Received: 19 October 2023 | *Revised:* 17 November 2023 | *Accepted:* 20 January 2024
DOI: 10.37917/ijeee.20.2.0 *Early View* | *December 2024*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access
IJEEE University of Basrah College of Engineering

An Image Copy-Move Forgery Detection Based on Integrated Descriptor Features and Clustering Techniques

Khawla Hussein Ali * [1],Wijdan Yaseen A. AlKarem [1]
[1]Computer Science Dept, College of Pure Science, University of Basrah, Basrah, Iraq

Correspondance
*Khawla Hussein Ali
Computer Science Dept, College of Pure Science,
University of Basrah, Basrah, Iraq
Corresponding address
Email: Khawla.ali@uobasrah.edu.iq

Abstract
One common form of simple manipulation is image copy-move forgery. To overcome issues like the high temporal complexity of conventional copy-move forgery detection approaches and the challenge of identifying forgeries in areas with clean edges, this study presents an algorithm for copy-move image forgery identification and detection that integrates features with clustering. The algorithm first extracts descriptive features by decreasing the contrast threshold by using two detection techniques: Harries Corner and Speeded-up Robust Features (SURF). Then, mismatched matches are filtered out and false positives are minimized using the HDBSCAN clustering approach. To increase The precision of the forgery location, the algorithm evaluates similarities in the same position between the original image and the image modified by the affine matrix. Three test datasets (MICC-F220, IMD, and CoMoFoD datasets) were utilized to evaluate the suggested technique. The results promised high accuracy in the detection of image copy-move forgery.

Keywords
Affine matrix Transformation, Copy-Move, HDBSCAN clustering, Harris Corner, Similar of the location, SURF descriptor.

I. Introduction

addition to using cameras or mobile devices to take their high-resolution images and films, users can see high-resolution images and movies online.

Programs for picture modifying and tempering, such as Adobe, also help people to alter and edit photos more rapidly and simply.

Lightroom and Photoshop. On the other hand, these state-of-the-art techniques for processing software simplify life and increase the potential for criminal activity. Widespread image manipulation and tampering have caused sincere problems for news reporting, creation, digital forensic analysis, and social media [1, 2]. The accuracy and uniformity of digital photos The authenticity and dependability of digital images are especially important in areas like medical registers, journal scientific publications, celebrity publications, news articles, political actions, and court assessments, which are being called into doubt. One of the most popular forms of tampering at the moment is image copy-move forgery [3]. To emphasize particular visual information or hide certain picture content, the approach includes pasting and copying a certain region of one image onto other areas of the identical image. An illustration of image copy-move forgery is shown in Fig. 1 [4]. The tampered area in picture copy-move forgery might not be the same as the source area since post-processing procedures including scaling, rotation, blurring, edge softening, JPEG compression, and noise addition, are frequently applied to it. Consequently, it is simple for the visual human to be tricked

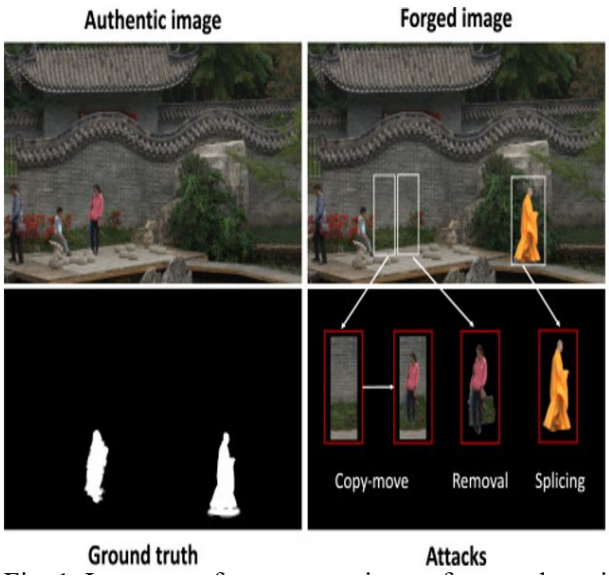

Fig. 1. Instances of copy-move image forgery detection in the dataset. The left part: is original (authentic) images; the Right part: is forged images and attacks.

by tampered images, leading to misunderstanding [5]. The detection of image copy-move forgeries has been thoroughly studied by several academics. To detect copy-move fraud, there are currently two primary types of techniques: either breaking the image up into picture blocks or extracting feature pixels [6]. It was discovered that because block characteristics are extremely sensitive to geometric transformation assaults, the block-based technique, which necessitates matching a lot of crossing over blocks, is ineffective.

changes about rotation and scale, which eventually need a lot of processing power. Feature pixel-based approaches are widely used in the detection of copy-move forgeries because they are very reliable due to their insensitivity to scaling and rotation. Several scholars have conducted extensive research on the identification of image copy-move frauds. There are currently two main methods for detecting copy-move fraud: either extracting feature points or dividing the image into image blocks [7]. It was found that block attributes are highly delicate to rotation and scale changes, which eventually results in significant computational costs, making geometric transformation assaults ineffective for the block-based approach. Feature point-based approaches are widely used in image copy-move forgery detection because they are not affected by scaling or rotation.

This research proposes a forgery detection approach based on two detection methodologies, Harris's corner and speeded-up robust features (SURF), to minimize the computing expense and excerpt more features in smooth areas and rounded places. Because it is unaffected by rotation or scaling and has a lower-dimensional feature description, the SURF detector moves faster. Conversely, smooth regions can gain from the capacity of clustering to extract a high number of significant feature points, hence improving the region's accuracy in detecting forgeries. After matching the features of the two detectors using K-NN (k=2), we utilized the K-means clustering technique to identify areas that had been tampered with and to remove mismatched pairs.

