance relies on identifying efficient SIFT features, it causes a limitation for the regions with few visual structures. Another limitation is for the images with intrinsically identical areas, which leads to an increase in a high false-positive rate (FPR). Bo et al. [14] introduced an effective approach for locating CMF based on SURF. It is used for detecting SURF interest points to find the possible copied areas in the suspected samples. This framework is efficient for image transformations and postprocessing attacks like noise, blurring, size, and angle variations; however, it is inefficient for automatically locating forged regions and their boundary. Guo et al. [15] presented a hybrid LBP scheme that matches globally rotation invariant with locally invariant LBP keypoints using local binary pattern variance (LBPV). LBPV is used to measure the directions of the texture image and the distinction between images. This method could decrease the feature dimensions while maintaining the classification accuracy better and better categorization certainty than existing rotation invariant LBP.

Hu moments were used by Liu et al. [16] to detect image forgery. By Gaussian pyramid decomposition, they acquire a low-frequency subimage. They used the overlapping circular subimage blocks and extracted from those circular blocks the Hu moments' characteristics. As they computed Hu moments on the square's inscribed circle, their method is robust to the rotation. So, the false alarm rate increases due to discarding the pixels outside of the inscribed circle. For image forgery detection, Bravo-Solorio and Nandi [17] made attempts based on log-polar maps. To obtain 1D rotation/reflection-invariant descriptors, they used log-polar maps. Then, to those descriptors, they mapped independent overlapping pixel blocks. Then, they mapped independent overlapping blocks of pixels to those descriptors. Their method is efficient in memory usage because of dimension reduction of blocks but is not much robust to high postprocessing like reflection, rotation, and scaling. By integrating discrete cosine transform (DCT) coefficients analysis, Lin and Wu [18] presented a technique for splicing and CMF localization. It blends them with double JPEG compression and SURF. To locate the copy-and-paste operations of sample portions, the former approach is used. To find duplicates of the same entity, SURF is used. This method can identify the forged regions effectively, identify the nonoriginal regions, and detect multiple artifacts. Shivakumar and Baboo [19] suggested detecting SURF and k-dimensional tree-(KD-Tree-) based copy-move forgery. To find copied regions of various sizes, SURF is used. For multidimensional data matching, the latter procedure is used. In image distortion and scaling, this method works well but cannot detect tampered regions of a small scale. A tempered image detection approach based on improved DCT was introduced by Cao et al. [20]. They applied DCT and extracted four features from each block on the fixed-sized image blocks to minimize keypoint vectors' size. For multiple CMF, Gaussian blurring, and noise pollution, this method is successful. It uses the function vector of a reduced dimension.

A passive forgery identification approach employing a dyadic wavelet transform (DWT) was suggested by Muhammad et al. [21]. This scheme's input image is split into approximation (LL1) and subbands of detail (HH1). Matched pairs are obtained based on the resemblance between LL1 and HH1. For booming copy-move detection, this method offers the best approach to finding matched and unmatched portions among blocks of a sample. Kakar et al. [22] suggested a booming content-based image recovery technique to find image forgery based on the MPEG-7 image signature tools. Using a keypoint corresponding procedure that uses the critical constrictions in similar feature pairs distinguishes the copied parts. These techniques help us get high true-positive rates and low false positives for real and synthesized forgeries. Nevertheless, it is accurate only for separate samples and wide duplicated regions. Zhao and Guo [23] suggested a DCT- and SVD-based CMF identification methodology. To obtain quantized blocks further distributed into subblocks, the former technique is employed for fixed-size overlapping image blocks. SVD is implemented in each block, and its highest singular value is used to decrease the dimension as a feature. For a sample influenced by Gaussian blurring or JPEG compression, this technique may identify the forged regions. Lynch et al. [24] used comparison blocks as a dominant feature to minimize the processing cost of image forgery detection. As the dominant function, they used the average grey value of blocks. If their dominant feature varies greatly, a deep level comparison (made by a statistical hypothesis test) of the two blocks will not be made. For images influenced by JPEG compression, Gaussian blurring, etc., or in the case of lighter or darker duplicated areas, their technique worked well. Li et al. [25] used circular block characteristic vectors for CMFD. Feature vectors using rotation-invariant LBP were mined. Their system works well for typical postprocessing activities such as blurring or scaling and geometric transformations such as rotation or flipping. Their methodology, however, lacks the required range of feature dimensions and has less robustness for lower-angle rotations such as 200 or 300 degrees.

Hashmi et al. [26] introduced an effective method for CMF localization employing discrete wavelet transform (DWT) and SIFT features. The former method distributes the suspected sample into four parts. SIFT is used to find the key features. These key features are used to detect the resemblances between descriptor vectors, which helps find the tempered image. This framework identifies image tempering even when the image is scaled/rotated and then pasted. Li et al. [27] worked on the CMFD for the image subjected to affine transforms. They extracted rotation and scaling-invariant features from the image's overlapping circular blocks using polar harmonic transform (PHT). Then, circular blocks were lexicographically sorted, and their Euclidean distances were compared to detect tampered regions. Their method performs well for lower rotation angles like 100 or 120 degree and general angles like 300 or 350 degree. In [28], a digital image forensic technique is proposed that focuses on the detection of image forgery based on the assessment of the light source for an image. This is an object-based method that estimates the lighting properties and hence detects the forgeries for various objects in the image. The model for digital forensics identifies the lighting discrepancies in the objects of an image and provides results indicating a difference between real and fake images. Lighting directions are estimated using azimuth and orientation parameters. The errors that appeared in the results are overcome by implementing the automatic selection of probes. This approach generates the 3D shape which is further used to detect the 3D lighting in the image for various objects. Finally, least-square optimization is used to improve the accuracy of this technique. Zandi et al. [29] presented an accommodative similarity threshold for a CMF identification approach based on locality-sensitive hashing (LSH). LSH is employed for finding the adjacent neighbors, which helps in detecting the forged image. The proposed technique could greatly decrease the number of false matches, improving computational cost and performance. Tian et al. [30] presented a method to locate the forensic changes from the digital images. Initially, the input sample was divided into overlapping blocks. The oriented FAST and rotated BRIEF (ORB) algorithm was employed over each block to compute the features. After that, the cosine and Jaccard distance metrics were used to measure the similarity between the computed keypoints. The approach in [30] exhibits better forgery detection accuracy which utilize ORB features and novel similarity measure technique; however, it may not perform well for the images showing huge scale variations. Kumar et al. [31] proposed a technique to correctly identify the forgery and imitations in the digital images. This technique works for images having any type of object present in the scene. By assessing the lighting parameters, this technique identifies the manipulated object and returns the angle of incidence concerning the light source direction. Two patches are taken from the original part while one patch is chosen from the fake part of the image. The differences between their angle values prove that the image is fake concerning lighting assessment in the scene. In this approach, if the angle difference is more or less than 10 degrees between the fake and original patch, then the patch is considered a forgery. If the angle is within this defined angle difference range, then image patches are considered consistent patches; otherwise, the patches are inconsistent and therefore belong to a forged part. The proposed method is tried on JPEG images browsed from online forged images or taken from well-known research datasets. The demonstrated results produce a robust forgery recognition rate on an image dataset comprising various types of manipulated images.

