IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 July 2023, accepted 8 August 2023, date of publication 14 August 2023, date of current version 17 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3304728

RESEARCH ARTICLE

Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Keypoint Architecture

ANJALI DIWAN[1], (Senior Member, IEEE), DINESH KUMAR[1], (Senior Member, IEEE), RAJESH MAHADEVA[2,3], (Member, IEEE), H. C. S. PERERA[2], AND JANAKA ALAWATUGODA[4,5]

[1]Department of CE-AI, Marwadi University, Rajkot, Gujarat 360003, India
[2]Department of Physics, Khalifa University, Abu Dhabi, United Arab Emirates
[3]Division of Research and Innovation, Uttaranchal University, Dehradun 248012, India
[4]Research Innovation Centers Division, Faculty of Resilience, Rabdan Academy, Abu Dhabi, United Arab Emirates
[5]Institute for Integrated and Intelligent Systems, Griffith University, Nathan, QLD 4111, Australia

Corresponding authors: Anjali Diwan (anjali.diwan@ieee.org) and Rajesh Mahadeva (rajeshmahadeva15@gmail.com)

This work was supported by the Rabdan Academy, Abu Dhabi, United Arab Emirates (UAE), funded by the Research Internal Fund.

ABSTRACT The authentication of digital images poses a significant challenge due to the wide range of image forgery techniques employed, with one notable example being a copy-move forgery. This form of forgery involves duplicating and relocating segments of an image within the same image, often accompanied by geometric transformations to deceive viewers into perceiving the forged image as authentic. Furthermore, additional processing techniques like scaling, rotation, JPEG compression, and the application of Additive White Gaussian Noise (AWGN) are frequently employed to further obscure any traces of forgery, making the detection and verification process even more complex. This paper presents a novel approach for detecting copy-move forgery in digital images using the self-supervised image keypoint detector, SuperPoint. Our approach leverages the advanced capabilities of SuperPoint, which combines keypoint detection and descriptor extraction, to identify and localize copy-move forgery accurately. One important aspect of our approach is its ability to handle images with different textures, including smooth and self-similar structural images. The proposed approach is able to produce stable results in images with various attacks, making it a functional and reliable tool for detecting copy-move forgery in a diverse range of forged images. Comparative analysis with existing forgery detection methods shows the superior performance of our proposed approach. Furthermore, the computational efficiency of our algorithm enables real-time forgery detection. Our approach using SuperPoint offers an effective solution for detecting copy-move forgery in digital images, making it valuable for image forensics and authenticity

INDEX TERMS Multimedia forensics, digital image forgery, image forgery detection, copy-move forgery, image duplication, keypoint detector, SuperPoint detector, deep learning.

I. INTRODUCTION

Digital images have become a primary source of information in today's world, with the widespread use of low-cost digital cameras and social media platforms. However, this has also led to the proliferation of image manipulation, which raises doubts about the authenticity of digital images, particularly in fields such as news reporting, research, and legal proceedings. However, the easy availability of powerful image editing software like Photoshop, GIMP, Fireworks, and Inkscape has made it easy to manipulate images without leaving any discernible evidence of forgery, which poses a significant threat to the authenticity and trustworthiness of digital images. To address this problem, various techniques have been developed, which can be broadly classified into two categories: active and passive methods. Active methods use digital watermarking or digital signatures to verify the authenticity of images, but they require pre-embedded

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

information, limiting their availability. In contrast, passive methods, also known as blind authentication methods, do not require any prior information and can detect copy-move forgery. Passive approaches are more practical and widely applicable, making them a popular area of research.

Copy-move forgery is a popular image forgery approach where a portion from an image is copied and moved at a different region on the same image, making it appear as if the duplicated region is authentic. This approach is used to exaggerate certain image information or to conceal specific parts of an image. Forgery perpetrators employ a variety of geometrical and post-processing techniques to eliminate traces of forgery, rendering forgery detection a challenging task. The extensive modifications made to image features complicate the process of identifying and verifying the authenticity of digital images. Figure (1) shows some examples of images with copy-move forgery from CASIA V2.0 and MICC-F220 datasets.

Traditional methods of copy-move forgery detection can be categorized into two groups based on their reliance on handcrafted features: block-based and keypoint-based. Block-based methods extract local features from overlapping patches, while keypoint-based methods focus on patches of keypoints. We will discuss these techniques in detail in the following subsections.

A. BLOCK-BASED METHOD

In block-based approaches, the image is split into overlapping or nonoverlapping blocks of fixed size, and feature vectors are determined for each block to identify forged images [1], [2]. Various techniques have been developed for block-based copy-move forgery detection. Emam et al. [3] used PCET kernel with ANN searching along with LSH for finding the similarity in the blocks. It results in the effective detection of forgery in geometrical transformed copy-move images. Wang et al. [4] employed Quaternion Exponent Moments (QEMs) for block feature extraction, enabling the detection of forgery in rotated and scaled images. However, this approach falls short in detecting multiple copy-move instances within an image. Bi and Pun [5] utilized local bidirectional coherency as a technique for detecting copy-move forgery. Thirunavukkarasu et al. [6] employed LL sub-band DSWT (Discrete Stationary Wavelet Transform) and multidimensional scaling to reduce the dimensionality of features in their study. Chen et al. [7] utilized Fractional Quaternion Zernike Moments (FrQZMs) along with patch-matching techniques for detecting copy-move forgery in their study. Yan et al. [8] employed circular PCET blocks of multiple radii and lexicographic order matching to effectively detect forged regions with large-scale rotation and scaling.

B. KEYPOINT-BASED APPROACH

Block-based approaches can detect ordinary copy-move forgery without post-processing in images but are limited in their ability to detect geometrical attacks and require high computational costs. Keypoint-based methods extract and match keypoints to detect a forgery in images [9]. Emam et al. [10] have used tow stage detection where a scale-invariant feature operator and Harris corner detector are used. Warif et al. [11] utilized the SIFT and Mirror SIFT algorithms to handle variations in scale and image rotation. Beijing Chen et al. [7] have proposed a method for detecting copy-move forgery using fractional quantization moments and a patch-match scheme. Chen et al. [12] have proposed a copy-move forgery detection method based on SIFT features and invariant moments. Liu et al. [13] have proposed a combined feature extraction method using Local Intensity Order Pattern (LIOP) and SIFT keypoint for copy-move forgery detection. The nearest neighbor matching algorithm is used to match keypoints. Elhaminia et al. [14] proposed a probabilistic method for forgery detection using Markov Random Fields. Their approach involves over-segmentation of images, followed by clustering of similar regions, and extraction of SURF and PCT features from labeled keypoints. Emam et al. [15] have used SFOP detector and MROGH descriptor to address copy-move with geometrical. Emam et al. [16] have further used the MROGH descriptor with the DoG operator to address copy-move forgery in the smooth image where the number of keypoints is less. They have addressed this problem effectively in their approach. Meena and Tyagi [17] proposed a two-step method for copy-move forgery detection, where the SIFT keypoint detector is used for the textured region, and Fourier Miller Transform (FMT) is used for the smooth region. Wang et al. [18] proposed a forgery detection method that uses keypoint detection and segmentation to address images with different textures. The method uses SURF keypoints and PCET features. However, the method struggles to detect forged images with large-scale changes, and the time complexity is high in some steps. Armas et al. [19] proposed a hybrid method for detecting copy-move and splicing forgeries. The method is based on two approaches: error level analysis (ELA) and color filter array (CFA), which require both modified and unmodified images.

But, these methods have limitations, such as the need for robustness against image processing techniques and computational inefficiency. This has led researchers to explore deep learning models as an alternative, which have shown promising results in improving the accuracy of copy-move forgery detection. Several deep learning-based methods have been proposed for copy-move forgery detection [20], including end-to-end deep neural networks, two-branch architectures, adaptive attention, residual refinement networks, and pyramid feature extractor blocks [21]. These methods have different strengths and limitations, such as their ability to detect accurate boundaries and small forged regions [20], [22]. Deep learning approaches are useful in making the detection approach time-efficient [23], [24]. Some of the researchers used deep learning-based methods for copy-move forgery detection [21], [25], [26]. Prelearn-trained neural networks can be used for a real-time comprehensive forgery detection approach.

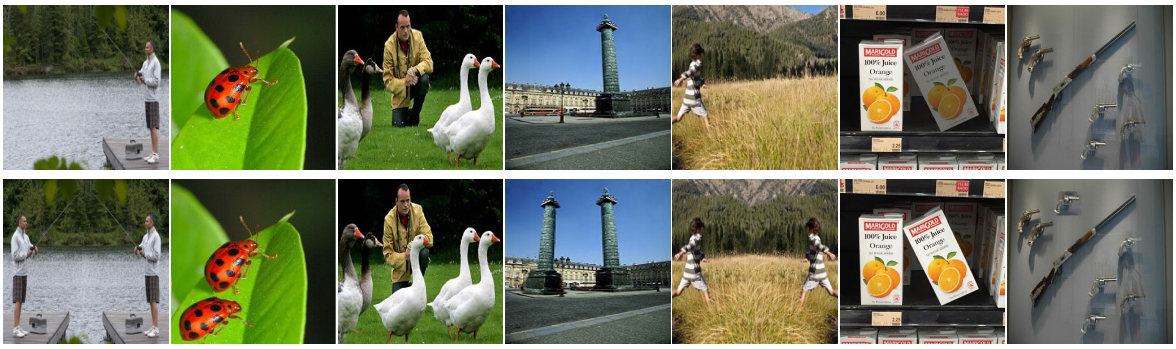

FIGURE 1. Some example images depicting copy-move forgery: here the first row consists of an authentic image and the second row consists forged image.