This program assesses the degree of similarity between the original and affine matrix-modified images. The results of the experiment demonstrate the effectiveness of the recommended approach. The principal inputs consist of:

• Development of an image copy-move forgery detection method that combines feature extraction methods, and leverages density clustering to reduce false positives.

• Increases the precision of the localization of forgeries. It also exhibits resilience to a range of post-processing techniques, including noise addition, rotation, scaling, and geometric transformations.

• Improved performance in detecting forgeries in smooth image regions

II. Related Works

The detection of Copy-Move Forgeries (CMFD) techniques is currently available in feature point-based and image block-based. Using the image blocks approach, the image is generally split into interfering blocks, either round or rectangular, from which feature points are obtained.

Following feature extraction, feature similarity is carried out. The block-based technique of this methodology was first proposed by Fridrich et al. [7] and employs CMFD with Discrete Cosine Transform (DCT). Several features were proposed to describe these blocks. For instance, Kumar et al. [8] suggested a method for image CMFD based on Principal Component Analysis (PCA). Using the Haar transform to extract image features, this technique then uses PCA to minimize the computational cost of the data before identifying, locating, and removing spurious boundaries. The textural characteristics of the enter image are also evaluated using the gray-level co-occurrence matrix (GLCM). With block segmentation based solely on the estimated DWT coefficients, Fattah et al.'s [9] two-dimensional discrete wavelet transform (DWT) was applied to manipulated images. Matching was done by computing features that are matched after the data has been extracted. CMFD with discrete cosine transform (DCT) is used in this algorithm, which was first proposed by Fridrich et al. [7].

Certain features were put forth to explain these blocks. The gray-level co-occurrence matrix (GLCM) is also used to assess the texture aspects of the input image. When Fattah et al. [9] used tampered photos, they used a two-dimensional discrete wavelet transform (DWT), only taking into account the roughly DWT coefficients for matching and segmentation of the block, which was done by computing Feature matching was then done after the data had been extracted. An approach using CMFD and discrete cosine transform (DCT) was first proposed by Fridrich et al. [7] in a block-based method.

For these blocks, several features were suggested. Using principal component analysis (PCA) as an example, Kumar et al. [8] suggested a method for image CMFD. Using the Haar transform to extract image features, this technique subsequently reduces computing complexity by simplifying the features through PCA. Finally, erroneous boundaries are found and eliminated. Utilizing the gray-level co-occurrence matrix (GLCM), the texture elements of the input image are also examined. Only the approximate DWT coefficients were taken into account for block segmentation when A two-dimensional discrete wavelet transform (DWT) was used by Fattah et al. [9] to manipulate pictures, and matching was accomplished by computing When Fattah et al. [[9] segmented blocks from manipulated images using a two-dimensional discrete wavelet transform (DWT), they only took into account approximations of the DWT coefficients. Matching was then done by calculating the distance between adjacent blocks. The findings demonstrated that the system was ineffective at detecting forgeries when subjected to geometric transformation attacks. Euclidean distance was used to compare the features, and non-similarity feature points were found [10].

Sabeena et al. [11] addressed a strategy for image CMFD that takes Harlick features and Local Binary Patterns (LBP) for feature identification and extraction. To authenticate the verification of the image, different classifiers for supervised machine learning were used, such as gradient boosting, random forests, and support vector machines (SVMs). The accuracy of forgery detection based on these classifiers was investigated. The problem of processing operations like scaling and rotation in the tampered region has been resolved through the application of various local invariant characteristics, including Zernike moments, Hu moments, and others, in the study of CMFD forensics [11–13].

Lee et al. took statistical attributes created with a Histogram of Gradients (HOG) for CMFD [14, 15]. The findings demonstrate the need for method improvements to identify forgeries when large chunks are scaled and rotated. mental image. In this study, center of symmetric local binary patterns are addressed as image feature descriptors. Changes in grayscale do not affect the amount of computation required for this approach. Wang et al. suggested a CMFD method Utilizing the principles of the Polar Complex Exponential Transform (PCET).

Initially divided into overlapping circular sections in this method, the geometric invariant properties of each block are then extracted using PCET. However, the way the image is divided into circular blocks may cause some loss of visual data, which could impact the system's ability to recognize objects. Because block-based methods are computationally expensive and have limitations in detecting scale displacement tampering, researchers are turning more and more to feature point-based methods for image CMFD to address these problems. These methods construct and match feature vectors for each point, extract feature points from the high-entropy areas of the image, and finally detect tampered areas. These algorithms perform best when used for pixel extraction, pixel description, pixel matching, and positioning approaches [16–21]. An early feature point-based CMFD technique was presented by Pun et al. [22, 23] to make copy-move detection algorithms more sensitive to modifications such as rotation and It performs affine modifications [24] to remove mismatched pairings using the random sample consensus (RANSAC) technique [25].

This method's temporal complexity is rather high, even though it can only identify a single kind of tampering operation. Following these discoveries, researchers looked into several tampering strategies. On pixel-level datasets, this algorithm's location accuracy is still only mediocre. Currently, feature-point-based methods have trouble detecting modifications in parts that are smooth or little. To solve this issue, Liu et al. [26] addressed an identification strategy using K-means clustering. Using SIFT and sector mask characteristics, this technique may identify each site where tampering has happened by segmenting the image into smooth and complicated portions. Nonetheless, there is a need to improve the precision of this approach. Those based on feature points have many advantages over those based on blocks [24, 25, 27]. The feature point, To extract the most representative key points from the target region, for example, the feature point can be utilized. This approach enables more precise target region identification and positioning. Most feature point extraction methods are strong enough to withstand scaling and rotation post-processing [28]. Feature point extraction and matching usually take less time than block-matching algorithms, It results in a reduction of the computational complexity. Nevertheless, feature point-based approaches continue to have several problems.