Abdel-Basset et al. [32] introduced a method to identify the image manipulations. Initially, the SIFT approach was applied to an input image to calculate the keypoints. Then, density-based spatial clustering technique was used to compute the clusters from detected features. Thirdly, RANSAC was utilized to remove the false clusters. Finally, the Structural Similarity Index (SSIM) metric was used to detect the matching areas. The method in [32] is robust to copy-move forgery detection; however, it may not detect the forgeries made within flat image areas. The method in [33] shows better manipulation detection accuracy, however, at the expense of huge computational complexity. Niyishaka and Bhagvati [34] introduced a framework to identify the alterations made within digital images. After preprocessing, the Laplacian of Gaussian (LoG) was applied to compute the blobs of the input sample. Then, BRISK features were computed from each blob, and Euclidian distance was computed among them to locate the matching areas. The method in [34] shows better performance than CMFD; however, for input samples with a large background area, its detection accuracy degrades badly. Soni et al. [35] presented a method to detect image forgeries. Initially, the input sample was distributed into nonoverlapping blocks on which the SURF algorithm was applied to detect the keypoints. Then, similar regions were localized. After this, the maximally stable extremal regions (MSER) technique was used to form the large blocks from each detected matched region. The SURF features were extracted from the identified MSER blocks. In the next step, the affine transform was used to remove outliers. Finally, the similarity was computed to locate forensic changes. The method in [35] performs well for CMFD; however, it may not show good performance under the presence of multiple CMF attacks in an image. Rani et al. [36] introduced the image manipulation detection approach to find image forgeries. To achieve this, a pixel-based forgery detection framework for copy-move and splicing-based forgeries is suggested in this paper. The preprocessing is performed on data to enhance textural information by applying enhanced SURF. Various features are estimated, and template matching is done for the identification of fake image regions. The relevant key parameters are estimated and compared with the calculated threshold value. The demonstrated results show that the proposed framework attains robust detection accuracy compared to the state-of-art image forgery detection techniques. In [37], a technique is proposed for multiple light source-based forgery detection for heterogeneous image surfaces, nearby surface geometry, and texture information to assess the lighting environment. The Phong reflection model is implemented to estimate the structural profiles. The method works in two phases. In the first phase, preprocessing over selected patches is performed followed by angle and error estimations in the second phase. To identify such forgeries, elevation angles concerning mounted light sources are estimated. The value of the elevation angle is computed for various patches of the image. This method is also validated for synthetic image datasets and tested for generalized forged images. An experimental result demonstrates better forgery detection accuracy compared with state-of-the-art methods in this domain. [38] proposed a technique to detect image manipulation. By using a single light source, the incident light source angle is returned which is achieved by estimating illumination from the image. This technique is validated by computing the angle for all objects in the scene. The incident and reflection angle for all the image objects should be consistent; however, if these conditions are violated then, objects are not consistent concerning light source direction. Errors are approximated by applying a least-square estimation. The technique shows that from subpatch estimations, the calculation of light source direction can be approximated which itself is unique to detecting image forgery. The obtained differences in the estimated values of angle above a threshold angle are considered as a fake object w.r.t light source, and therefore, the image is taken as phony. Finally, the results demonstrate that the identification of forged parts is successfully done for light-based image forgery detection. Kumar et al. [39] presented a forgery detection technique based on estimations of multiple light source directions. This method uses a pixel patch from the image region to estimate the source light vector. The implementation is done for images where one and more light sources are available in the scene. This technique can identify image forgery in terms of elevation angle obtained from a source of light and surface normal. This technique is tested for both outdoor and indoor images under certain known parameters. The novelty of this technique is that photo manipulation detection is done using a multiple-light source detection. It produces robust performance as compared with state-of-the-art image forensic techniques by making certain assumptions about surface properties and illumination parameters.

Javed and Jalil [40] presented a novel approach for detecting suspicious images using deep learning. The technique transforms the image into the byte level to identify the forgery in real-time. Zhang et al. [41] utilized the joint probability density matrix [JPDM]; the technique after detecting the input image as forged uses JPDM to correlate within the discrete coefficients transform [DCT]. Islam et al. [33] presented a deep learning-based framework, namely, generative adversarial network (GAN) to show the forensic changes made within digital images. Initially, VGG-19 architecture was used to measure the deep features of a suspected sample. Then, two atrous spatial pyramid pooling (ASPP) operations were used to compute both contextual and cooccurrence keypoints, which were later combined to pass to the detection branch. Agarwal and Verma [42] presented a deep learning-based technique, namely, VGGNet along with the adaptive patch matching (APM) method was applied for CMFD. This approach is robust to various image transformation attacks like blurring and compression; however, the technique is suffering from high computational costs. Table 1 presents the critical analysis of the state-of-the-art CMFD methods.

3. Methodology

A detailed description of the proposed CMFD method for the detection of copy-move forgery is presented in this section. Firstly, the color image is converted to grayscale. Secondly, the image is distributed into circular blocks of 8×8 pixels. In the third step, features are extracted from each circular block of the image by applying the LIOP descriptor [48]. In the fourth step, a comparison of blocks' features is performed by applying Euclidean distance to highlight the forged regions of the image. Postprocessing is performed as the last step to make the detection results clearer. A visual presentation of the proposed CMFD method is exhibited in Figure 2.

3.1. Formulation of the Problem. In CMF, similarities of the tampered regions are always small against a predefined threshold. So, for tampered grayscale images, CMFD focuses on identifying two nonintersecting regions that are hole-less and have larger similarities.

For an image represented by $I(x, y)$, the forged image $I^{'}(x, y)$ depends on the regions $S = \{s_1, s_2, \cdots . s_n\}$ that is

Table 1: Overview of the state-of-the-art CMFD methods.

Reference	Framework	Limitations
Bilal et al. [1]	SURF descriptor along with mDBSCAN clustering technique was employed to locate the forged area in a given image. This method exhibits better CMFD performance.	The approach is unable to detect the manipulation from the flat regions of the image.
Roy et al. [43]	The SURF descriptor together with the RLBP approach was utilized for keypoint computation, while the g2NN method was used for similarity measurement. Finally, hierarchical clustering [44] approach was utilized to cluster the manipulated part of the input image. The method works well under the presence of postprocessing operations.	The approach exhibits poor detection accuracy over samples of low quality.
Alkawaz et al. [9]	In this method, correspondence between the DCT coefficients was computed by employing the Euclidian distance formula to identify the forgeries from the input images. This framework exhibits better CMFD performance.	The false choice of block size can lead to a serious reduction in detection accuracy.
Bilal et al. [10]	In this approach, two methods, namely, SURF and BRISK, were used to compute the image features. The hamming distance was computed to measure the similarity between the keypoints. And the DBSCAN clustering approach was employed to localize the altered content. This method is robust to image transformation operations.	The intense changes in scaling, brightness, and color reduction may degrade the detection performance.
Bi et al. [45]	This work employed SIFT descriptor for features computation along with an adaptive patch matching algorithm for similarity measurement. The work performs well for CMFD.	This technique is computationally complex.
Chen et al. [46]	A block-based CMF detection approach, namely, the BSMRG algorithm, was applied to identify the altered image patches. The method is computationally efficient.	The performance of this method is highly dependent on the block size.
Muzaffer and Ulutas [47]	This method used a SIFT descriptor-based approach for CMFD where binarized descriptors were employed to identify the manipulated regions. This work is computationally less expensive.	Performance needs further improvements.
Tian et al. [30]	After dividing the image into small blocks, the ORB algorithm was employed over each block to compute the features. Then, the cosine and Jaccard distance metrics were used to measure the similarity to locate the CMF. The approach exhibits better CMFD accuracy.	Performance degrades for the samples with huge scale variations.
Abdel-Basset et al. [32]	In this work, the SIFT approach together with the density-based spatial clustering technique was used to identify the forensic changes. The method is robust CMDF and exhibits better detection accuracy.	Unable to locate the changes made within flat image regions.
Islam et al. [33]	A deep learning-based framework DOA-GAN was introduced to locate the image forgeries. The approach shows better manipulation detection accuracy even under the occurrence of postprocessing attacks.	This technique is economically inefficient.
Niyishaka and Bhagvati [34]	In this technique, the LoG was applied to compute the blobs of the input sample. Then, BRISK features were computed from each blob, and Euclidian distance was computed among them to locate the matching areas. The approach shows better performance to CMFD.	The performance of this method degrades for samples with a large background area.
Soni et al. [35]	In the presented framework, the SURF algorithm along with the MSER technique was applied to detect the digital alterations from the input samples. The method performs well for CMFD under the occurrence of noise and light alterations.	Not robust to detect the multi-CMF attacks.