C. MOTIVATION

There are several limitations present in the existing approaches for copy-move image forgery detection. Some of them are mentioned below:

1) Sensitivity to image quality: Some methods may be sensitive to variations in image quality, such as compression artifacts, noise, and distortion. This can lead to false positives or false negatives in forgery detection.
2) Limited scalability: Some methods may not be scalable to large datasets of images, or may have high computational complexity, which can limit their practical use.
3) Limited generalization: Many existing methods may not generalize well to unseen or unknown types of forgery, or to images with significant differences in texture, lighting condition, blur, brightness change, colour reduction, contrast adjustment, JPEG compression, noise addition, and non-affine transformation over forged images.
4) Limited image type: The existing literature lacks studies that specifically address the detection of forged images with diverse properties, including variations in image sizes, forged region sizes, and image file formats. There is a notable research gap in the detection of forged images with diverse characteristics.

D. OUR CONTRIBUTION

Our proposed technique for copy-move image forgery detection utilizes a novel keypoint-based approach SuperPoint [27]. SuperPoint is a deep neural network that takes an input digital image and produces keypoint and their descriptors. SuperPoint is designed to be fast and efficient, making it suitable for real-time applications. The SuperPoint detector is used to extract keypoints from the image and prepare descriptors for the detected keypoints. To identify similar keypoints, the k-NN is used for the matching process, and for the search technique we are using BBF with the k-d tree. The forged region within an image is detected using keypoint clustering, specifically employing the Fuzzy C-Means clustering algorithm. To eliminate outliers in the forgery detection process, RANSAC (Random Sample Consensus) is utilized.

Some of the main contributions of the proposed method are mentioned below:

1) Previous research has paid less attention to detecting forged images that have been subjected to flip attacks, and even fewer studies have addressed the detection of forged images that suffer from combinations of rotation, scaling, and other post-processing attacks. In contrast, our proposed method demonstrates strong capability in effectively detecting forged images subjected to flip attacks, and a combination of scaling, rotation, and other post-processing.
2) Our method is capable of detecting various novel attacks, such as significant differences in texture, lighting condition, blur, brightness change, colour reduction, contrast adjustment, JPEG compression, noise addition, and non-affine transformation over forged images. Furthermore, our method demonstrates effective detection of forged images that undergo combined attacks with rotation, and scaling within the forged region.
3) Our proposed approach for detecting copy-move image forgery surpasses existing methods in terms of processing time required.
4) Our approach demonstrates efficient detection of forged digital images created from diverse datasets using original images. These datasets have images with different sizes, forged region sizes, and image file formats. These datasets are CMFD, GRIP, MICC-F2000, MICC-F220, MIC-F220, COVERAGE, CoMoFoD, and CASIA V2.0. This demonstrates the versatility and robustness of our approach in detecting copy-move image forgery across different datasets.

In this paper, we propose a novel approach that combines keypoint detection with a SuperPoint architecture to detect copy-move forgery in digital images, with a focus on improving the accuracy and robustness of detection in the presence of various image manipulations.

The structure of this paper is as follows: In Section II, the Methodology for copy-move forgery detection is discussed.

In Section III, the SuperPoint detector and descriptor are discussed. In Section IV, the proposed SuperPoint-based approach is discussed. In Section V, the type of Copy-move forgery and the evaluation metrics used are discussed. In Section VI, Dataset used is discussed. In Section VII, results and discussion is done. In Section VIII, we discuss the conclusion.

II. METHODOLOGY FOR COPY-MOVE FORGERY DETECTION

Our forgery detection method consists of six main steps: Pre-processing, Extraction of Feature (Keypoint), Keypoint Descriptor Computation, Keypoint Matching, Keypoint Clustering, and Affine Transformation Estimation. This section briefly discusses the standard copy-move forgery detection pipeline.

With the development of various approaches for forgery detection, the workflow can be represented as follows:

- Pre-processing: Pre-processing is an optional step in digital image forensics that is used for information reduction of the digital image. Examples include RGB to grayscale or YCrCb image conversion [28], and various methods like HSV, LBP, filters, and transforms can be used [29].
- Feature representation: Feature representation involves extracting image keypoint feature descriptors. The quality of the feature representation directly impacts the accuracy and efficiency of the forgery detection system. Different methods, such as filters, transforms, and descriptors like SIFT and SURF, can be used to extract feature vectors. This step is crucial as it reduces the amount of data that needs to be processed while retaining the relevant information for forgery detection.
- Keypoint matching: Keypoint matching involves finding similarities between feature descriptors of duplicated regions in an image. Different methods have been used for this purpose, such as sorting, nearest neighbor technique, hashing, hierarchical structure-based, and segmentation-based approaches. The matching process is critical in determining the accuracy and effectiveness of the forgery detection system [30].
- Outlier removal: False matching can occur during the feature matching process, where non-forged regions may appear as forged. To address this, outlier removal techniques are used. Some common techniques include RANSAC, thresholds, constraints, and criteria-based decisions. These techniques help to eliminate false positives and increase the accuracy of the detection [31].
- Localization: Localization of the forged region's accurate boundary is crucial for understanding the extent of the forgery, but limited research has been conducted in this area [32].
- Optimization: Optimization is the process of refining the detected forged region by removing false positives and filling small holes or smoothing broken edges. Morphological operations such as dilation, erosion, opening, and closing are commonly used for this purpose [33].

III. SuperPoint KEYPOINT DETECTOR AND DESCRIPTOR

SuperPoint is a self-supervised interest point detector and descriptor that was proposed by DeTone et al. [27]. Unlike traditional methods that require manual annotations or pre-defined filters for feature extraction, SuperPoint learns to detect and describe keypoints in an end-to-end manner. It constructs a fully convolutional neural network (CNN) that takes an image as input and outputs a set of keypoint locations and descriptors. The network is trained in a self-supervised manner by generating synthetic homographic transformations of input images and computing ground-truth correspondences between them. SuperPoint can handle changes in illumination, viewpoint, and scale.

A. SuperPoint ARCHITECTURE

SuperPoint is a neural network architecture that can detect interest points and produce descriptors of fixed length. It operates on the whole image and has a shared encoder that reduces the dimensionality of the input image. The architecture is subsequently divided into two decoder heads, one dedicated to interest point detection and the other focused on interest point description. The network's parameters are mostly divided between detector and descriptor, unlike traditional systems where interest points are first detected, and then descriptors are computed separately. Efficient sharing of computation and representation is enabled by this approach, as the network's parameters are mostly shared between the two tasks.

B. SuperPoint AS DETECTOR

The SuperPoint detector is a fully convolutional neural network that operates on an input image with full size and outputs a set of interest point detection. It first processes the input image using a shared encoder that reduces the dimensionality of the input. Following the encoder, there are two decoder heads in the architecture: one dedicated to interest point detection, and the other focused on interest point description.

The interest point detection head is responsible for predicting a dense heat map of interest points for the input image. The heat map is a 2D array with the same spatial dimensions as the input image, where each pixel value represents the probability of that pixel being an interest point. The detection head predicts this heat map by applying several layers of convolutional and pooling operations on the encoded input image. Finally, a softmax function is applied to the output to obtain the probability distribution over the pixel values.

The mathematical formulation for the SuperPoint as a detector can be summarized as follows:

Let I be an input image with dimensions $H \times W$, and let $f(I)$ be the output of the shared encoder network. The detection head takes $f(I)$ as input and outputs a heat map M

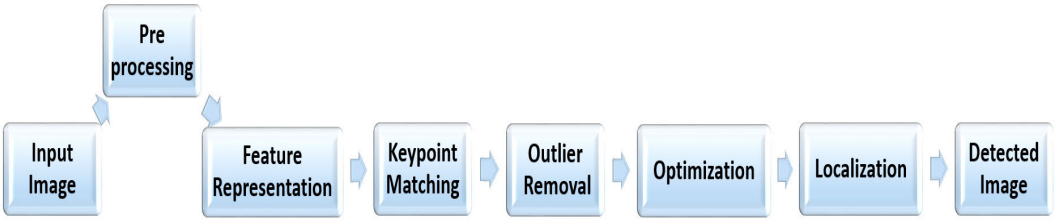

FIGURE 2. Working pipeline of copy-move forgery detection.

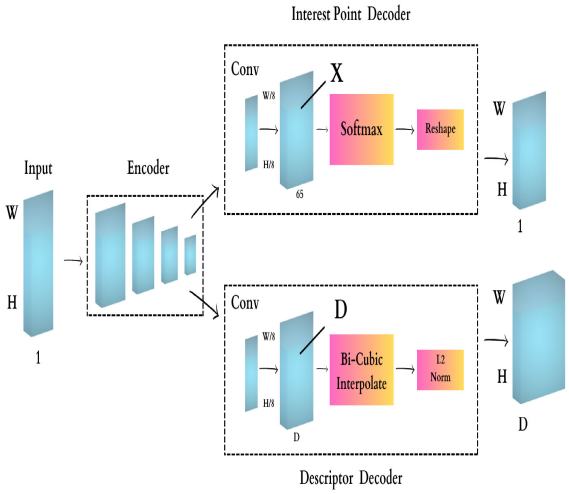

FIGURE 3. Architecture of SuperPoint self-supervised keypoint detector.

with dimensions $H \times W$:

$$M = Softmax(g(f(I))) \tag{1}$$

where g is a function that maps the output of the encoder to the space of the heat map. The softmax function is applied to obtain a probability distribution over the pixel values in M.

The detector then selects the N pixels with the highest values in M as the interest points. These interest points are further processed by the description head to obtain fixed-length descriptors that can be used for matching and registration.

C. SuperPoint AS DESCRIPTOR

SuperPoint generates descriptors by computing feature maps and feature descriptors for each keypoint. The feature maps are extracted using a series of convolutional layers, and the descriptors are computed by pooling the feature maps around each keypoint.

The feature maps are computed as follows:

Let I be the input image with dimensions $H \times W$, and f_θ be the convolutional neural network with parameters θ. The output of the network is a feature map F with dimensions $\frac{H}{8} \times \frac{W}{8} \times D$, where D is the dimensionality of the feature maps.

The keypoints are detected on the feature map F using non-maximum suppression, resulting in a set of keypoints $K = {k_i}^n$, where each keypoint k_i has a 2D location (x_i, y_i) and a scale s_i.