For example, matching becomes slower, and detecting tampering in smooth areas becomes more difficult when the extracted key points are dense [29, 30].

III. SURF Descriptors and Harris Corner

The feature descriptors SURF and Harris Corner are primarily summarized in this section [29].

A. SURF Descriptors

$$H(x,y) = \begin{bmatrix} C_{xx}(x,\sigma) & C_{xy}(x,\sigma) \\ C_{xy}(x,\sigma) & C_{yy}(x,\sigma) \end{bmatrix} \quad (1)$$

Currently, the SIFT and SURF descriptors make up the majority of image CMFD techniques obtained on feature points. The SURF technique solves the drawbacks of SIFT regarding excessively large feature dimensions and lengthy complexity time [31] by using the Hessian matrix for quick calculations. The SURF algorithm turns the convolution smoothing operations, addition and subtraction operations, the modifies the Gaussian encoder differential template in the Hessian matrix, the SURF algorithm outperforms the SIFT technique in terms of robustness and time complexity. SURF offers excellent resistance to alters in illumination and affine warping, but it is unable to preserve the SIFT's rotation and scale invariance. By calculating the scale space's extreme points, SURF may calculate the important points [31].

In the formula, $x = (x,y)$ C_{xy}, (x,σ) is the convolution of the second-order partial derivative $\frac{\partial G(x,y,\sigma)}{\partial x^2}$ of the Gaussian function and the image at the pixel point. The matrix's determinant $H(x,\sigma)$ is expressed as:

$$\det(H) = C_{xx}(x,\sigma) + C_{yy}(x,\sigma) - [C_{xy}(x,\sigma)]^2 \quad (2)$$

Because it takes a lot of processing power to calculate partial derivatives as second-order images, SURF utilizes filters of the box that is rectangular to calculate the second-order partial derivatives of Gaussian functions in approximation. The box filter consists of a basic template as a rectangle, that reduces time complexity and speeds up convolution processing. Applying the filter as a rectangular box to the image yields $C_{xx}(x,\sigma)$, $C_{xy}(x,\sigma)$, and $C_{yy}(x,\sigma)$. From there, one may calculate the Hessian matrix determinant for each coordinate pixel to assess the Hessian determinant matrix. A pyramid image and multiple Hessian determinant images are produced as a result of scale variations, which are made feasible by altering the scale of the Gaussian function and the dimensions of the filter, which is a rectangular box.

The point is identified as a key point if its value exceeds that of its 26 neighbors and the predetermined threshold TS (subscript S implies SURF). The response of a 6-radius circular region centered on the key point determines the guidance of SURF feature points. By applying the focal point as the main and looking through a sector area with a $\sqrt{3}$ angle within the circular area, the sum of the vertical and horizontal Harr feature points of whole points and the sum of the vertical and horizontal Harr feature points area are found. The vector direction that is the longest is chosen as the main guidance of the key point. Once the guidance of the critical point has been determined, a SURF description is created. The neighborhood is deliberately selected, and the major axis of the significant notion is aligned with a square space measuring 20 centimeters on each side. Four-by-four subregions make up the square region, as are four-dimensional properties like the Harr wavelet's horizontal and vertical responses in directions $\sum dx$ and $\sum dy$ are computed for each of the five grids, together with the absolute values of the responses in the directions $\sum |dx|$ and $\sum |dy|$. Lastly, a 64-dimensional feature vector descriptor is produced by splitting each sub-region into 16 sub-regions and adding the 4-dimensional attributes of each sub-region collectively [32–34].

B. Harris Corner Detection

Computer vision algorithms frequently use the Harris corner detector to extract corners and infer features from an image. Harris' corner detector is more accurate at differentiating between edges and corners than its predecessor because it directly considers the difference of the corner score with relation to direction rather than moving patches for every 45-degree angle [3]. Then, it has undergone improvements and has been included in a variety of algorithms to preprocess images for use in later processes. If the image considered by I and shifting it by the sum of squared differences (SSD) between two patches is given below:

$$f(\Delta x, \Delta y) = \sum (I(x_k, y_k) - I(x_k + \Delta x, y_k) + \nabla y)^2 \quad (3)$$

$$M = \sum \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix} \begin{bmatrix} \sum I_x^2 & \sum I_x I_y \\ \sum I_x I_y & \sum I_y^2 \end{bmatrix} \quad (4)$$

Set a specified threshold on the value that finds pixels with responses above this threshold. Finally, compute the non-max suppression to pick up the optimal corners.