mathematically defined as follows:

$$S_l = S_k \Rightarrow \|s_2\| < s_t \Leftrightarrow |\Delta| > V_t, \tag{1}$$

where

$$\|s_2\| = \sum_{i=1}^{n} |s_{li} - s_{ki}|, \tag{2}$$

where s_2, a metric norm, represents the distance between source regions s_k and destination regions s_l of the forged region. The s_2 must be less than the similarity threshold d_t, whereas $\Delta = (\Delta x, \Delta y)$ is the translation vector, and $V_t = [V_{tx}, V_{ty}]$ is the corresponding threshold. Therefore,

$$\begin{aligned} s_k &= \mathrm{s}_l + \Delta, \\ \mathrm{s}_l &= s_k - \Delta. \end{aligned} \tag{3}$$

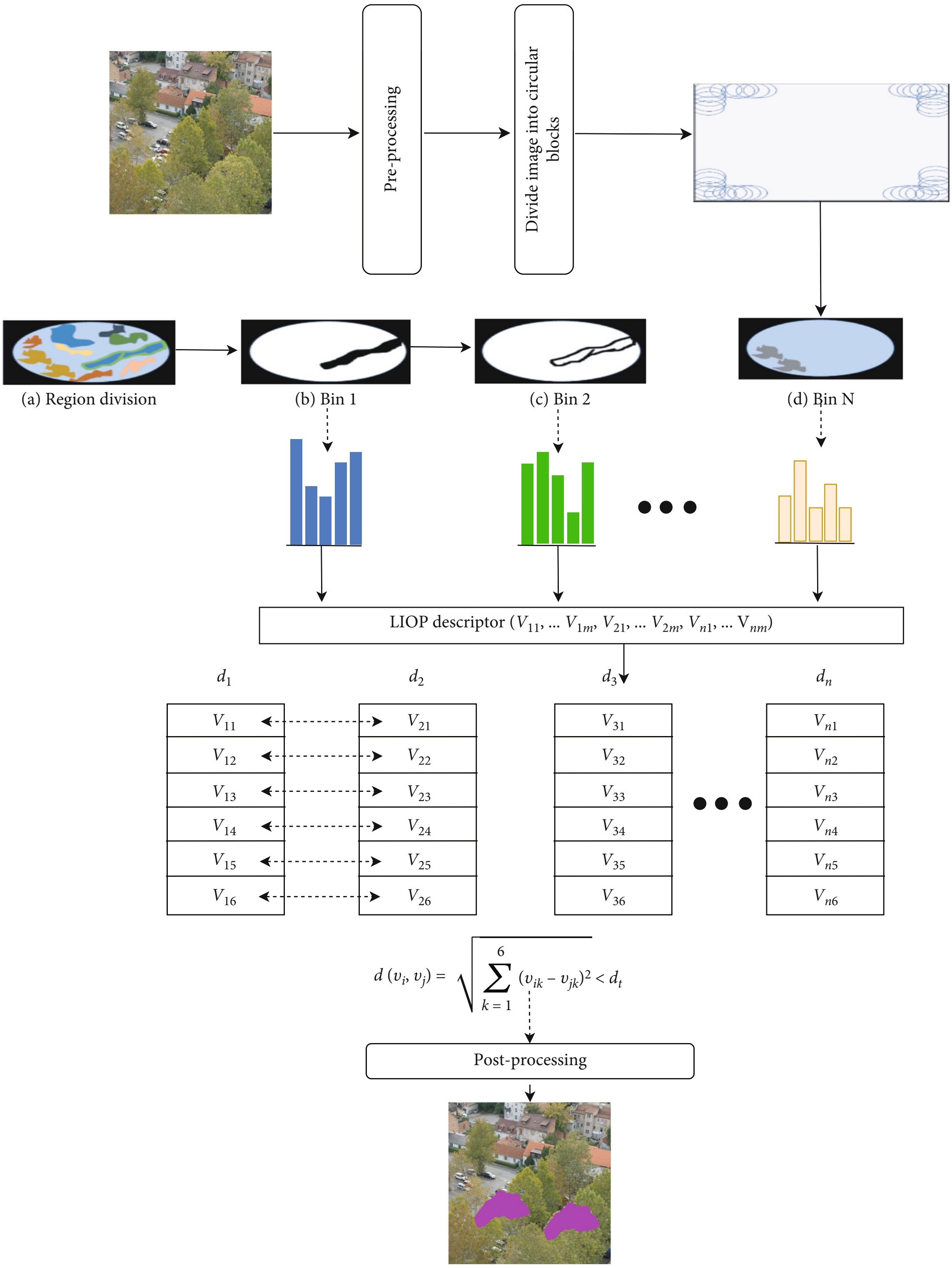

Pre-processing
Divide image into circular blocks
(a) Region division
(b) Bin 1
(c) Bin 2
(d) Bin N
LIOP descriptor (V_{11}, ... V_{1m}, V_{21}, ... V_{2m}, V_{n1}, ... V_{nm})
d_1
d_2
d_3
d_n
V_{11} V_{12} V_{13} V_{14} V_{15} V_{16}
V_{21} V_{22} V_{23} V_{24} V_{25} V_{26}
V_{31} V_{32} V_{33} V_{34} V_{35} V_{36}
V_{n1} V_{n2} V_{n3} V_{n4} V_{n5} V_{n6}
$d\,(v_i, v_j) = \sqrt{\sum_{k=1}^{6} (v_{ik} - v_{jk})^2} < d_t$
Post-processing

Figure 2: A visual presentation of the proposed CMFD method.

Due to the postprocessing attacks on the images, detecting forgery while handling rotation and scaling attacks can be harder for rotation and scale-invariant descriptors. Hence, the proposed CMFD method also incorporates the mechanism for handling rotation and scale variances within the image. The postprocessing attacks of scaling and rotation on the forged image can be mathematically modeled using the following equations that serve as an image forgery

```
ImgIn ➔ The input image matrix
ImgGray ➔ Grayscale image
ImgBlocks ➔ A two-dimensional matrix where each block is represented by $8 \times 8$ pixels
ImgFeatures ➔ Matrix representing feature space
EDist ➔ Euclidean distance between neighborhood features
D ➔ Region marker based on the threshold
ImgReconst ➔ Reconstructed image
Thresh ➔ Threshold determining if the Euclidean distance between feature spaces could mark the region
Step 1: ImgGray ← Grayscale(ImgIn) //Convert the RGB image into grayscale image
Step 2: ImgBlocks ← Divide(ImgGray,8) //divide the image into [$8 \times 8$] circular blocks
Step 3: FOREACH block in ImgBlocks
        ImgFeatures ← Extract LIOP features(block) //extract LIOP features from each circulate block
        END
Step 4: For $i$ = 1: Size(ImgFeatures)-1
          EDist ← Euclidean(ImgFeatures[i], ImgFeatures[i+1])
            IF(EDist <= Thresh)
            D[i]=1
            ELSE
            D[i]=0
            END
        END
Step 5: ImgReconst ← Postprocessor(D)
```

Algorithm 1: Algorithm of the proposed CMFD method.

model:

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix},$$
$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \varphi & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}, \quad (4)$$
$$x'' = \lambda\varphi x' \cos\theta + \lambda\varphi y' \sin\theta,$$
$$y'' = -\lambda\varphi x' \sin\theta + \lambda\varphi y' \cos\theta,$$

where x' and y' denote the coordinates of the duplicated area of the image; θ, λ, φ denote the angle of rotation, a scaling factor, and flipped area of the forged image, respectively. Forger applies postprocessing attacks over an entire image like blurring and noise, to conceal the forgery effects, making it difficult to detect forgery. Hence, the proposed CMFD method aim is to detect the duplicated regions d_l and d_k to highlight the duplicated contents in the existence of various postprocessing operations.