The descriptors are computed as follows:

For each keypoint k_i, a feature descriptor d_i is computed by pooling the feature map F around the keypoint. Let $p_{i,j}$ be the j-th pixel in a $P \times P$ patch centered at k_i. The descriptor d_i is defined as:

$$d_i = \frac{1}{p^2} \sum_{j=1}^{p^2} f_{i,j} \tag{2}$$

where $f_{i,j}$ is the feature value at pixel $p_{i,j}$ in the feature map F.

The resulting descriptor d_i is a vector of dimensionality D, which captures the local appearance around the keypoint k_i.

In summary, SuperPoint generates descriptors by first computing feature maps using a convolutional neural network, then detecting keypoints on the feature maps, and finally computing descriptors by pooling the feature maps around each keypoint.

D. HOMOGRAPHIC ADAPTATION OF SuperPoint

Homographic adaptation in SuperPoint is an important step to refine the keypoints detected by the network. The goal of homographic adaptation is to adjust the keypoints detected in the source region of the image so that they are more accurately localized in the target image region, taking into account any perspective distortion between the two.

To perform homographic adaptation, SuperPoint first detects keypoints in both the source and target image regions using the same neural network. Then, for each keypoint in the source image region, the network predicts a descriptor and a 2D coordinate location. Next, SuperPoint estimates a homography matrix that maps the source image region to the target image region, using the RANSAC algorithm. This homography matrix takes into account any perspective distortion between the two image regions.

Finally, SuperPoint applies the homography matrix to the 2D coordinate locations of the keypoints detected in the source image region, which adjusts them to be more accurately localized in the target image region. The descriptors of the keypoints remain the same. The homographic adaptation step can be formulated mathematically as follows:

Let x be a 2D coordinate location of a keypoint in the source image, and H be a homography matrix that maps the source image to the target image. Then the adapted location of the keypoint in the target image, x', can be computed as:

$$x' = H * x \tag{3}$$

where $*$ denotes matrix multiplication.

In practice, the homography matrix H is estimated using RANSAC based on a set of correspondences between keypoints detected in the source and target images.

IV. PROPOSED SuperPoint-BASED APPROACH

Our copy-move forgery detection method consists of three main steps: keypoint Extraction and Descriptor Computation, Matching of keypoints, and Clustering of keypoints. In the keypoint extraction step, we use the SuperPoint algorithm to extract keypoints from the image. keypoint descriptors are then computed using the SuperPoint descriptor architecture. To identify matched keypoint descriptors, we use the Euclidean distance and a user-defined threshold. The BBF search algorithm is used to efficiently search for the nearest neighbors. Finally, the matched keypoints are clustered.

SuperPoint detector is a keypoint-based technique that simplifies the process of computing image descriptors for geometrically transformed images. In traditional keypoint-based methods, affine transformation estimation is a crucial step in detecting copy-move forgery in such images. However, with the SuperPoint detector, the need for additional affine transformation calculations is eliminated, as it allows for the easy computation of image descriptors for geometrically transformed images. This simplifies the overall process and improves the accuracy of the forgery detection method.

A. KEYPOINT MATCHING

In copy-move forgery detection, we first obtain a set of keypoints $P = k_1, k_2, k_3, \ldots, k_n$, where n is the total number of keypoints in the image. Next, we compute feature descriptors using which can be represented as $D = D_1, D_2, D_3, \ldots, D_n$, where each feature vector D_i corresponds to a keypoint ki.

To identify similar feature descriptors, we need to match each feature vector F_i with all other feature descriptors f_j, except itself. However, if we only examine exact matches of feature descriptors, there is a risk of missing numerous similar feature descriptors in the forged region of the image that has undergone additional post-processing operations.

Hence, we need to compute the Euclidean distance between feature descriptors to effectively detect matched feature descriptors. Therefore, it is essential to calculate the Euclidean distance between feature descriptors in order to accurately identify matched feature descriptors.

To match feature descriptors, we compare the Euclidean distance between f_i and its closest neighbor f_j with the distance between f_i and its second-closest neighbor f_k. If the ratio of these distances is less than a user-defined threshold Th, we consider f_i and f_j as a match. This is represented by the equation:

$$\frac{|f_i - f_j|}{|f_i - f_k|} \leq Th \tag{4}$$

The choice of threshold Th during forgery detection plays a crucial role in determining the accuracy of correct and false matches obtained. A higher value of Th leads to more false matches, while a smaller value of Th may result in some homogeneous feature descriptors remaining undiscovered.

An efficiently search for nearest neighbors in high-dimensional spaces, we use a k-d tree to store the feature descriptors. The construction of a k-d tree involves computational operations on the order of $O(N \log_2 N)$, where N represents the total number of feature descriptors. The Best Bin First (BBF) search algorithm consists of several components that aid in the efficient nearest neighbor search. The algorithm uses a bin structure to organize the feature descriptors.

A set of pivot feature descriptors is chosen from the dataset. These pivots divide the feature space into smaller regions, aiding in efficient search and exploration. The BBF algorithm employs a search strategy that prioritizes exploring the most promising regions first. It begins with the nearest pivots and progressively expands the search to other bins based on calculated distances. Also, pruning techniques are applied to eliminate unpromising regions or bins during the search process. This helps reduce unnecessary distance calculations and speeds up the search. To limit the number of queries, a maximum query number Q_{max} is set. The algorithm drops the query point without further searching for other matching points once reaches Q_{max}.

By utilizing these components, the BBF algorithm efficiently searches for nearest neighbors, providing accurate results for applications like forgery detection.

B. KEYPOINT CLUSTERING

In the process of clustering matched keypoints we are using Fuzzy C-Means (FCM) technique. FCM is a powerful clustering technique capable of effectively grouping data points into multiple clusters. To improve the efficiency of FCM clustering, efforts are made to reduce the computational time by minimizing the objective function. This ensures that the clustering process is completed in a shorter period, allowing for faster analysis and decision-making. The objective function used in FCM is given by:

$$F_m = \sum_{i=1}^{n} \sum_{j=1}^{V} u_{ij}^{m} \left| x_i - c_j \right|^2, 1 \leq m < \infty \tag{5}$$

In the given equation, m is a positive number larger than 1. The total number of data points is represented by n, and the clustering process has v number of clusters. In the given equation, u_{ij} represents the degree of data point x_i in cluster j. Here, x_i represents the i^{th} component of the representative data points, and c_j is the cluster center. The $\|*\|$ denotes the norm that is used to calculate the similarity between a specific feature vector corresponding to the center.

To improve the FCM algorithm, fuzzy partitioning can be used. Fuzzy partitioning utilizes the updation of membership degree u_{ij} and the cluster centers c_j as follows:

$$u_{ij} = \frac{1}{\sum_{k=1}^{v} \left(\frac{\|x_i - c_j\|}{\|x_i - c_k\|}\right)^{\frac{1}{m-1}}} \tag{6}$$

$$c_j = \frac{\sum_{i=1}^{m} u_{ij}^m \cdot x_i}{\sum_{i=1}^{m} u_{ij}^m} \tag{7}$$

Here, um_{ij} represents the membership degree of data point x_i in cluster j after the m_{th} iteration. The repetition of u_{ij} stops when $max_{ij}(u_{ij}^{k+1} - u_{ij}^{k}) < \epsilon$ where ϵ represents the termination value. Here k represents the number of iterations. This step is used to calculate local minima for f_m.

The descriptors of keypoints generated by SuperPoint are compared using the FCM algorithm to cluster them. The matching of center keypoints and their neighbors with different center keypoints and their neighbor clusters leads to a reduced need for analyzing all image keypoints, thereby accelerating the forgery detection process. Each cluster represents a group of keypoints that are similar to each other. By clustering the matched keypoints, the forgery detection process becomes faster and more accurate.

C. PARAMETER SELECTION

We need to take care of setting the parameters for the SuperPoint detector in copy-move forgery detection. It is important to note that parameter selection requires experimentation and fine-tuning based on the specific dataset and the forgery detection task at hand. Additionally, considering the limitations and constraints of computational resources is crucial for real-time or large-scale applications.

The threshold determines the minimum score required for a detected keypoint to be considered valid. Setting a higher threshold may result in fewer keypoints but with higher confidence. It helps filter out weaker keypoints, reducing the chance of false detections. However, a higher threshold may also lead to missing some genuine keypoints. It is essential to strike a balance between the number of keypoints and their quality based on the specific forgery detection requirements. We have selected this threshold on an experiment basis keeping other parameters constant and finding responses for different thresholds for all datasets used.

Non-maximum suppression is a technique used to remove redundant keypoints. It helps to retain only the most salient keypoints by suppressing those in close proximity with similar scores. The suppression radius or distance threshold determines how close two keypoints need to be to consider them redundant. A larger suppression radius may result in more keypoints being suppressed, while a smaller radius may retain more keypoints but with a higher likelihood of redundancy.

D. ALGORITHMIC STEPS OF COPY-MOVE DETECTION

The SuperPoint-based copy-move forgery detection algorithm follows a series of steps to identify and locate forged regions in an input image. Firstly, the input image I undergoes pre-processing operations to enhance its quality and normalize its characteristics, resulting in a preprocessed image. Next, the SuperPoint architecture is employed to detect keypoints in the image. These keypoints, represented as K, are a set of distinct locations within the image that exhibit significant visual features. Feature descriptors are then extracted for the detected keypoints K using the SuperPoint architecture, resulting in a set of feature descriptors. These descriptors capture detailed information about each keypoint, allowing for subsequent analysis and comparison.

To cluster the keypoints based on their similarity, a clustering algorithm such as Fuzzy C-Means (FCM) is applied. The FCM algorithm groups the keypoints with similar feature descriptors into clusters, generating a set of clusters denoted as C. Each cluster represents a group of keypoints that exhibit similar visual characteristics.

The matching and verification stage compares the feature descriptors within and across clusters to identify potential copy-move regions in the image. By analyzing the similarities between the descriptors, matched keypoints or regions are determined and represented as M. These matched keypoints indicate areas within the image that are potentially manipulated or duplicated.

In the forgery localization step, the exact regions that have been forged are localized based on the matched keypoints M. The boundaries of the forged regions are determined by analyzing the distribution and arrangement of the matched keypoints, allowing for the accurate delineation of the copy-move forged areas within the image. Finally, the algorithm generates an output image or report that highlights the locations of the detected copy-move forgery providing a visual representation or detailed information about the forged regions in the input image.