IV. The Proposed Method

The main process of the strategy suggested in this paper is shown in Fig. 2. First, two detection techniques—Harris Corner and SURF—are used to extract feature points from the input image. We decreased the contrast threshold and combined the two detection methods to extract feature points to solve the issue of insufficient feature point extraction in smooth regions. Next, utilizing feature matching with K-NN (K=2), comparable feature vectors are discovered. To make the tampering

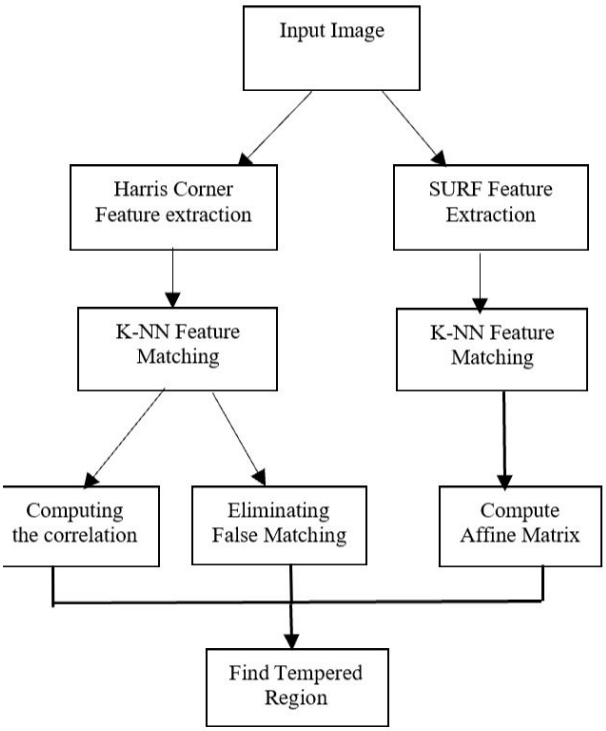

Fig. 2. Flow chart of proposed method

localization more precise, The k-means clustering technique was employed to eliminate false positives. Using an affine transformation, the degree of similarity between the original and altered images is finally used to determine the tampered area.

A. SURF and Harris Corner Features

We integrated two detection techniques, SURF and Harris Corner, to address the problems of challenging identification and high computing costs that arise in smooth areas with tampering at the present level. When using SURF to extract feature points from the image, the value of the threshold for contrast is set to Cs, and stores the extracted feature points in matrix $X_s = \{x_1, x_2, \ldots, x_n\}$, it represents $x_s^i = (x_x^i, y_s^i)$. When extracting feature points from Harris corner, the contrast threshold is set to CH, then stored in matrix $X_H = \{x_1, x_2, \ldots, x_m\}$. The coordinates of the i_{th} feature points are defined as $x_H^i = (x_x^i, y_H^i)$. Then the SURF feature matrix is $f_s = \{f_1, f_2, \ldots, f_n\}$and Harris corner matrix $f_H = \{f_1, f_2, \ldots, f_m\}$are computed individually. In this paper, the contrast criterion C_S is set to 0.2, and the contrast criterion C_H is set to 0. 0002.

B. K-NN (K Nearest Neighbor)

When extracting feature points, k-NN is used to compute feature similarity on SURF feature $f_s = \{f_1, f_2, \ldots, f_n\}$ and Harris corner features feature $f_H = \{f_1, f_2, \ldots, f_m\}$ to search for similar feature vectors [36]. Assuming there are n features, $f = \{f_1, f_2, \ldots, f_n\}$, the Euclidean distance is used to determine the similarity between two feature vectors. For the ith key point, its corresponding feature is represented by fi, and the Euclidean distance between fi and the remaining features $\{f_1, f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n\}$ is calculated. The results are sorted in ascending order to obtain $D = \{d_1, d_2, \ldots, d_{n-1}\}$. It is simple to implement, robust to the noisy training data and it can be more effective if the training data is large [38].

C. Eliminating Incompatible Pairs

Contrast standard In the previous step, matching point pairs were obtained, although many of them have defects. Currently, to improve the accuracy of forgery localization and detection, an effective technique is needed to eliminate the mismatched pairs. The challenge with existing mismatch removal techniques is that they ignore the limitations between point pairs and only think about the positional data of matching point pairs. The hierarchical clustering algorithm and the K-means clustering algorithm are two examples of these techniques.
Before clustering, a must be determined. A density-based clustering technique was proposed by Ester et al. [35] that divides dense areas based on clusters' maximum density-connected sets of points. HDBSCAN is capable of handling clusters of any shape, even when noise is present, and doesn't require the setup or extraction of clustering parameters.
To reduce mismatched matches, feature clustering is done in this work by employing HDBSCAN. We use the classical K-means approach knowing the predicted number of clusters, and we compare the output labels with those using HDBSCAN. The six categories listed below are employed by HDBSCAN to define point sets, as seen in Fig. 3:

K-means is unable to classify the data into meaningful clusters, as demonstrated in Fig. 4, even when given the appropriate number of clusters. In contrast, HDBSCAN provides the anticipated grouping.
• Dense areas separating extremely dense areas
• Extremely likely locations divided from unlikely regions
• We count the number of points within each ε-radius hyper sphere that is drawn around a given point. This is the density at that location in space, as estimated locally by us.

D. Redesigned Region Localization

In this work, we calculate the affine matrix of matched pairings and alter the dense regions of the image at the pixel level.

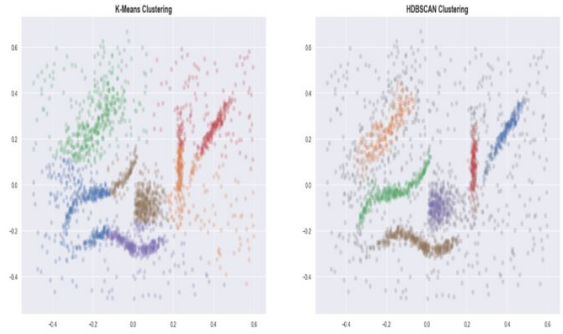

Fig. 3. HDBSCAN Diagram showing the relationship between three densities: (a) direct density; (b) reachable density; and (c) connected density [35].

to further increase the disturbed region localization accuracy. By comparing the altered image's similarity to the original image at the same unidentified place, the final tampered region is found.