3.2. Preprocessing and Division of the Image into Circular Blocks. After visually analyzing duplicated regions in the illumination domain, a standard color space conversion method is employed by the proposed CMFD method to convert each RGB forged image to a grayscale forged image. At first, image key points highlighting the distinct information of image content are located, and then, the corresponding feature vectors are captured. A feature vector is a collection of image statistics obtained from the keypoints' local neighborhood. For key points and features to be effective, they should capture distinct positions in an image, and be robust against local geometric distortions, noise, illumination variations, etc. The proposed methodology utilizes LIOP descriptor for keypoint detection and description. For the sake of distinction, the keypoint-based techniques divide the image into subparts, and features are collected for each subpart separately, which are joined together at the end. Most of the existing methods use a pixel-based approach to extract image features. For example, SIFT used a 4×4 grid as the feature extraction source region and 3 to 8 bins in one direction. The other direction, respectively, is utilized by gradient location-orientation histogram (GLOH) as a log-polar grid. These existing methods require a consistent orientation for each subpart of the image and descriptor construction per that specified orientation to make the descriptor rotation invariant. So, the accuracy and efficiency of these methods depend on the selection of subparts orientation. Due to these limitations, these methods are not robust to detect forgeries in postprocessed images. To avoid the orientation estimation for rotation-invariant features, the spin image technique is used, which further divides the image subparts into five circles/rings. However, its discriminative power is low, as it splits the image in one direction, i.e., radial direction, and is unable to handle angular direction. In the proposed CMFD method, the input grayscale image (forged image) is transformed into the circular block using the polar coordinate system that is defined using the following mathematical equation:

$$I(r, \Theta) = P(I(a, b): (a_0, b_0)), \quad (5)$$

where (a_0, b_0) is the origin of the circle, r is the radius, and the Θ is the axis of the circle. As compared to grid-type region decomposition methods, it has low discriminative power. In grid-type region decomposition, all local pixels of an image subpart are sorted as per their intensities in

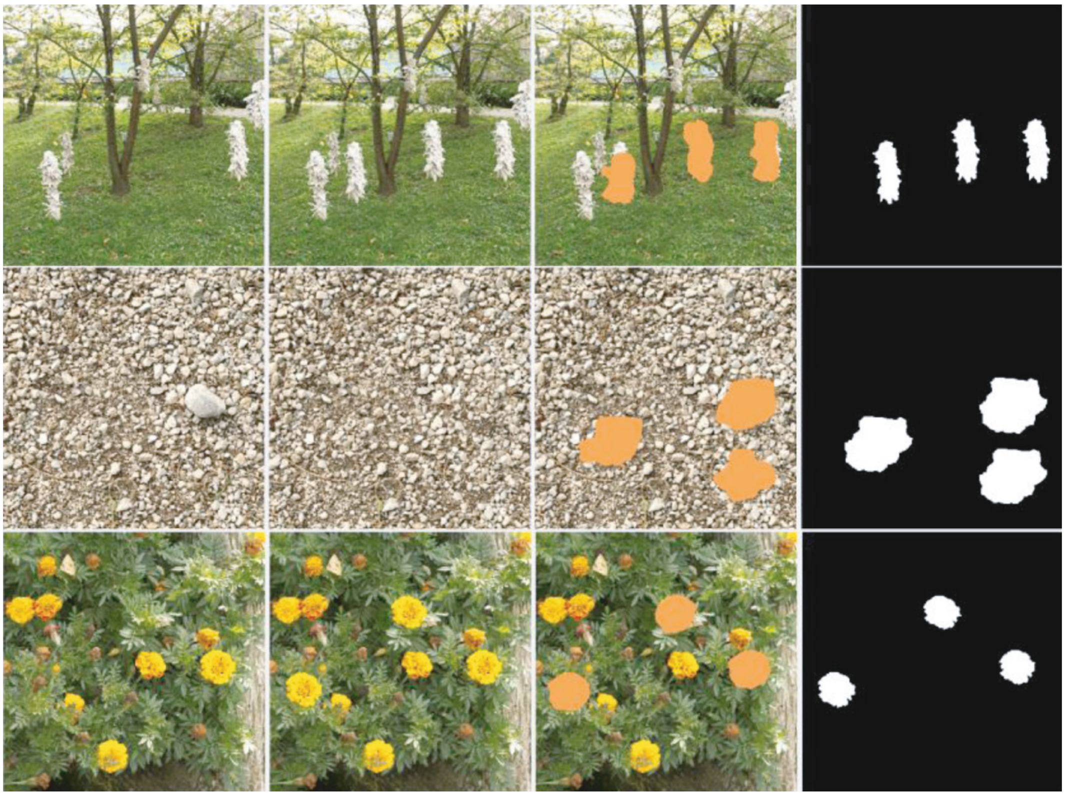


Figure 3: Visual results of multiple CMFD using the proposed CMFD method on tampered images of the CoMoFoD dataset.

Table 2: Precision, recall, and F-measure of the proposed CMFD method on the CoMoFoD dataset (values of the performance parameters are in normalized form).

CoMoFoD images	Precision	Recall	F-measure
Leaves	0.9029	0.7774	0.8355
Rocks	0.8407	0.9791	0.9046
Flowers	0.9890	0.7521	0.8544

Table 3: Performance analysis of the proposed CMFD method on the CoMoFoD dataset after applying different postprocessing attacks on the images (values of the performance parameters are in normalized form).

Operation	Precision	Recall	F-measure
JPEG compression	0.9967	0.7637	0.8518
Rotational transformation	0.9794	0.7571	0.8541
Color reduction	1	0.6268	0.7706
Scale transformation	0.9998	0.7212	0.8379
Additive noise	1	0.7222	0.8387
Blurring	0.9929	0.6738	0.8028
Contrast adjustment	1	0.7178	0.8358
Brightness change	0.9993	0.7474	0.8552

ascending order. Then, subparts are further decomposed into B ordinal bins as per their order of intensities. This region decomposition is invariant to postprocessing attacks like rotation and contains more information than ring-type region decomposition. The circular blocks are fed into the feature extraction step of the next section.

3.3. Local Intensity Order Pattern-Based Features. The local information of subparts of the image varies depending upon the methods used for feature description. For example, the spin image method develops a histogram based on the intensity change of local subparts of the image while SIFT and GLOH populate histograms based upon the gradient's orientation. More recent methods focus on more robust features of local regions of the image, like LBP-based methods used histogram of local binary patterns which are centrally symmetric, and local ternary patterns (LTP) are also used to populate histogram which is a step ahead of LBP. LBP and LTP use the intensities of sample points that are centrally symmetric, so do not consider the relationship of sample points in the neighborhood. They also require locally consistent neighboring points in orientation to make rotation invariance better. However, these methods make them vulnerable to errors in orientation estimation. Keeping these facts into view, the local intensity order pattern (LIOP) can be used to overcome these limitations of existing methods for effective feature representation of the image contents. The proposed CMFD method uses LIOP features for the salient objects of the forged image which uses the intensity order of neighboring sampled points as the local information. It is robust to the rotation because its sampling is rotation-invariant and maps the consistent local orientation. Due to all these reasons, its expected discriminative power is