Algorithmic steps for the proposed approach are given in the algorithm 1.

V. TYPES OF COPY-MOVE FORGERY AND EVALUATION METRICS USED

To ensure that our forgery detection method is robust and effective in detecting all types of copy-move forgery, we have conducted experiments on various types of copy-move forged images. These include images with different sizes, resolutions, additive noise, compression levels, blur, brightness change, colour reduction, and contrast adjustment, as well as images that have undergone different types of geometric transformations such as rotation, scaling, flip, and combined

TABLE 1. Details of the dataset used to collect images for experimental work.

Dataset	Total Image	Image Size	Image Content	Image Format
CMFD	1632	388x2592 800x533	Outdoor places, Animals, Building, Indoor scene	PNG
CASIA V2.0	12323	800x600 320x240	Indoor scenery, Plant Animal, Architecture	BMF, TIFF JPEG
GRIP	240	1024X768	Animal, Bird, Flowers, Building, Desert, Human, Sky.	PNG
MICC-F600	600	2048x1536	Flower, Animals, Human House, Natural scene	JPEG
MICC-F220	220	737x492	Beach, Humans, tree bookshelf, Road, mountain	JPEG
CoMoFoD	2160	3000X2000 512X512	Human, City view, Vehicles Grass, Wall, Roof, Building	JPEG PNG
COVERAGE	200	400X486	Indoor view, Rooms, Stores Public places, objects	TIFF

Algorithm 1 Algorithm for SuperPoint Copy-Move Forgery Detection

1: Input digital image (copy-move forgery image or authentic image).
2: Input digital image to Key-point feature extraction.
3: Descriptor generation of the detected keypoints.
4: Clustring of the keypoints by FCM.
5: Affine transformation calculation.
6: Nearest neighbourhood calculation.
7: Feature matching based on set parameters.
8: Outliers and inliers are removed with RANSAC.
9: Binary mask crested for Copy-move forgery perdition and localization.
10: Output image generated for forgery localization if any.

effect. We also tested our method on images that have been subjected to multiple copy-move operations or partial forgery.

A. TYPE OF FORGERY CONSIDERED

Copy-move forgery can be divided into four major categories based on the approach forgery is created. They are:

1) Simple copy-move forgery involves copying and pasting a part of an image into another part of the same image. This can be a single instance or multiple instances of the same copied part. The latter is referred to as multiple copy-move forgery. There is no post-processing applied to these forged images.
2) We conducted an analysis that encompassed forged images subjected to post-processing in order to conceal the forgery. In such instances, the post-processing is often executed with a professional level of skill to increase the difficulty of detecting forgery. Our investigation included examining the impact of various levels of JPEG compression and noise addition on these manipulated images.
3) In addition to the primary post-processing techniques used to conceal footprints of forgery, there are other operations that significantly aid in hiding the forgery. These techniques are difficult to detect as they uniformly alter the image pixels. Some of these techniques include Brightness change (BC), Colour reduction (CR), Contrast adjustment (CA), and Image blurring (IB).
4) Geometrical transformations are a popular technique used in creating forged images, as they can produce realistic copy-move forgery. Such transformations can be applied in three ways: 1) copying a region and moving it by rotating it, 2) scaling a copied region and moving it, and 3) a combination of both scaling and rotating. We particularly focus on flipped images that have undergone a 180-degree rotation.

B. EVALUATION METRIC USED

The experiments conducted in our study focused on evaluating the performance at the pixel level. We used True Positive (TP) to indicate the total number of pixels detected as forged, that is actually forged, False Positive (FP) to indicate the total number of pixels falsely detected as forged, and False Negative (FN) to indicate the total number of pixels falsely detected as not forged. Using these values, we calculated Precision (P), Recall (R) or True Positive Rate (TPR), and F1-Score metrics. The F1-Score is the primary evaluation metric used to assess the efficiency of our proposed approaches and compare them with other reported methods. Its value ranges from 1 (best) to 0 (worst), and we have presented it as a percentage by multiplying it by 100 in our paper. The relationships between P, R or TPR, and F1-Score with TP, FP, and FN are as follows:

$$P = \frac{TP}{TP + FP},$$
$$R = TPR = \frac{TP}{TP + FN},$$
$$F1 = \frac{2TP}{2TP + (FP + FN)}.$$

To assess the effectiveness of our method, we employed various evaluation metrics including precision, recall (or true

TABLE 2. Details of the range of different attacks applied on copy-move forged images.

Attacks	Criterion	CMFD	MICC-F600
Rotation	Degree	2:2:10, 180, 60	2: 2: 10
Scaling	Ratio	0.91: 0.02:1.09	0.91: 0.02: 1.09
JPEG F600	Quality Factor	20:10:100	20: 10: 100
Noise	Standard Deviation	0.02: 0.02: 0.1	20: 20: 100

positive rate), and F1-Score. Precision indicates the ratio of correctly identified positive detections to the total number of detections. The recall represents the ratio of correctly identified positive detections to the total number of actual forged regions. The F1-Score, on the other hand, is the harmonic mean of precision and recall, offering a balanced measure of the overall performance of the algorithm. These metrics provide valuable insights into the accuracy and effectiveness of our method in detecting copy-move forgery in images.

VI. DATASET USED

We have used seven open source datasets CMFD [34], GRIP [35], CoMoFoD [36], MICC-F600 [37], MICC-F220 [37], COVERAGE [38] and CASIA V2.0 [39]. The tables provided give information about the different datasets used in the study and the types of forgeries and their corresponding levels. The datasets used for both training and testing are listed in Table (1), while Table (2) provides a more detailed breakdown of the different types of forgeries and their levels.

1) **CMFD:** The dataset contains over 1.5K images with various textures that have been subjected to copy-move forgery with translation, rotation, scaling, and combinations of these. Both forged and original images have undergone post-processing with JPEG compression and additive Gaussian noise, with nine levels of compression (ranging from 100 to 20 with a step of 10) and five levels of noise (ranging from 0.02 to 0.1 with a step of 0.02).
2) **CASIA V2.0:** The dataset comprises 7491 images, including 5123 forged ones, with various forms of forgery such as splicing and copy-move. From this dataset, we selected 3274 copy-move forged images with different manipulations and post-processing techniques. These images involve translation, rotation, and scaling manipulations, and some are subject to post-processing techniques like JPEG compression and edge blurring.
3) **MICC-F220:** The dataset comprises 220 images, including both original and forged images. The forged images are created using copy-move manipulation with translation, rotation, scaling, or a combination of these processes. Post-processing techniques, such as JPEG compression and additive Gaussian noise, are applied to the images to hide traces of forgery. Some images have single copy-move forgery, while others have multiple instances of copy-move forgery.
4) **MICC-F600:** The dataset consists of 600 images, out of which 440 are original and the remaining 160 have been forged using similar manipulations and post-processing as that of the MICC-F220 dataset.
5) **CoMoFoD:** The dataset comprises original images, and forged images, with each accompanied by its corresponding ground truth image. The forged images are created using five different types of manipulations, namely translation, rotation, scaling, combination, and distortion, with 40 images per category. Moreover, post-processing operations such as JPEG compression, additive noise, brightness change, color reduction, contrast enhancement, and image blur are applied to all the forged images. In total, this dataset provides over 4,000 forged images for analysis.
6) **Coverage:** The dataset comprises 100 images, each with an original and forged version, along with corresponding ground truth images. The images feature a common object and are captured both indoors and outdoors. The forged images have undergone six different types of manipulations, including translation, rotation, scaling, illumination change, free form, and a combination of any of these five. Additionally, the dataset includes 20 images with a combination of different copy-move forgeries.
7) **GRIP:** The GRIP dataset comprises 80 original and 80 forged images with their corresponding ground truth images. The images feature a variety of textures, including smooth, coarse, and self-similar structural textures of monuments. The textural diversity of the images makes this dataset particularly challenging. It is worth noting that the GRIP dataset only includes simple copy-move images without any post-processing or geometrical transformation attacks.

The Table (3) provides details of the images used for training and testing from different datasets in the context of copy-move forgery detection. In Table (3), the ''Training Images'' row indicates the number of images used for training the copy-move forgery detection model from each dataset. Similarly, the ''Testing Images'' row shows the number of images used for evaluating the performance of the trained model on unseen data.

VII. RESULTS AND DISCUSSION

The SuperPoint detector can extract robust and stable keypoints from the images, even when the original features have been altered. By comparing the extracted keypoints from different regions of the image, the detector can identify potential copy-move forgery. Additionally, the SuperPoint descriptor can be used to match the extracted keypoints and accurately determine the degree of geometric

TABLE 3. Details of the image used for the training and testing phase of experimental work.