Geometric transformations between objects can be shown using an affine transformation matrix, such as scaling, rotation, and other comparable changes. This allows for the estimation of the affine transformation. Based on feature point matching, the coordinates of the matched pairs can be utilized to estimate the affine transformation between the original and tampered regions. The following diagram shows the relationship between two matched pair coordinates that correspond to each other,

$X = (x, y)$ and $\hat{X} = (\hat{x}, \tilde{y})$

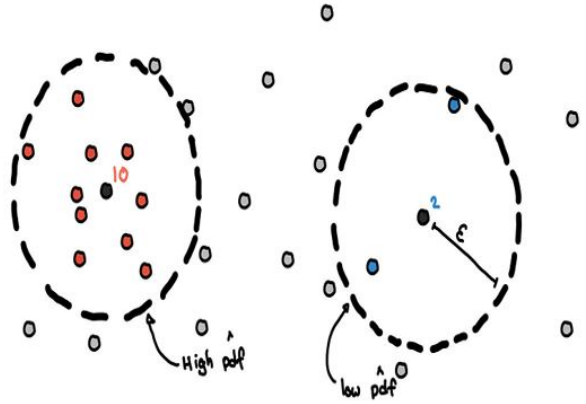

Fig. 4. Utilizing neighbor counts to estimate the probability density function (pdf) [36].

$$\begin{pmatrix} X^{\sim} \\ Y^{\sim} \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & t_x \\ c & d & t_y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ 1 \end{pmatrix} = T \begin{pmatrix} X \\ Y \\ 1 \end{pmatrix} \tag{5}$$

he translation parameters in the formula are t_x and t_y, whereas the scale and rotation transformation parameters are a, b, c, and d. There are at least three non-collinear matching pairs that can be used to calculate matrix T [37,38]. The set of matching pairs is designated as $\{(X_1, \tilde{X}_1), (X_2, \tilde{X}_2), \ldots, (X_n, \tilde{X}_n)\}$. after the mismatched pairs have been eliminated. An affine transformation matrix Ti is estimated from the three pairs of randomly chosen points, corresponding points from the matching list, and three randomly chosen points from each cluster. After computing each matrix, an ideal matrix T is covered that reduces the error, as indicated by the following equation:

$$argmin_T \, \|\tilde{X} - T_i\|^2 \tag{6}$$

All of the image's pixels receive the transformation using the acquired affine matrix T. Next, the original image and the modified image are superimposed, with the tampered portion Y_M overlying the original region Y_R. Similarly, region T-1 undergoes the inverse transformation, with the altered region Y_M overlaying the original region Y_R

$$Y_M = TYR, \quad Y_R = T^{-1} Y_M \tag{7}$$

Using the rapid polar cosine transform (PCT) as the basis, To identify the tampered areas, we compute the fast polar harmonic transform (PHT) feature as the similarity measure for corresponding locations in both the original and modified images. When the difference between two features is less than a predefined threshold, a place is tagged to create a map of the region of interest. Results of PHT feature computation for n-order continuous picture g for l consecutive times are shown below [38].

$$FasterM_{nl}^{c} = \Omega_n \int \int \sum_{k=1}^{K} \left(\cos(\pi n k^2 (x^2 + y^2))\right) (G_l(k_x, k_y) - iH_l(k_x, k_y))\, dx\, dy \tag{8}$$

Where:

$$K = \left\lfloor \frac{1}{\sqrt{x^2 + y^2}} \right\rfloor \tag{9}$$

and

$$A = \{(x,y) \mid 0 \le x \le 1, 0 \le y \le x, 0 \le x^2 + y^2 \le 1\}, rpp(x,y) \tag{10}$$

$\lfloor x \rfloor$ is floor function that backs the integral part of x. where $G_l(k_x, k_y)$ denotes the polar coordinates used to represent the image. The region is located and the final correlation map is generated by comparing the feature differences in the overlapping areas using a threshold value of t. For denoise and detail processing, a Gaussian filter with a window size of 5 x 5 and a standard deviation of 0.2 is then used. The final detection result is then obtained by completing the closing process.

V. Programming Environment

In the implementation of the image copy-move forgery detection technique using SURF, Harris Corner, and HDBSCAN clustering, the following tools, libraries, and programming languages were utilized:

A. Python

Python was chosen for its versatility and the availability of numerous libraries that facilitate image processing and machine learning tasks.

B. Libraries and Tools

OpenCV: Used for image processing tasks, including reading images, converting color spaces, applying filters, and extracting features. OpenCV's 'cv2' module provides efficient implementations of SURF and Harris Corner Detection.

1) NumPy

Utilized for numerical operations, particularly for handling image data as arrays and performing matrix operations, which are essential in image processing.

2) Scikit-Image

Provides additional image processing functionalities that complement OpenCV, such as morphological operations and feature extraction.

3) Scikit-Learn

Used for machine learning tasks, particularly clustering and dimensionality reduction. Although the primary clustering technique used was HDBSCAN, Scikit-Learn provided auxiliary tools for data preprocessing.

4) HDBSCAN

A specialized Python library for density-based clustering. This library was crucial for implementing the HDBSCAN algorithm, which was used to identify clusters in the feature space corresponding to potential forgeries.

5) Matplotlib

For visualizing the results, including plotting the detected regions, clusters, and performance metrics.