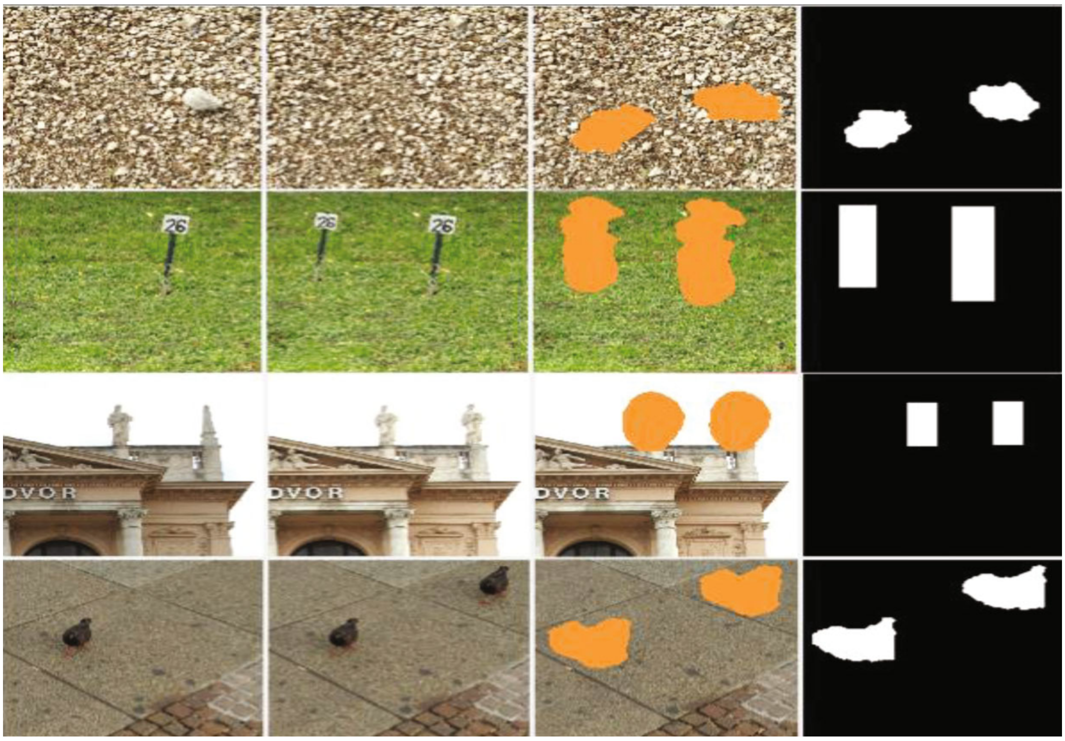


FIGURE 4: Visual results of the proposed CMFD method on the CoMoFoD dataset after applying different postprocessing attacks on images (top-bottom, rotational, scale transformation, blurring, and color reduction).

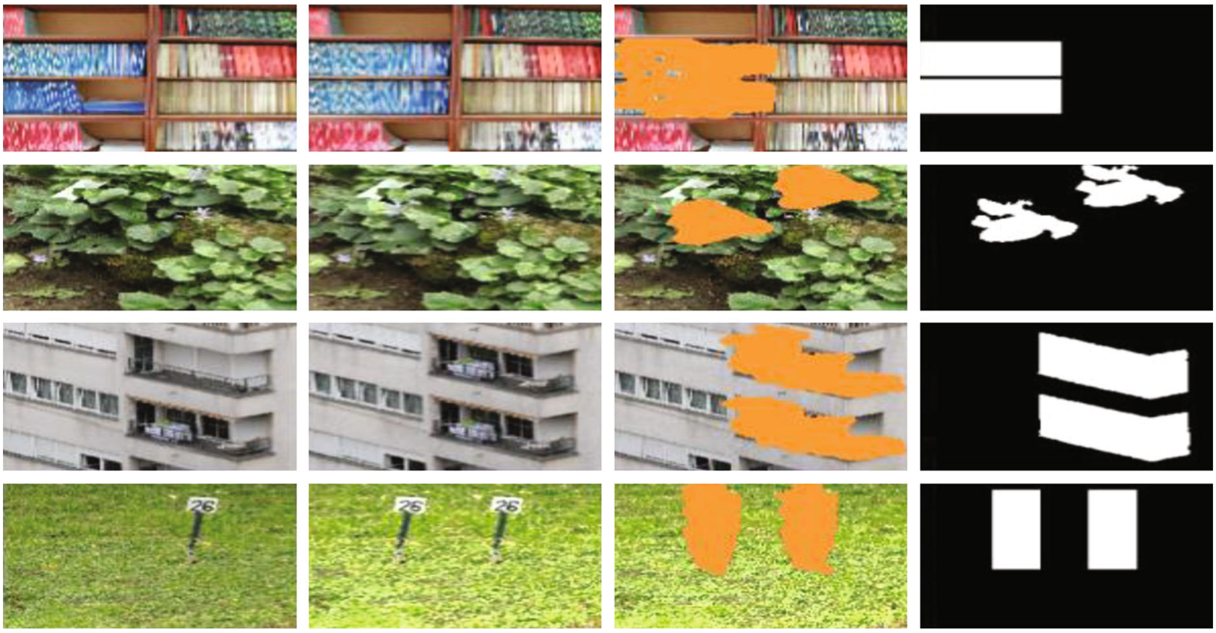


FIGURE 5: Visual results of the proposed CMFD method on the CoMoFoD dataset after applying different postprocessing attacks on images (top-bottom, contrast adjustment, JPEG compression, additive noise, brightness change).

high as compared with existing sparse representation-based methods like SIFT and SURF.

3.4. The Formation of LIOP Feature Vectors. In this step, the proposed CMFD method computed the LIOP descriptors from detected keypoints that are stored in ordinal bins and formed the feature descriptor from each circular block of the image. Mathematically, the LIOP descriptor can be defined as follows:

$$\text{LIOP descriptor} = \left(\text{des}_1, \text{des}_2, \text{des}_3, \cdots \cdots, \text{des}_p\right),$$
$$\text{des}_i = \sum_{x \in \text{bin}_i} w(x)\text{LIOP}(x), \tag{6}$$

Table 4: Performance comparison in terms of precision, recall, and F-measure parameters of the proposed CMFD method with its competitive methods on the CoMoFoD dataset.

Name of the parameter	Agarwal and Chand [50]	ZM-cart [51]	PCT-polar [51]	Proposed CMFD method
Precision (%)	95.70	0.8480	0.8770	**96.60**
Recall (%)	97.80	0.5090	0.4910	**98.00**
F-measure (%)	96.73	0.6361	0.6295	**97.29**

Table 5: Performance analysis of the proposed CMFD method in the existence of different postprocessing attacks on the tampered images of the KLTCI dataset (values of the performance parameters are in normalized form).

Operation	Translation	Scale+Flip	Rotate+Flip	Illumination change	Blur 3 × 3	Blur 5 × 5	Average performance
JPEG-80	0.9907	0.9641	0.9701	0.9703	0.9841	0.9516	0.9718
JPEG-100	0.9981	0.9756	0.9812	0.9929	0.9905	0.9737	**0.9853**
SNR-30	0.9711	0.9251	0.9365	0.9419	0.9406	0.9297	0.9408
SNR-40	0.9957	0.9705	0.9812	0.9834	0.9887	0.9692	0.9814

where $w(x)$ is the weighting function, which, upon any changes in rotation and monotonic intensity, increases the invariance of LIOP descriptors, and LIOP(x) is the LIOP descriptor of a circular block of point x (origin of a circular block). A LIOP point with a more distinct neighborhood is given a larger weight to make the descriptor more robust. The weighting function $w(x)$ is mathematically defined as follows:

$$w(x) = \sum_{i,j} \operatorname{sgn}\left(\left|I(x_i) - I\left(x_j\right)\right| - T_{l_p}\right) + 1, \tag{7}$$

where sgn () is the sign function and $w(x)$ counts the distinct sample pairs and measures the intensity variations of neighboring sample points for a circular block of point x. Let $B(x)$ be an M-dimensional vector of point x in the local patch, with the intensities of M neighboring sample points of point x. The LIOP(x) is mathematically expressed as follows:

$$\begin{aligned} \mathrm{LIOP}(x) &= \Theta(\gamma(B(x))), \\ \mathrm{LIOP}(x) &= U_{M!}^{\mathrm{Ind}(\gamma(B(x)))}, \\ \mathrm{LIOP}(x) &= \left(0, \cdots, 0, \ (\mathrm{Ind}\overset{1}{(}\pi)) \, , 0, \cdots, 0\right), \end{aligned} \tag{8}$$

where $B(x) = (I(x_1), I(x_2), \cdots, I(M_x)) \in B_M$ and $I(x_i)$ represents the intensity of i^{th} neighboring sample point x_i. The local patch is distributed into $M!$ partitions where a LIOP represents every partition. The point x has M neighboring sample points, which are distributed equally along a circle having a radius R. For creating rotation invariant samples, the first point is sampled to point x from the local patch's center along the radial direction, and the farther point out of the two radial direction points is chosen as the starting sample point. The $M-1$ points that are remaining are inspected in an anticlockwise way. The four neighboring points of x, i.e., x_1, x_2, x_3, and x_4, remain consistent in all the patches that are rotated, i.e., x'_1, x'_2, x'_3, and x'_4, respectively. Due to the one-to-one relationship between the subset and the permutation, all the probable permutations in Π^M listed in an index table can be made by encoding BM's subsets. To map $M!$-dimensional feature vector $W_{i_{M!}}$ with permutation π, a function Θ is formulated over the index table; all Θ elements are 0 besides the i^{th} element, which is Equation (6). The Θ is mathematically formulated as:

$$\Theta(\pi) = \mathrm{W}_{M!}^{\mathrm{Ind}(\pi)}, \pi \in \Pi M, \tag{9}$$

where $\mathrm{Ind}(\pi)$ is the index of π in the index table and $W(\mathrm{Ind}\,(\pi)/M!) = (0,\cdots,0, (1/(\mathrm{Ind}(\pi))), 0,\cdots,0)$. The extracted circular block-based features of each circular region of the image are now ready to get matched in the next step.