Dataset	CMFD	CASIA V2.0	CoMoFoD	MICC F600	MICC F220	COVERAG	GRIP
Training Images	864	800	1220	340	110	100	120
Testing Images	768	600	940	260	110	100	120

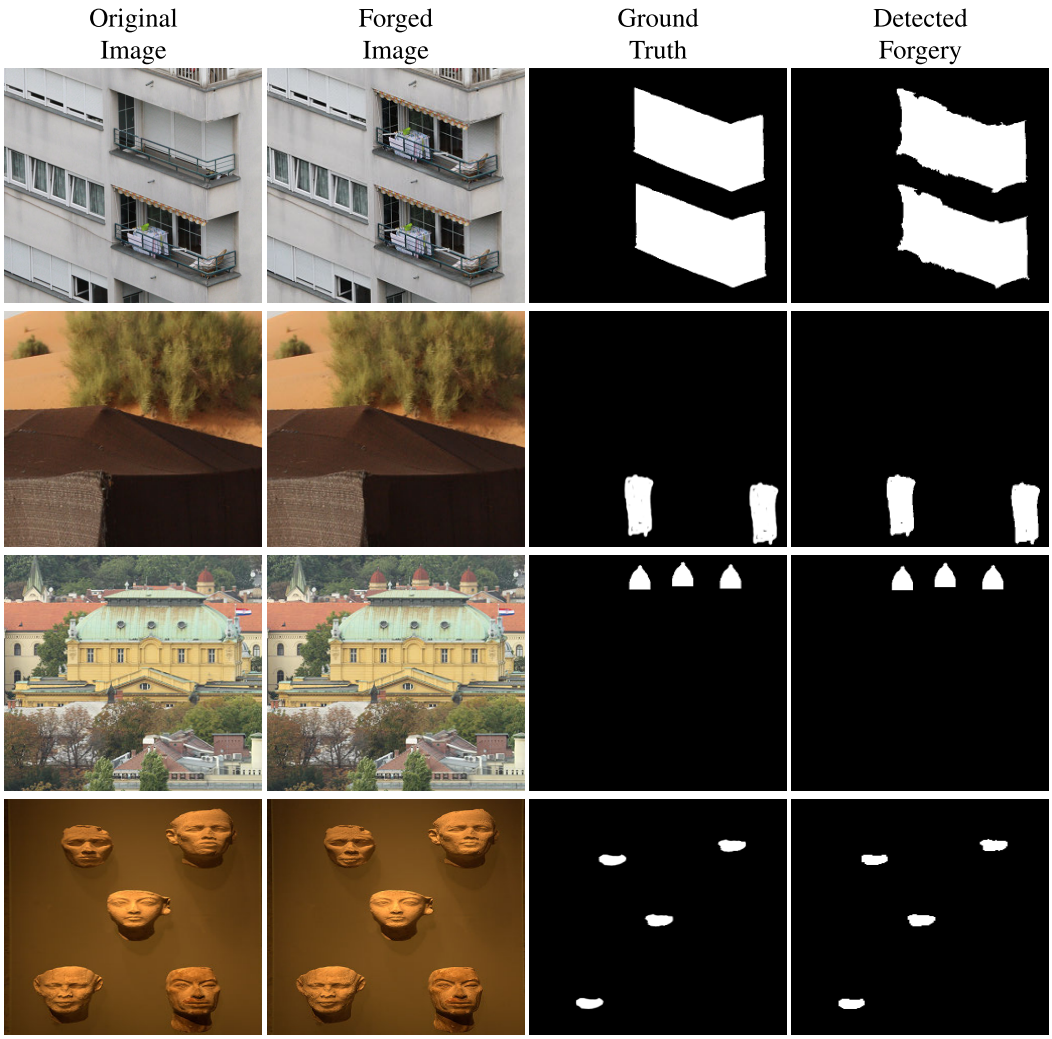

FIGURE 4. Single and Multiple Copy-move forgery detection results from all seven datasets.

transformation that has been applied to the copied region. This information can then be used to localize and detect the forgery.

Through our experiments and evaluation, we have shown that our method is capable of accurately detecting copy-move forgery in various types of images, including those that have undergone different types of forgery and transformations. Our evaluation metrics have demonstrated that our method achieves high precision, recall, and F-measure scores. These results indicate that our method is effective in detecting copy-move forgery and can be a valuable tool in forensic image analysis.

The Table (3) displays the number of images that were utilized for training and testing from each of the seven datasets: CMFD, CASIA V2.0, GRIP, COVERAGE, MICC-F600, MICC-F220, and CoMoFoD. To conduct the forgery detection, we evaluated the results separately for each category of forged images. A detailed analysis of the quantitative results for each category is further discussed in the following subsections.

A. DETECTION OF SIMPLE COPY-MOVE

We are addressing simple copy-move forgery on images of all the datasets. Experiments are carried out for two conditions

TABLE 4. Comparison of our results (F1-Score) with recently published works for simple copy-move forgery in images.

Dataset	Zhu [40]	Bi [41]	Li [42]	Diwan [43]	Proposed
CMFD	–	92.87	98.91	97.61	**98.53**
GRIP	–	92.98	100	95.12	**96.93**
MICC-F600	–	–	91.50	97.14	**97.26**
MICC-F220	–	–	99.10	98.43	**97.50**
CoMoFoD	–	–	–	98.43	**98.39**
COVERAGE	50.99	–	72.28	97.50	**98.03**
CASIA V2.0	45.52	–	–	95.36	**98.51**

of simple copy-move, i.e., single and multiple copy-move. Our proposed approach performed well in both situations. In Figure (4), we have included some of the detected forgeries for single and multiple copy-move cases. The proposed approach maintains accuracy through various images with different textures.

Table (4) presents the results obtained for simple copy-move forgery detection. The results demonstrate consistent performance across different datasets. Our proposed approach outperforms the traditional keypoint-based approach [41], [43] in the CMFD, CASIA V2.0, GRIP, CoMoFoD, MICC-F600, MICC-220, and COVERAGE datasets. However, in the GRIP dataset, the results are slightly lower. This can be attributed to the presence of extremely smooth images and images with intricate textures, such as monuments with similar carvings. In smooth images, the number of keypoints is insufficient for accurate detection and localization of forgery. Conversely, in highly textured images with self-similar structures, a large number of similar keypoints can lead to false localization of forged regions. It is important to consider these factors when analyzing the performance of the proposed approach in specific datasets.

Similarly, experiments were carried out for multiple copy-move forgery detection and localization. Results are shown in Figure (4). If we compare these results with the earlier keypoint-based approach, we readily can say that the SuperPoint based approach is more efficient.

B. DETECTION OF POST-PROCESSED COPY-MOVE

When a forgery is carried out skillfully, the manipulated image may undergo post-processing techniques to hide the forgery. Our study analyzed several post-processing methods such as JPEG compression, noise addition, brightness change (BC), color reduction (CR), contrast adjustment (CA), and image blurring (IB). Our proposed approach successfully detected and pinpointed the location of the forgery, even in images that had undergone post-processing. These operations are often utilized to mask copy-move forgery in digital images.

The SuperPoint detector is capable of extracting stable and robust keypoints from these post-processed images, even when the original features have been altered. By comparing the extracted keypoints from different areas of the image, the detector can identify possible copy-move forgery. Moreover, the SuperPoint descriptor can be employed to match the extracted keypoints and precisely determine the degree of geometric transformation applied to the copied region. This data can then be utilized to detect and localize the forgery accurately.

TABLE 5. The average result of copy-move forgery detection for images with various JPEG compression levels for CMFD and CoMoFoD datasets and its comparison with traditional keypoint-based CenSurE approach [43].

Attack Level	F1-Score Proposed CMFD	F1-Score Diwan [43] CMFD		F1-Score Proposed CoMoFoD	F1-Score Diwan [43] CoMoFoD
JPEG100	**98.53**	94.87		**98.39**	94.51
JPEG90	**97.65**	94.87		**97.75**	93.92
JPEG80	**97.00**	93.96		**97.01**	93.75
JPEG70	**96.28**	93.61		**96.89**	92.80
JPEG60	**96.19**	92.88		**95.99**	91.77
JPEG50	**95.95**	90.18		**95.18**	90.53
JPEG40	**95.03**	90.18		**94.83**	90.53
JPEG30	**94.30**	89.01		**93.72**	89.45
JPEG20	**94.13**	87.23		**93.14**	87.31
Noise20	**97.54**	91.90	Noise1	**97.52**	90.89
Noise40	**97.17**	91.90			
Noise60	**96.38**	91.90	Noise2	**96.48**	90.36
Noise80	**94.96**	91.01			
Noise100	**93.28**	90.88	Noise3	**95.76**	89.91

1) JPEG COMPRESSION

JPEG compression is a lossy compression technique that reduces the file size of an image by removing some of its details. This makes it difficult to detect forgery in such images. SuperPoint works by detecting and describing the distinctive features of an image, such as edges, corners, and blobs. These features are detected using a convolutional neural network, which learns to identify image patterns at different scales.

To detect JPEG compression using SuperPoint, we first extract keypoints and descriptors from the copied and moved image regions using the SuperPoint detector. We then match the keypoints between the two using a nearest-neighbor search algorithm.

In our experiment, we used images with different levels of JPEG compression, ranging from JPEG100 (least compressed) to JPEG20 (most compressed). As shown in Table (5), the results gradually deteriorated as the compression level increased. As expected, with higher compression, the F1-Score decreased, but we still achieved good results in all cases. It is known that with increasing compression, high-frequency information such as edges, corners, and gradients of the image gradually gets smoothed out. These high-frequency features are crucial for the keypoint detector, which relies on them to detect robust and stable keypoints.

When images are compressed using JPEG compression, visual degradation and blocking artifacts become noticeable when the compression level is below 50. These artifacts can affect the detection of forgery in images that have undergone