6) Jupyter Notebooks

Employed for development, testing, and documentation of the code. It allowed for an interactive environment where code, visualizations, and explanations could be combined seamlessly.

C. Practical Results

This section outlines the experimental studies on datasets of public images as well as the comparative analysis utilizing evaluation indicators and diagrams of the detection effects. This section demonstrates how the suggested technique is comparable to current research methods and proves the benefits of the accuracy and resilience of the suggested technique against changes in geometry.

1) Prepared Datasets

In our results, we applied three challenging datasets for testing: MICC, IMD, and CoMoFod [39].

2) MICC dataset

The most extensively used datasets in this field are MICC-F220 [39]. This dataset contains between-size images, the majority of them with a size of either 722 × 480 or 800 × 600 pixels. The total number of images is 220, 110 for original images, and 110 for tempered images. The first two subsets of this dataset were made by choosing a rectangular component of an image and placing it over another portion of the image, followed by a number of affine transformations. This dataset is broken into four subsets. In Fig. 5, samples from the dataset are shown. The dataset's advantage is that it uses gradual attack levels to thoroughly examine the relationship between various attack levels and detection accuracy. MICC dataset is available at
http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.

3) IMD dataset

With the help of the realistic images gathered from cameras, Christlein et al. (2012) built the Image Manipulation Dataset (IMD). The dataset was made up of real-world photographs in six images 3000 x 2300 in which the pixels were painted, used as backgrounds as in Fig. 6, or some other type of processing.

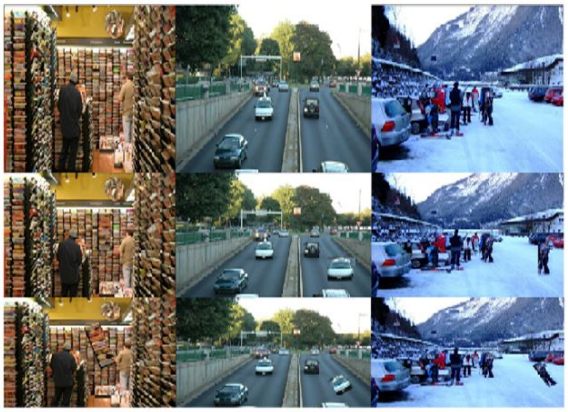

Fig. 5. Instances from dataset MICC-F220; First image - original image, All the images in the first row are tampered images with scaling. Second row, images with scaling are done at various levels combined with scaling. Third row, images with rotation are done at various levels combined with scaling.

Additionally, it contains contour pixels, where the duplicated data is rendered as partially transparent and creates seamless transitions between the original and nearby copied pixels. The dataset is available at https://www5.cs.fau.de/research/data/image-manipulation/.

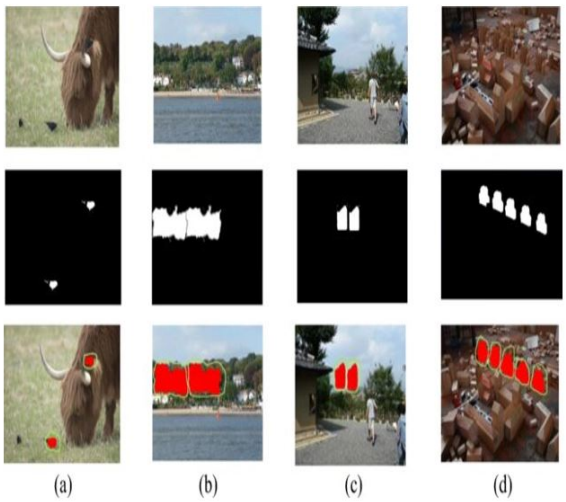

Fig. 6. Image copy-move forgery examples: First column: original image; second column: forgeries image of different attacks.

4) CoMoFoD dataset

The dataset consists of 200 original 512x512 pixel images that have been subjected to different geometric changes. These transformations are categorized into five groups: rotation, scaling, translation, combination, and deformation. There are 40 examples of altered photographs in each category, each of which has been altered using a different technique. These techniques include noise, blur, JPEG compression, rotation, and scale. The area of the duplicated region varies from 0.14 to 14.3% of the image area among the 10,400 images that make up the CoMoFoD collection.

D. Evaluation Metrics

The detection performance of the suggested strategy is thoroughly examined in this study using the most popular testing evaluations, recall, precision, and F1 score. R, P, and F1 are the corresponding symbols for these evaluation measures, and their respective formulas are as follows:

$$P = \frac{N_{MM}}{N_{MM} + N_{GM}}, \quad R = \frac{N_{MM}}{N_{MM} + N_{MG}}, \quad F_1 = 2 \times \frac{R \times R}{R + R} \tag{11}$$

where N_{MM} stands for the number of suspected modified and tampered images or pixels, N_{GM} for the number of suspected altered genuine images or pixels, and N_{MG} for the number of suspected modified and modified images or points that are found to be original. The superiority of the suggested method can be substantiated by comparison with other pertinent algorithms. This strategy not only relies on intuitive detection outcomes but also makes it possible to thoroughly assess the suggested method using factual facts.

E. Detection of Copy-Move Forgeries

This section displays the results of the experimental detection. The efficiency of the algorithm was verified by comparing the detection results with the grounded truth in the binary image provided by the dataset. The modified image in the first row, the binary ground truth image in the second row, which displays the real tampered area, and the experimental identification result of the approach described in this work in the third row reflect each detection result. The tampered area that was correctly identified is displayed in blue, the tampered region that was incorrectly detected is displayed in red, the tampered region that was missed is displayed in white, the true tampered region is displayed in dark gray, and the tampered area following border post-processing is displayed in light gray. to assess the efficiency.