3.5. Feature Matching. As mentioned earlier, CMFD focuses on identifying duplicated regions that are (a) nonintersecting and (b) have a similarity count less than a defined threshold. To show the copied regions from the given query image, the resemblance among each circular block-based feature is computed using the Euclidean distance formula that is mathematically defined as follows:

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 - \left(y_i - \mathrm{y_j}\right)^2} < T, \tag{10}$$

where x_i, y_i, x_j, and y_j are indicating the locations of the pixels of keypoints from two blocks. T is a defined threshold with a global value of 0.7 for the proposed CMFD method. Therefore, the data points from the two circular block-based features are said to be similar if the distance d_{ij} among them is less than 0.6; otherwise, they are declared as unforged. The threshold value has a substantial impact on the matching process, as choosing a very small value of the threshold results in an increased rate of false matches, while using a large threshold value in the CMF process causes to eliminate the detection of forged areas.

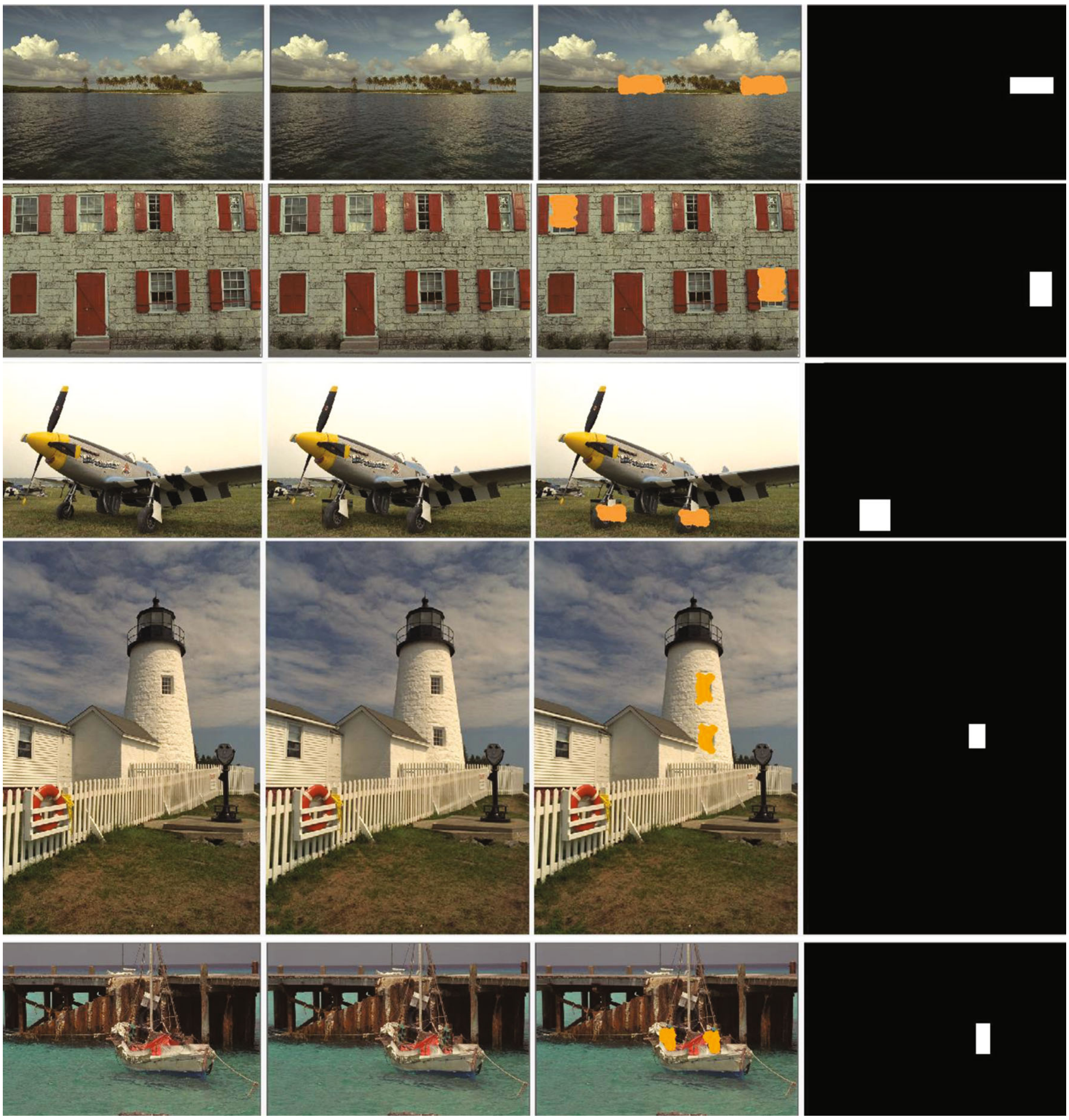


Figure 6: Visual results of the proposed CMFD method on tampered images of the KLTCI dataset.

The complete algorithm of the region duplication detection from digital images using the proposed CMFD method is as follows:

4. Evaluation Measures, Experimental Results, and Discussions

4.1. Performance Evaluation Measures. For the proposed CMFD method, assessment measures, i.e., precision (P), recall (R), and F-measure, are utilized to measure and compare the detection results of the proposed CMFD method with ground-truth images. Precision is the fraction of the percentage of predicted forged samples that are forged. (i.e., locate samples that are already manipulated). A recall is the fraction of the percentage of actual forged samples that are properly predicted forged (i.e., the number of returned samples being identified as manipulated from all the forged). F-measure is a composite metric that is used to measure the accuracy of the proposed CMFD method as it employs both P and R parameters. These performance parameters are mathematically defined in the following equations.

$$P = \frac{T_p}{T_p + F_p},$$
$$R = \frac{T_p}{T_p + F_n}, \tag{11}$$
$$F\text{-measure} = 2 \times \left(\frac{P \times R}{P + R}\right),$$

where T_p indicates the total samples, which are accurately detected as forged, F_p indicates the total misclassified