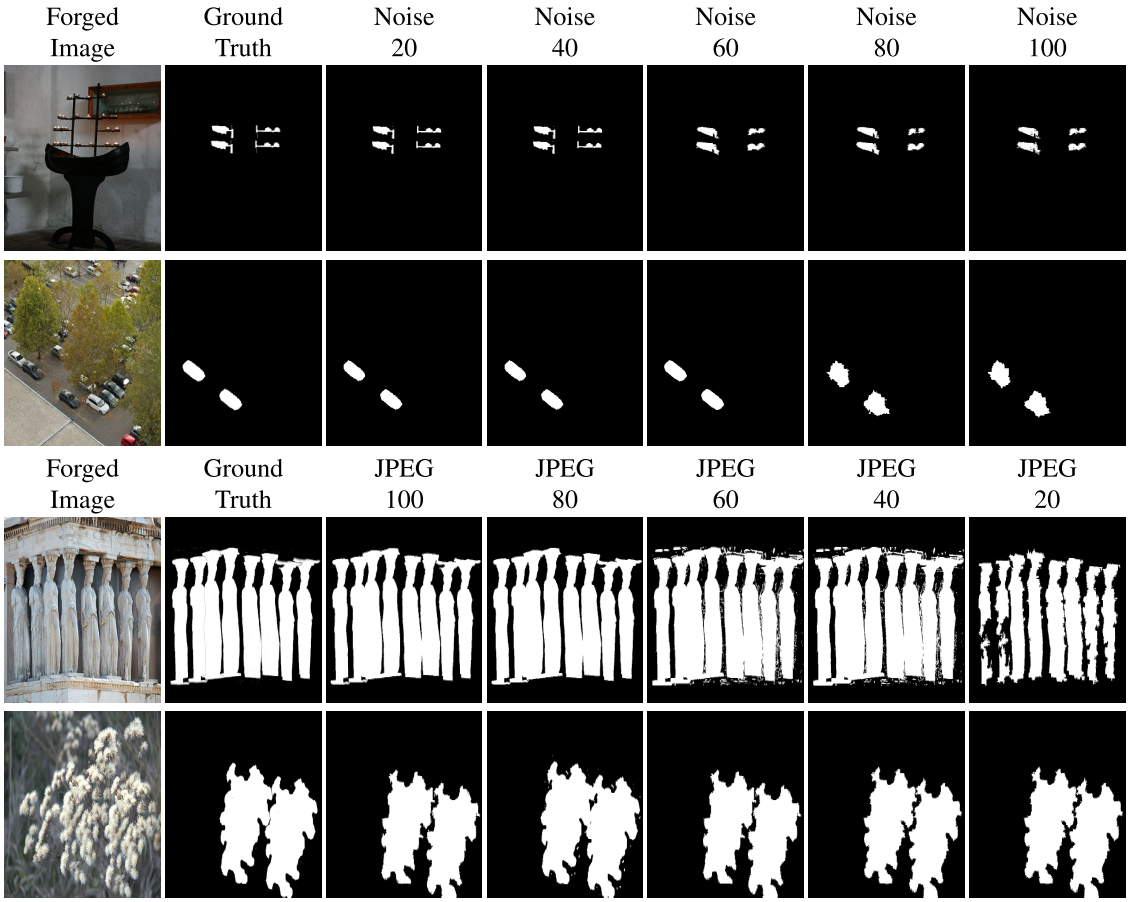

FIGURE 5. Copy-move forgery detection results for images with low to high JPEG compression and additive noise.

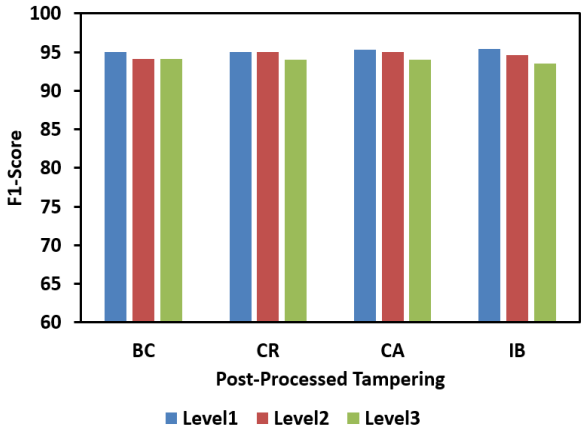

FIGURE 6. Copy-move forgery detection results for images with additional post-processing, e.g., Brightness change (BC), Colour reduction (CR), Contrast adjustment (CA), and Image blur (IB) for the CoMoFoD dataset.

higher levels of compression. The SuperPoint architecture is capable of reducing the impact of higher compression levels by detecting the low-level features of the image. However, the impact of compression artifacts is evident in the F1-Score and in the localization of the copy-move forged region.

2) ADDITIVE NOISE

Additive noise is another common post-processing technique used to hide image forgery. It involves adding random pixel values to an image to make it more difficult to detect. SuperPoint can be used to detect additive noise by comparing the detected keypoints and descriptors of an original and noisy image. To detect additive noise using SuperPoint, we first extract keypoints and descriptors from the copied and moved image regions using the SuperPoint detector. We then match the keypoints between the two regions of the image using a nearest-neighbor search algorithm.

The addition of noise to an image generates various edges and corners, and as the noise level increases, it can create a blur effect. These miscellaneous edges can have a negative impact on the detection of keypoints. However, the multi-level SuperPoint architecture can extract detailed image features, which can aid in better detection and localization of forgery. Hence, SuperPoint has resulted in a better F1-Score compared to the keypoint-based approach. The results for different levels of additive noise are shown in Table (5), where it can be observed that the F1-Score for images with higher levels of noise is degraded. This happens due to the presence of fewer keypoints in the image, which affects the localization of the forged region. Nonetheless,

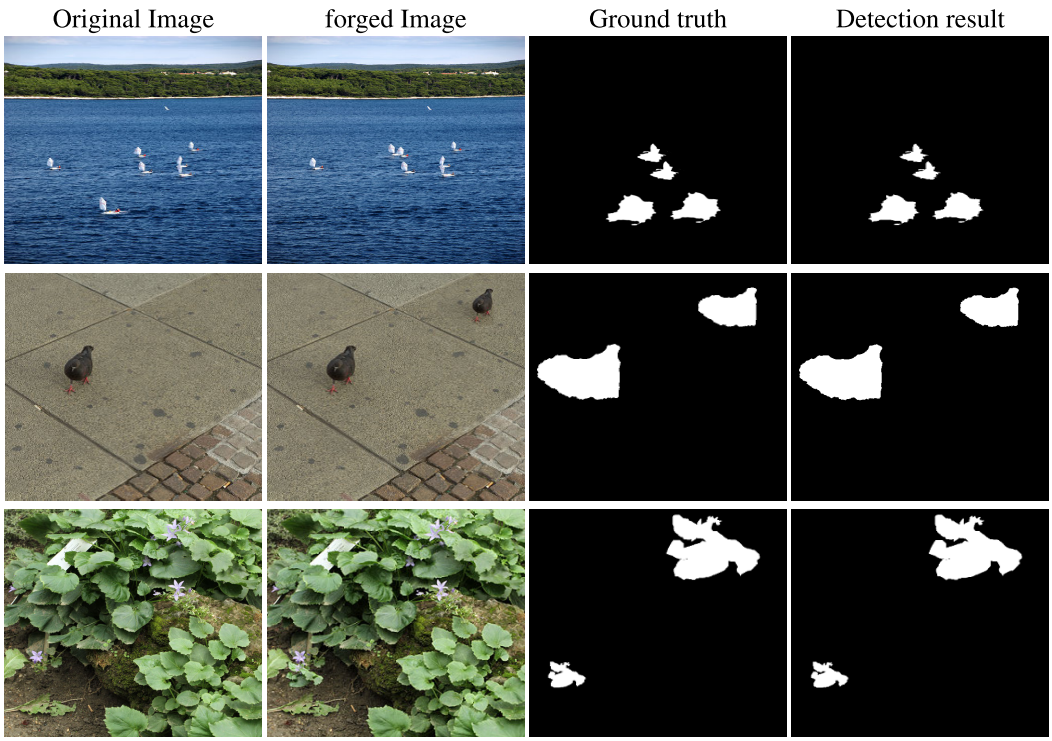

FIGURE 7. Copy-move forgery detection results for images with scaled transformation.

we were still able to detect the forged region in images with higher levels of noise.

In both JPEG compressed and noise images, SuperPoint is able to detect and localize the forgery by comparing the distinctive features of the original and manipulated images.

3) ADDITIONAL POST-PROCESSING

Copy-move forgery can be hidden by various post-processing operations, which make changes to the pixel level of the image and mask the traces of forgery. Such operations include colour reduction, contrast adjustment, brightness change, and image blurring. For instance, an increase in the brightness of the forged image reduces the contrast value and leads to more false negatives, resulting in decreased recall and overall detection accuracy (F1-Score). On the other hand, colour reduction reduces the intensity level in all colour channels, resulting in many colours being represented by the same value, which expands edges and affects detection accuracy.

Our proposed SuperPoint-based approach can effectively detect and locate forgery even in images that have undergone various post-processing operations. We have conducted experiments on additional post-processing approaches from the CoMoFoD dataset, and the results show that our approach can detect and localize forgery for different levels of post-processing operations consistently, from soft (level1) to harsh (level2). Results for additional post-processing are shown in Figure (6). The SuperPoint detector retains similarity in keypoints by clustering them, in addition to registering local image features effectively through SuperPoint features.

C. DETECTION OF GEOMETRICALLY TRANSFORMED COPY-MOVE

Detecting forgery in images becomes even more challenging when the copied region is subjected to geometric transformations before being moved to a new location. In such cases, the correspondence between the copied and moved regions becomes significantly altered, especially when the degree of rotation and scaling is large. Extracting similar features from regions that have undergone extensive geometric transformations is more difficult than in cases where the transformations are small.

1) GEOMETRICAL TRANSFORMED COPY-MOVE

Detecting copy-move forgery in geometrically transformed images is challenging because not all image features are invariant to rotation and scaling. To address this, we used the SuperPoint keypoint detector, which provides stable image keypoints that are robust to rotation and scaling. Homography adaptation in SuperPoint is useful for copy-move forgery detection in geometrically transformed images because it allows the detection and matching of keypoints even when the forged region has undergone a geometrical transformation (e.g., rotation, scaling, combination transformation).