In contrast to block-based techniques, the feature point identification part of feature point-based methods is extremely

TABLE I.
SHOWS THE NUMBER OF FEATURE POINTS IN THE ALTERED REGION (TEMPERED) THAT MATCH EACH OTHER.

Features	First Row	Second Raw	Third Raw	Fourth Raw
SURF	0	2	120	4
SIFT	0	14	211	12
Harris Corner	0	19	170	4
SURF+ Harris Corner	82	134	311	15

crucial, particularly the number of feature points identified in smooth areas. We examined SIFT, SURF, and Harris corners, in this experiment. When employing conventional techniques, feature extraction does not require the prior setting of a contrast threshold, and feature matching is accomplished using functions from the OpenCV database.

Experimental outcomes, once incorrect pairings have been removed, the set of matched pairings is totaled as indicated in Table I. The MICC dataset provided the photos for the first and second columns, whereas the IMD dataset provided the images for the third and fourth columns. For testing, we selected these pictures from the IMD dataset. Between them, are the first and third columns.

It is clear from Table I's testing outcomes for the four image columns in Fig. 7 that the suggested SURF and Harris corner feature points outperform other feature points by a significant margin. In the method proposed in this work, SURF and Harris corners were fused to create more additional corresponding and matching feature points in the feature extraction step, and a small contrast threshold was set in contrast to other traditional feature points that do not require it. Other feature extraction techniques, particularly for the evaluated image in the first column of Fig. 7, If manipulation takes place in the rounded area of the sky, don't find the required matching pairs. Only the recommended approach does.

Methods fail to find any signs of manipulation. As a result, the tampering activities in the smooth area are disregarded, decreasing the efficiency of detection.

1) Geometric Transformation Forgery Detection

The main focus of this study is on geometric transformation fraud experimentation and testing, including basic translation forgery detection, scaling forgery detection, and rotation forgery detection. A distinct effort is made to detect forgeries for each type of tampering. For every kind of tampering, a preset number of photographs were chosen from the dataset,

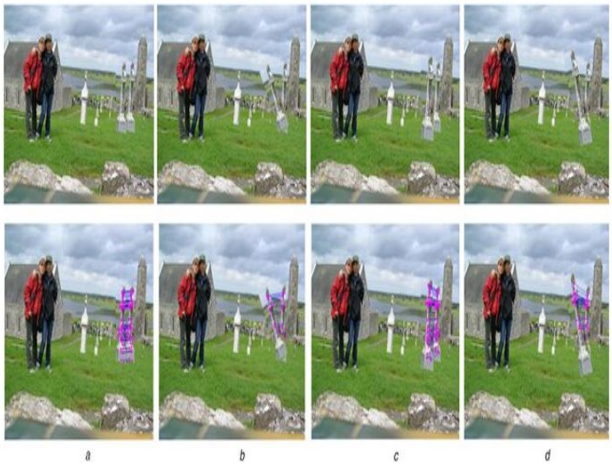

Fig. 7. The MICC-F220 experimental photographs are used to count the number of matching points of various key point features in the tampered area. The images are divided into four categories: hidden, tampered, b, and d.

and the experimental detection findings were presented as detection effect images. Our geometric transformation forgery research included a straightforward translation fraud detection study. A specific number of images from the dataset were chosen for trials for each sort of modification, and the outcomes of the testing detection are shown.

Fig. 6 and the partial experimental findings are provided below. The original image is shown in the figure's top row, followed by the dataset's images of binary truth from the dataset (used to compare with the detection findings), and the effect images in the third row. The suggested algorithm's detection findings, which were primarily utilized to test for simple translation forgery operations, are displayed in the third row.

Fig. 8 shows intuitively that there are no missing detection regions and that the experimental effect image of the suggested strategy nearly aligns with the binary image given in the dataset. The suggested method can discover tampered areas more precisely for photos that have not suffered complex manipulation, and there are no instances of erroneous identification and detection or missing identification in simple tampering.

Rotation alters forgery detection: Using photos from three publicly accessible datasets, we experimented with forgery detection by rotating the images at various angles. The detection results for rotation at various angles are shown in the photos in Fig. 9.

The original images are displayed in the first row of the figure, the images of binary truth are displayed in the second row for dataset comparison with the identification algorithm, and

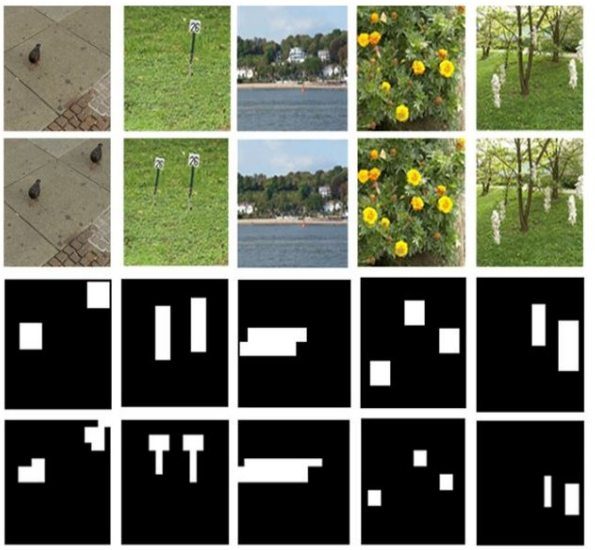

Fig. 8. Detection Simple translational forgery detection experimental findings. The original images are in the first row; the corresponding updated images and ground truth maps are in the second row; binarized truth images and forgery detection for 32 × 32 nonoverlapping blocks are in the third row; and forgery detection for 16 × 16 nonoverlapping blocks is in the fourth row.