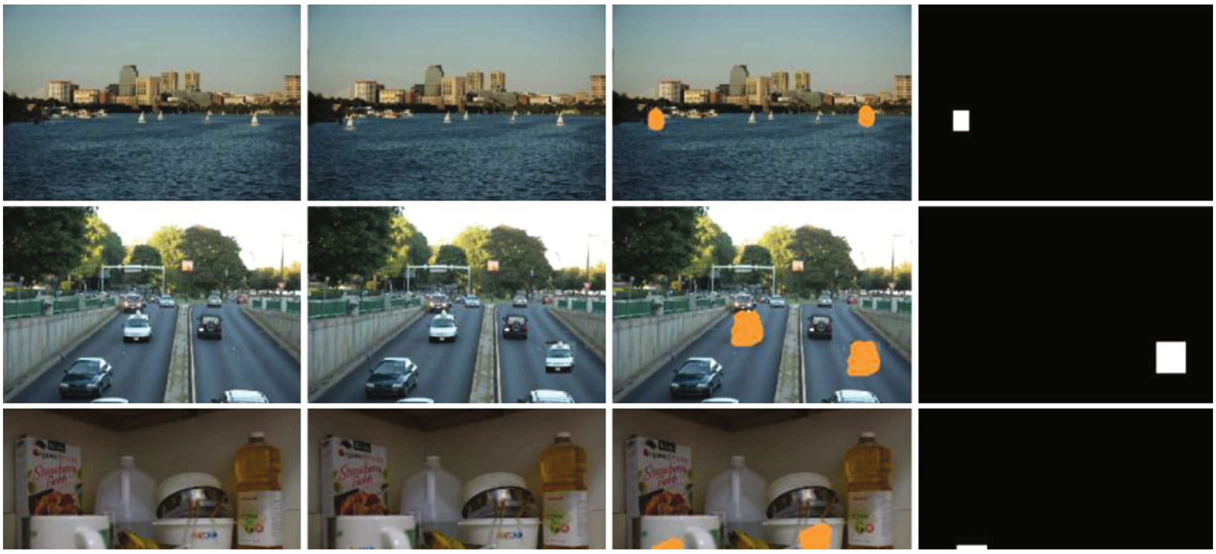


Figure 7: Visual results of the proposed CMFD method on the tampered images of the MICC-F220 dataset.

Table 6: Performance comparison of the proposed CMFD method on the MICC-F220 dataset with state-of-the-art CMFD methods (values of the performance parameters are in normalized form).

Methods	Precision	Recall	F-measure
Manu and Mehtre [54]	0.9050	0.9550	0.929328
Cozzolino et al. [51]	1.0000	0.5940	0.745295
Thampi et al. [55]	0.8160	0.9273	0.868097
Proposed CMFD method	0.9835	0.9682	0.97579

Table 7: Performance comparison in terms of the computational complexity of the proposed CMFD method with its competitor CMFD methods on the MICC-F220 dataset.

Methods	CPU time (in seconds)
Proposed CMFD method	03.32
Yang F. et al. [56]	12.40
Yang B. et al. [57]	10.20
Soni et al. [35]	09.20
Popescu and Farid [8]	70.97
Fridrich et al. [58]	294.69

samples as forged, and F_n indicates the proportion of samples wrongly classified as original and forged.

4.2. Experimental Requirements and Results. The performance of the proposed method is evaluated using three standard datasets of the CMF that are CoMoFoD, KLTCI, and MICC-F220. The experiments are computed on a computer with the following hardware and software specifications; Microsoft Windows 8.1 (64-bit), MATLAB 2017b (64-bit), Intel Core i7 processor with 2.4 GHz, 500 GB hard disk drive, and 8 GB of RAM.

4.2.1. Performance Evaluation on Copy-Move Forgery Detection (CoMoFoD) Dataset. The CoMoFoD dataset contains 260 forged image sets in two categories [49]. The first category contains image sets, each with a dimension of 512 × 512 pixels, and the second category contains 60 image sets, each with a dimension of 3000 × 2000 pixels. These images have different forgery attacks like translation, splicing, rotation, distortion, and scaling. Different types of postprocessing methods are applied to all tempered and genuine samples, such as JPEG compression, noise adding, blurring, and color reduction. The experimental details of the proposed method on this dataset are reported in the following subsequent sections.

(1) Multiple CMFD Demonstrations. In this section, experimental details of the proposed CMFD method are analyzed by tampering with multiple forged areas of the image on the CoMoFoD dataset. The performance analysis of the proposed method in terms of visual results is presented in Figure 3. Table 2 presents its experimental details on different images of the CoMoFoD dataset in terms of performance parameters that are precision, recall, and F-measure. After analyzing experimental details in this section, it can be concluded that the proposed CMFD method produces robust performance on the CoMoFoD dataset in the case of multiple forged areas of the image.

(2) Postprocessing Attack Demonstration. Postprocessing attacks on images include blurring, additive noise, compression, variations in brightness levels, color reduction, contrast adjustment, and rotational and scale invariance. Table 3 illustrates that the proposed CMFD method performs remarkably even in the presence of postprocessing attacks on the images of the CoMoFoD dataset. The visual results of the proposed CMFD method are shown in Figures 4 and 5 after applying different postprocessing attacks on the images of the CoMoFoD dataset, which also proves the robust performance of the proposed CMFD method.

The robustness of the proposed CMFD method is also tested by comparing its performance with state-of-the-art forgery detection methods. Table 4 presents experimental details in terms of precision, recall, and F-measure parameters of the proposed CMFD method and its comparison with competitive forgery detection methods. After analyzing experimental details in Table 4, it can be concluded that the proposed CMFD method also produces robust performance as compared with its competitive methods.

4.2.2. Performance Evaluation on the Kodak Lossless True-Color Image (KLTCI) Dataset. The KLTCI dataset [52] contains 24 photographic-quality images of different subjects under various lighting conditions and various locations; the images are high-dimension with a resolution of 1024×1536 pixels. The images of this dataset comprise several backgrounds and exterior conditions such as sea, sky, walls, and buildings. By using Adobe Photoshop, tempered images for the KLTCI dataset are manipulated. The various combinations of postprocessing attacks, i.e., translation, blurring, and rotation, along with CMF, are used to construct forged images. Copy-move regions in this dataset possess an approximate dimension that varies from 100×100 pixels to 550×200 pixels. Table 5 presents the performance analysis of the proposed CMFD method on the KLTCI dataset in the occurrence of several postprocessing attacks. After reviewing the experimental information provided in Table 5, it can be concluded that in the presence of various postprocessing attacks on the tampered images, the proposed method also exhibits a robust performance on the KLTCI dataset.

The visual results of the proposed CMFD method on different sample images of the KLTCI dataset are shown in Figure 6, which also proves its robust performance on this dataset. In Figure 6, the first to fourth columns show the original images, tampered images, detection results of the proposed CMFD method, and ground-truth images, respectively.

4.2.3. Performance Evaluation on the MICC-F220 Dataset. The MICC-F220 [53] dataset contains 220 images. The dataset contains a tampered image using a scale and rotational transformation. The tampered images included in this dataset have different sizes ranging from 700×400 pixels to 800×600 pixels. The analysis of the proposed CMFD method is evaluated using the MICC-F220 dataset, and its experimental results are compared with state-of-the-art CMFD methods that are Manu and Mehtre [54], Cozzolino et al. [51], and Thampi et al. [55]. The visual results of the proposed CMFD method conducted on the MICC-F220 dataset are shown in Figure 7. The comparison detail of the proposed CMFD method in terms of performance evaluation parameters is presented in Table 6. The experimental analysis in terms of visual and evaluation parameters on this dataset also proves the robustness of the proposed CMFD method.

4.2.4. Comparison of Computational Complexity. The performance analysis of the proposed CMFD method is also performed by considering its computational complexity as compared with competitor CMFD methods. Its computational complexity is reported on a desktop computer equipped with the following hardware and software resources: CPU: Intel Core i7@2.10 GHz, RAM: 8 GB, hard disk: 500 GB, Windows 10 operating system (64 bit), MATLAB 2017B (64 bit), VLFeat version 0.9.21-MATLAB library. Table 7 presents details of the computational complexity (time in seconds) of the proposed CMFD method and its comparison with competitor CMFD methods on the MICC-F220 dataset.

5. Conclusion and Future Directions

In this article, a novel method of copy-move forgery detection from digital images is presented. The proposed CMFD method divides the image into circular blocks and computes a rotation-invariant feature vector from each circular block. The similarity between each feature vector is computed by applying a Euclidean distance to detect forged image areas and to remove false matches. The LIOP descriptor assists the proposed CMFD method in effectively detecting the tampered areas of the image even in the presence of different postprocessing attacks and also enables it to effectively detect the single and multiple CMF areas of the image. The LIOP descriptor also assists the proposed CMF method to detect the tampered regions more efficiently as compared with SIFT and SURF features. The proposed CMFD method produces promising results on the CoMoFoD, KLTCI, and MICC-F220 datasets as compared to the state-of-the-art CMFD methods. There is room for improvement of the proposed CMFD method to detect small and extremely smooth, or blurred regions from the tampered images. The performance of the proposed CMFD method can also be analyzed by considering the deep learning-based method for CMF as well as other types of forgeries can be considered like image splicing.