When a forged region undergoes a homographic transformation, the keypoints in the original and forged regions will no longer match directly. However, by estimating the homography matrix between the two regions, the keypoints in the original region can be transformed to the coordinates in the forged region, where they can be matched to the

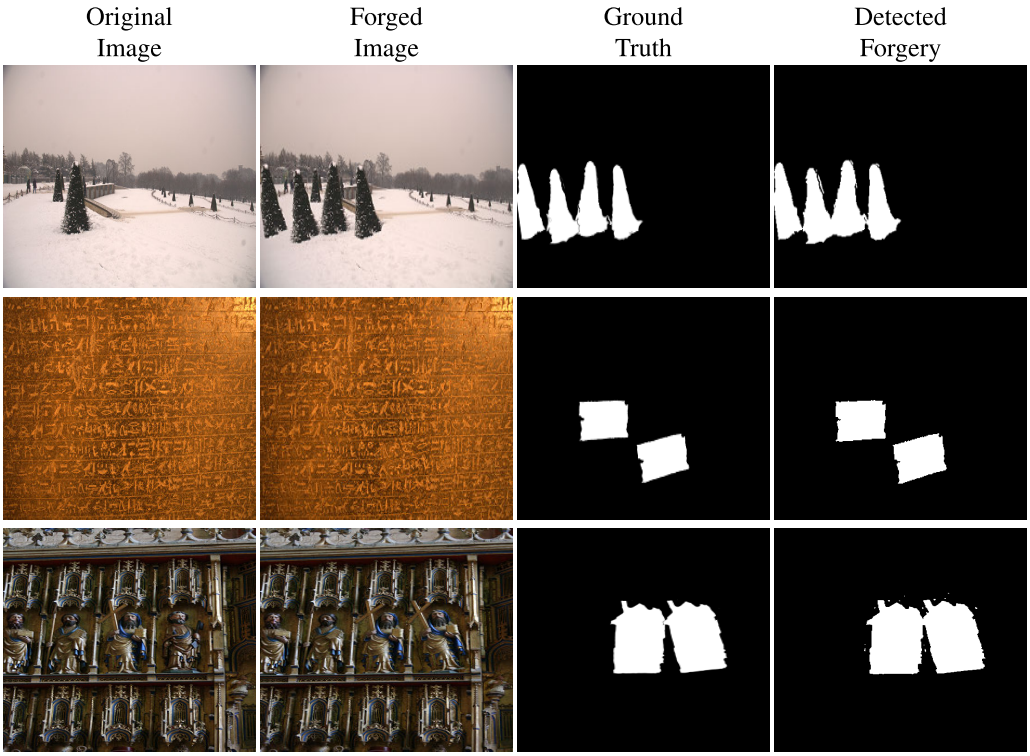

FIGURE 8. Copy-move forgery detection results for images with small rotation as a geometrical transformation.

keypoints detected in the forged region. This allows for the detection of copy-move forgery in images that have undergone homographic transformations.

The homography adaptation in SuperPoint involves estimating the homography matrix between the keypoints in the original and forged regions using the RANSAC algorithm. The homography matrix can then be used to transform the keypoints in the original region to the coordinates in the forged region, allowing for matching between the two regions.

The SuperPoint's repeatability is advantageous for detecting forgery in images with rotation. Its geometrical invariant property, coupled with transformation calculation, allows us to identify forgery even when the copy-move region undergoes a scale change from small to large or large to small. In our proposed approach, we leverage the benefits of SuperPoint by extracting features from the model, which helps maintain correspondence between copy-move images with small to large-angle rotations.

Diwan et al. [43] rely on affine transformation calculation for the detection of geometrically transformed copy-move. They are making an affine homographic matrix based on the copy-move region's coordinate information and calculated homographic matrix decomposition. The results shown in Table (6 and 7) clearly represent the superior performance of the proposed approach over results presented by the approach using additional affine transformation prediction.

In Table (6) we can particularly see the effectiveness in detecting forgery with large angle rotations, such as 20°, 40°, 60°, and 180°. Our results also demonstrate consistent performance for small degrees of rotation, including 2°, 4°, 6°, 8°, and 10°. Figure (8) showcases some examples of images with different rotation angles.

In Table (7) we can see the effectiveness of our proposed approach over the approach presented in [43]. Results demonstrate that for a small level of scale change

TABLE 6. The average result of copy-move forgery detection for images with various levels of angle rotation and its comparison with traditional keypoint-based CenSurE approach [43].

Angle Rotation	F1-Score Proposed CMFD	F1-Score CenSurE CMFD	Angle Rotation	F1-Score Proposed CMFD	F1-Score CenSurE CMFD
2	**97.53**	94.91	20	**92.88**	89.88
4	**97.06**	94.05	40	**91.81**	87.65
6	**96.66**	94.99	60	**91.10**	87.65
8	**94.92**	93.90	180	**90.81**	84.88
10	**94.53**	93.88	–	–	–

TABLE 7. The average result of copy-move forgery detection for images with various levels of scale factor and its comparison with traditional keypoint-based CenSurE approach [43].

Sacle Factor	F1-Score Proposed	F1-Score CenSurE
2	**97.92**	93.49
4	**96.88**	93.95
6	**95.98**	92.46
8	**94.52**	92.01
10	**93.48**	92.88

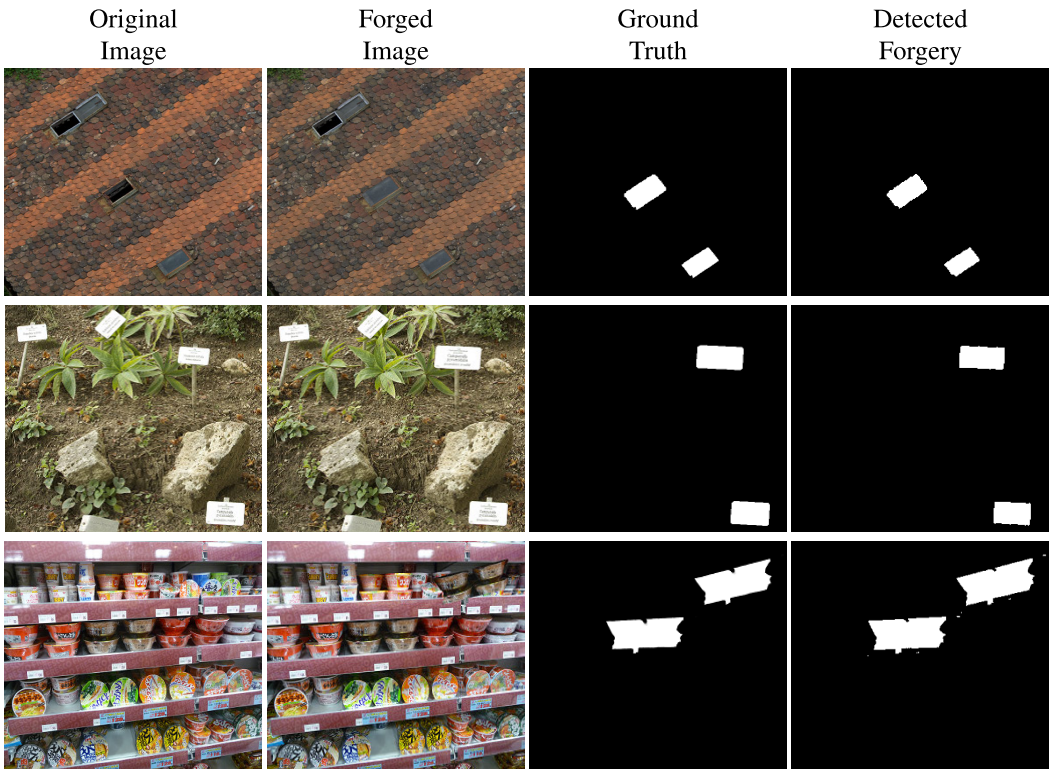

FIGURE 9. Copy-move forgery detection results for images combined geometrical transformation.

like 2, 4, and 6 the difference in result is significant. Figure (9) showcases some examples of images demonstrating this combination of rotation and scaling.

VIII. CONCLUSION

In conclusion, our research paper presents an end-to-end trainable copy-move forgery detection approach that leverages the SuperPoint architecture. Our method demonstrates superior performance in detecting and localizing copy-move forgery in digital images. The algorithm effectively handles various types of forgery, including simple and multiple copy-move, post-processed copy-move, and geometrically transformed copy-move.

The experiments conducted on multiple datasets validate the robustness and versatility of our approach. It outperforms existing methods in terms of detection accuracy and stability across different types of forged images. The algorithm's efficiency in processing time makes it suitable for real-time forgery detection applications.

However, there are still some limitations to address. The computational complexity of the SuperPoint-based approach may pose challenges for large-scale applications or real-time processing. Future research can focus on optimizing the algorithm to reduce computational requirements and improve scalability.

Furthermore, the combination of geometrical transformations with post-processing operations remains a significant challenge in forgery detection. Addressing this complex scenario would enhance the overall effectiveness of forgery detection methods. Future directions could involve exploring advanced feature extraction techniques, improving clustering and matching algorithms, and incorporating machine learning approaches to handle the intricacies of combined attacks.

Our research paper contributes a powerful SuperPoint-based approach for copy-move forgery detection. It offers a comprehensive and reliable solution for detecting a wide range of copy-move forgery in digital images. With further optimizations and advancements, our approach holds great potential for practical applications in image forensics and security domains.

REFERENCES

[1] M. Emam, Q. Han, L. Yu, Y. Zhang, and X. Niu, "A passive technique for detecting copy–move forgery with rotation based on polar complex exponential transform," *Proc. SPIE*, vol. 9631, pp. 16–21, Jul. 2015.

[2] A. Diwan, A. K. Roy, and S. K. Mitra, "Locality preserving projection based multiple copy-paste forgery detection," in *Proc. IEEE Appl. Signal Process. Conf. (ASPCON)*, Oct. 2020, pp. 158–162.

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

[4] X.-Y. Wang, Y.-N. Liu, H. Xu, P. Wang, and H.-Y. Yang, "Robust copy–move forgery detection using quaternion exponent moments," *Pattern Anal. Appl.*, vol. 21, no. 2, pp. 451–467, May 2018.

[5] X. Bi and C.-M. Pun, "Fast reflective offset-guided searching method for copy–move forgery detection," *Inf. Sci.*, vols. 418–419, pp. 531–545, Dec. 2017.

[6] V. Thirunavukkarasu, J. Satheesh Kumar, G. S. Chae, and J. Kishorkumar, "Non-intrusive forensic detection method using DSWT with reduced feature set for copy–move image tampering," *Wireless Pers. Commun.*, vol. 98, no. 4, pp. 3039–3057, Feb. 2018.

[7] B. Chen, M. Yu, Q. Su, H. J. Shim, and Y.-Q. Shi, "Fractional quaternion Zernike moments for robust color image copy–move forgery detection," *IEEE Access*, vol. 6, pp. 56637–56646, 2018.
[8] Y. Wo, K. Yang, G. Han, H. Chen, and W. Wu, "Copy–move forgery detection based on multi-radius PCET," *IET Image Process.*, vol. 11, no. 2, pp. 99–108, Feb. 2017.
[9] M. Emam, Q. Han, L. Yu, and H. Zhang, "A keypoint-based region duplication forgery detection algorithm," *IEICE Trans. Inf. Syst.*, vol. 99, no. 9, pp. 2413–2416, 2016.
[10] M. Emam, Q. Han, and H. Zhang, "Two-stage keypoint detection scheme for region duplication forgery detection in digital images," *J. Forensic Sci.*, vol. 63, no. 1, pp. 102–111, Jan. 2018.
[11] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Salleh, and F. Othman, "SIFT-symmetry: A robust detection method for copy–move forgery with reflection attack," *J. Vis. Commun. Image Represent.*, vol. 46, pp. 219–232, Jul. 2017.
[12] B. Chen, M. Yu, Q. Su, and L. Li, "Fractional quaternion cosine transform and its application in color image copy–move forgery detection," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8057–8073, Apr. 2019.
[13] K. Liu, W. Lu, C. Lin, X. Huang, X. Liu, Y. Yeung, and Y. Xue, "Copy move forgery detection based on keypoint and patch match," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31387–31413, Nov. 2019.
[14] B. Elhaminia, A. Harati, and A. Taherinia, "A probabilistic framework for copy–move forgery detection based on Markov random field," *Multimedia Tools Appl.*, vol. 10, pp. 1–19, Jan. 2019.
[15] M. Emam, Q. Han, and H. Zhang, "Detection of copy-scale-move forgery in digital images using SFOP and MROGH," in *Proc. Int. Conf. Pioneering Comput. Scientists, Eng. Educators*. Cham, Switzerland: Springer, 2016, pp. 326–334.
[16] M. Emam, Q. Han, Q. Li, H. Zhang, and M. Emam, "A robust detection algorithm for image copy–move forgery in smooth regions," in *Proc. Int. Conf. Circuits, Syst. Simul. (ICCSS)*, Jul. 2017, pp. 119–123.
[17] K. B. Meena and V. Tyagi, "A copy–move image forgery detection technique based on tetrolet transform," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102481.
[18] C. Wang, Z. Zhang, Q. Li, and X. Zhou, "An image copy–move forgery detection method based on SURF and PCET," *IEEE Access*, vol. 7, pp. 170032–170047, 2019.
[19] E. A. A. Vega, E. G. Fernández, A. L. S. Orozco, and L. J. G. Villalba, "Passive image forgery detection based on the demosaicing algorithm and JPEG compression," *IEEE Access*, vol. 8, pp. 11815–11823, 2020.
[20] S. Singhal and V. Ranga, "Passive authentication image forgery detection using multilayer CNN," in *Mobile Radio Communications and 5G Networks*, N. Marriwala, C. C. Tripathi, D. Kumar, and S. Jain, Eds. Singapore: Springer, 2021, pp. 237–249.
[21] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill, and B. Lee, "Lightweight deep learning model for detection of copy–move image forgery with post-processed attacks," in *Proc. IEEE 19th World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Jan. 2021, pp. 000125–000130.
[22] H.-T. Wang and P.-C. Su, "Deep-learning-based block similarity evaluation for image forensics," in *Proc. IEEE Int. Conf. Consum. Electron.*, Sep. 2020, pp. 1–2.
[23] H. H. Nguyen, J. Yamagishi, and I. Echizen, "Capsule-forensics: Using capsule networks to detect forged images and videos," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2307–2311.
[24] K. H. Rhee, "Composition of visual feature vector pattern for deep learning in image forensics," *IEEE Access*, vol. 8, pp. 188970–188980, 2020.
[25] L. Yu, Y. Zhang, H. Han, L. Zhang, and F. Wu, "Robust median filtering forensics by CNN-based multiple residuals learning," *IEEE Access*, vol. 7, pp. 120594–120602, 2019.
[26] J.-L. Zhong and C.-M. Pun, "An end-to-end dense-InceptionNet for image copy–move forgery detection," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2134–2146, 2020.
[27] D. DeTone, T. Malisiewicz, and A. Rabinovich, "SuperPoint: Self-supervised interest point detection and description," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2018, pp. 224–236.
[28] A. Diwan, P. A. Koringa, A. K. Roy, and S. K. Mitra, "Neighbourhood projection embedding based image tampering detection and localization," in *Computer Vision, Pattern Recognition, Image Processing, and Graphics*, R. V. Babu, M. Prasanna, and V. P. Namboodiri, Eds. Singapore: Springer, 2020, pp. 387–396.
[29] K. M. Hosny, H. M. Hamza, and N. A. Lashin, "Copy–move forgery detection of duplicated objects using accurate PCET moments and morphological operators," *Imag. Sci. J.*, vol. 66, no. 6, pp. 330–345, Aug. 2018.
[30] Y. Liu, H.-X. Wang, H.-Z. Wu, and Y. Chen, "An efficient copy–move detection algorithm based on superpixel segmentation and Harris keypoints," in *Proc. Int. Conf. Cloud Comput. Secur.* Cham, Switzerland: Springer, 2017, pp. 61–73.
[31] G. Nair, K. Venkatesh, D. Sen, and R. Sonkusare, "Identification of multiple copy–move attacks in digital images using FFT and CNN," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–6.
[32] G. Nirmala and K. K. Thyagharajan, "A modern approach for image forgery detection using BRICH clustering based on normalised mean and standard deviation," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2019, pp. 441–444.
[33] A. Diwan, V. Mall, A. Roy, and S. Mitra, "Detection and localization of copy–move tampering using features of locality preserving projection," in *Proc. 5th Int. Conf. Image Inf. Process. (ICIIP)*, Nov. 2019, pp. 397–402.
[34] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy–move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
[35] D. Cozzolino, G. Poggi, and L. Verdoliva, "Copy–move forgery detection based on PatchMatch," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5312–5316.
[36] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—New database for copy–move forgery detection," in *Proc. ELMAR-*, Sep. 2013, pp. 49–54.
[37] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[38] B. Wen, Y. Zhu, R. Subramanian, T.-T. Ng, X. Shen, and S. Winkler, "COVERAGE—A novel database for copy–move forgery detection," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2016, pp. 161–165.
[39] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, Jul. 2013, pp. 422–426.
[40] Y. Zhu, C. Chen, G. Yan, Y. Guo, and Y. Dong, "AR-Net: Adaptive attention and residual refinement network for copy–move forgery detection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6714–6723, Oct. 2020.
[41] X. Bi and C.-M. Pun, "Fast copy–move forgery detection using local bidirectional coherency error refinement," *Pattern Recognit.*, vol. 81, pp. 161–175, Sep. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320318301183
[42] Y. Li and J. Zhou, "Fast and effective image copy–move forgery detection via hierarchical feature point matching," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1307–1322, May 2019.
[43] A. Diwan, R. Sharma, A. Roy, and S. Mitra, "Keypoint based comprehensive copy–move forgery detection," *IET Image Process.*, vol. 15, pp. 1298–1309, May 2021, doi: 10.1049/IPR2.12105.

ANJALI DIWAN (Senior Member, IEEE) received the Ph.D. degree from the Dhirubhai Ambani Institute of Information and Communication Technology (DAIICT), Gandhinagar, Gujarat. She is a highly experienced academic and software industry professional with more than 19 years of expertise. She is currently a Faculty Member with the CE-AI/Big Data Department, Marwadi University, Rajkot, Gujarat, India. Her research interests include machine learning, image processing, artificial intelligence, deep learning, data security, multimedia forensics, and the application of technologies to address humanitarian challenges. She serves as a member of the SAC Team of IEEE R10, from 2023 to 2024. She serves as the Section Chair for the IEEE Young Professionals Affinity Group of Gujarat Section, from 2022 to 2024.

DINESH KUMAR (Senior Member, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology Kanpur, in 2002, and the Ph.D. degree in information science and technology (in the research domain of biomedical signal processing and machine learning) from the University of Coimbra, Portugal, in 2015. He holds a faculty position with Marwadi University, Rajkot, in computer engineering artificial intelligence. His research interests include signal processing and control, image processing, nonlinear dynamics, soft computing, and machine learning.

RAJESH MAHADEVA (Member, IEEE) received the B.E. degree in electronics and instrumentation engineering from the Samrat Ashok Technological Institute (SATI), Vidisha, Madhya Pradesh, India, in 2006, the M.Tech. degree in control and instrumentation engineering from the Dr. B R Ambedkar National Institute of Technology (NIT), Jalandhar, Punjab, India, in 2009, and the Ph.D. degree from the Department of Polymer and Process Engineering, Indian Institute of Technology (IIT) Roorkee, Uttarakhand, India, in 2022. From 2011 to 2017, he was an Assistant Professor with the Technocrats Institute of Technology (TIT), Bhopal, and Marwadi University (MU), Rajkot, India. He is currently a Research Scientist with the Department of Physics, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates. His research interests include modeling, simulation, optimization, and the control of desalination and water treatment plants/processes using artificial intelligence techniques.

H. C. S. PERERA received the B.Sc. degree in physics from the University of Peradeniya, Sri Lanka, in 2012, and the Ph.D. degree from the Queensland University of Technology, Australia, in 2016. She is currently a Senior Lecturer with the Department of Physics, University of Peradeniya. She collaborates with Dr. Das at Khalifa University, United Arab Emirates, and also visiting Khalifa University, as a Researcher Faculty. Her research interest includes water treatment using natural resources.

JANAKA ALAWATUGODA received the B.Sc. degree (Hons.) in computer science from the University of Peradeniya, Sri Lanka, and the Ph.D. degree from the Queensland University of Technology, Australia. He is currently an Associate Researcher and an Assistant Professor with the Rabdan Academy, United Arab Emirates. He is an Adjunct Research Fellow with the Institute for Integrated and Intelligent Systems, Griffith University, Australia, and a Visiting Lecturer with the Postgraduate Institute of Science, University of Peradeniya. He is a fellow of the British Computer Society, a Professional Member of the Association for Computing Machinery, and a member of the International Association for Cryptologic Research. He is a Reviewer of *zbMATH Open* database at FIZ Karlsruhe, Germany.