Data Availability

The authors have used publicly available data to support the findings of this study that is included within the article.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

All the authors declare no conflict of interest.

Authors' Contributions

Each author has worked equally.

Acknowledgments

This research work was carried out as a joint research collaboration at the University of Engineering and Technology, Taxila, Pakistan; Politecnico di Milano, Milano; Sejong University, Seoul, South Korea; Captial University of Science and Technology (CUST), Islamabad; and University of Jeddah, KSA. The authors are thankful for this support.

References

[1] M. Bilal, H. A. Habib, Z. Mehmood, R. M. Yousaf, T. Saba, and A. Rehman, "A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering," *Australian Journal of Forensic Sciences*, vol. 53, no. 4, pp. 459–482, 2021.

[2] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, *Detection of Copy-Rotate-Move Forgery Using Zernike Moments*, Springer, 2010.

[3] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[4] B. Shivakumar and S. S. Baboo, "Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors," *International Journal of Computer Applications*, vol. 27, no. 3, pp. 9–17, 2011.

[5] 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.

[6] T. Mahmood, A. Irtaza, Z. Mehmood, and M. T. Mahmood, "Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images," *Forensic Science International*, vol. 279, no. 10, pp. 8–21, 2017.

[7] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *Journal of Visual Communication and Image Representation*, vol. 53, no. 5, pp. 202–214, 2018.

[8] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, 2005.

[9] 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*, vol. 30, no. 1, pp. 183–192, 2018.

[10] M. Bilal, H. A. Habib, Z. Mehmood, T. Saba, and M. Rashid, "Single and multiple copy–move forgery detection and localization in digital images based on the sparsely encoded distinctive features and DBSCAN clustering," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2975–2992, 2020.

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

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

[13] 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.

[14] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *2010 International Conference on Multimedia Information Networking and Security*, Nanjing, Jiangsu, China, 2010.

[15] Z. Guo, L. Zhang, and D. Zhang, "Rotation invariant texture classification using LBP variance (LBPV) with global matching," *Pattern Recognition*, vol. 43, no. 3, pp. 706–719, 2010.

[16] 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.

[17] 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.

[18] S. D. Lin and T. Wu, "An integrated technique for splicing and copy-move forgery image detection," in *2011 4th International Congress on Image and Signal Processing*, Shanghai, China, 2011.

[19] B. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *International Journal of Computer Science Issues (IJCSI)*, vol. 8, no. 4, p. 199, 2011.

[20] 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.

[21] 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.

[22] P. Kakar, N. Sudha, and W. Ser, "Exposing digital image forgeries by detecting discrepancies in motion blur," *IEEE Transactions on Multimedia*, vol. 13, no. 3, pp. 443–452, 2011.

[23] 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.

[24] 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.

[25] 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.

[26] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," in *2013 13th International conference on intellient systems design and applications*, Salangor, Malaysia, 2013.

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

[28] M. Kumar and S. Srivastava, "Identifying photo forgery using lighting elements," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 1–5, 2017.

[29] M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2499–2512, 2016.

[30] X. Tian, G. Zhou, and M. Xu, "Image copy-move forgery detection algorithm based on ORB and novel similarity metric," *IET Image Processing*, vol. 14, no. 10, pp. 2092–2100, 2020.

[31] M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," *International Journal of Image and Graphics*, vol. 19, no. 3, p. 1950014, 2019.

[32] M. Abdel-Basset, G. Manogaran, A. E. Fakhry, and I. El-Henawy, "2-levels of clustering strategy to detect and locate copy-move forgery in digital images," *Multimedia Tools and Applications*, vol. 79, no. 7-8, pp. 5419–5437, 2020.

[33] A. Islam, C. Long, A. Basharat, and A. Hoogs, “DOA-GAN: dual-order attentive generative adversarial network for image copy-move forgery detection and localization,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Seattle, WA, USA, 2020.

[34] P. Niyishaka and C. Bhagvati, “Copy-move forgery detection using image blobs and BRISK feature,” *Multimedia Tools and Applications*, vol. 79, no. 35-36, pp. 26045–26059, 2020.

[35] B. Soni, P. K. Das, and D. M. Thounaojam, “Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features,” *Journal of Information Security and Applications*, vol. 45, pp. 44–51, 2019.

[36] A. Rani, A. Jain, and M. Kumar, “Identification of copy-move and splicing based forgeries using advanced SURF and revised template matching,” *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 23877–23898, 2021.

[37] A. Rani and A. Jain, “Digital image forgery detection under complex lighting using Phong reflection model,” *Journal of Electronic Imaging*, vol. 31, no. 5, article 051402, 2022.

[38] M. Kumar and S. Srivastava, “Image authentication by assessing manipulations using illumination,” *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12451–12463, 2019.

[39] M. Kumar, S. Srivastava, and N. Uddin, “Forgery detection using multiple light sources for synthetic images,” *Australian Journal of Forensic Sciences*, vol. 51, no. 3, pp. 243–250, 2019.

[40] A. R. Javed and Z. Jalil, “Byte-level object identification for forensic investigation of digital images,” in *2020 International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, 2020.

[41] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, and X. Sun, “A robust forgery detection algorithm for object removal by exemplar-based image inpainting,” *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 11823–11842, 2018.

[42] R. Agarwal and O. P. Verma, “An efficient copy move forgery detection using deep learning feature extraction and matching algorithm,” *Multimedia Tools and Applications*, vol. 79, pp. 7355–7376, 2020.

[43] A. Roy, R. Dixit, R. Naskar, and R. S. Chakraborty, “Copy-move forgery detection with similar but genuine objects,” in *Digital Image Forensics*, pp. 65–77, Springer, 2020.

[44] J. Friedman, T. Hastie, and R. Tibshirani, *The Elements of Statistical Learning*, Springer series in statistics, New York, 2001.

[45] X. Bi, C.-M. Pun, and X.-C. Yuan, “Multi-scale feature extraction and adaptive matching for copy-move forgery detection,” *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 363–385, 2018.

[46] C.-C. Chen, L.-Y. Chen, and Y.-J. Lin, “Block sampled matching with region growing for detecting copy-move forgery duplicated regions,” *Inf Hiding Multimed Signal Process*, vol. 8, no. 1, pp. 86–96, 2017.

[47] G. Muzaffer and G. Ulutas, “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.

[48] Z. Wang, B. Fan, and F. Wu, “Local intensity order pattern for feature description,” in *2011 International Conference on Computer Vision*, Barcelona, 2011.

[49] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, “CoMoFoD—new database for copy-move forgery detection,” in *ELMAR, 2013 55th international symposium*, Zadar, Croatia, 2013.

[50] S. Agarwal and S. Chand, “Image forgery detection using co-occurrence-based texture operator in frequency domain,” in *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, pp. 117–122, Springer, 2018.

[51] 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.

[52] M. M. Isaac and M. Wilscy, “Copy-move forgery detection based on Harris corner points and BRISK,” in *Proceedings of the Third International Symposium on Women in Computing and Informatics*, Kochi India, 2015.

[53] 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.

[54] V. Manu and B. M. Mehtre, “Copy-move tampering detection using affine transformation property preservation on clustered keypoints,” *Signal, Image and Video Processing*, vol. 12, no. 3, pp. 549–556, 2018.

[55] S. M. Thampi, A. Gelbukh, and J. Mukhopadhyay, *Advances in Signal Processing and Intelligent Recognition Systems*, Springer, 2014.

[56] 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.

[57] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, “A copy-move forgery detection method based on CMFD-SIFT,” *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 837–855, 2018.

[58] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” *in Proceedings of Digital Forensic Research Workshop*, Citeseer, 2003.