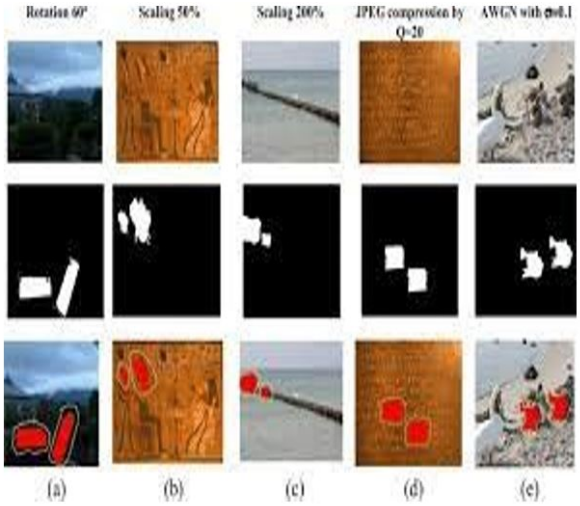

Fig. 9. Forging experiment results: rotation at 60 degrees, various scale values, JPEG compression, and AWGN noise. The original images are in the first row, binarized truth images are in the second, and effect images for forgery detection are in the third.

the detection results of the method suggested in this paper are displayed in the third row at various rotation angles. The suggested technique retains good detection accuracy even at various rotation angles, according to a comparison with the dataset's images of binary truth. There are essentially no missed detections when compared to the images of binarized truth in the second row. This benefit is especially noticeable in small-scale rotations, and the suggested technique performs well in terms of detection.

Scale transform forgery detection: Using photos from two freely accessible datasets, we executed scale manipulation tests. Scaling factors of 0.6 were employed. The experimental findings for these scaling variables are shown in Figure 8 from left to right. The original image is depicted in the first row, the binary ground truth from the dataset is shown in the second row, and the experimental findings from the suggested approach are shown in the third row. The suggested method still shows significant scale forgery identification capabilities, as can be seen by contrasting the identification results in the figure's third row with the binary photos provided in the dataset's second row. Particularly for moderate compression factors, the identification results have rarely missed detection zones. However, when the factor of scaling increases, as it does, for example, at a factor of scaling of 1.5, it is evident that there are missed detection areas in the perimeter of the detection findings. In summary, the method described in this research is an effective identification methodology, as demonstrated by comparisons with the binary images contained in the dataset, after experiments with basic translation forgery, rotation forgery at many perspectives, and compression factor forgery. In smooth areas where strong detection performance is still seen, the proposed technique may be able to identify tampered sections for geometric transformation forgeries accurately. When small-scale rotation and compression changes are used, it also works well. Suggested method with logical effect diagrams. All images from the MICC, CoMoFoD, and IMD datasets were used to perform the number of modified images correctly detected as tampered, the number of modified images falsely detected as original, and the number of original images incorrectly detected as tampered. Table II and Table III present the experimental results together with comparisons of precision, recall, and F1 to comparable methods in the literature. In addition, the three assessment metrics' standard deviations were calculated; the outcomes are displayed in Table IV.

We thoroughly evaluated the proposed algorithm's performance using three evaluation metrics and contrasted it with the techniques suggested in [16, 36]. It is evident from Table II's experimental data that the suggested algorithm has some benefits when compared to the comparison algorithms used for the Ardizzone dataset [35]. Our suggested algorithm has a higher degree of precision than the previous algorithms. The recall rate of the suggested algorithm is marginally reduced

TABLE II.
PRECISION (P), RECALL (R), AND F1 EVALUATION METRICS EXPERIMENTAL RESULTS

Method	Data set	P (%)	R (%)	F (%)
Guiwei et al. [1]	CoMoFoD	95.23	93.78	95.12
Sagnik et al. [40]	CoMoFoD	—-	——	90.93
Proposed model	CoMoFoD	96.21	94.76	96.12

TABLE III.
THE THREE EVALUATION INDICATORS' STANDARD DEVIATION ACROSS THE THREE DATASETS.

Image Dataset	Precision	Recall	F1
MICC	±0.12	±18	±19
IMD	±0.13	±22	±26
CoMoFoD	±0.14	± 24	± 23

than that of the approach in [16], but the F1 value shows a sizable advantage. This is mostly because we used two detection algorithms for feature extraction, and the Harris corner detector retrieved more features and points in smooth areas, leading to superior detection effectiveness in the tampering detection stage. This technique fares poorly in the identification of geometric transformation forgeries and is less resistant to rotational and scale invariance.
We combined SURF and Harris corners for the feature extraction step to collect sufficient feature points in smooth areas and eliminate mismatches using a density-based clustering approach to precisely and successfully find tampered areas. Using images from the MICC and IMD datasets, we conducted trials and recorded the times required by the recommended method. And the comparative algorithms to detect a single image to further verify the proposed technique's superiority in terms of time complexity. The data are shown in Table IV. The proposed method required an average of 2.54 s for feature extraction on the MICC dataset and 61.58 s for feature matching and mismatched pair detection. The average time for feature extraction on the IMD dataset was 4.29s, whereas the average time for other detections was 51.99s. On the CoMoFoD dataset, the suggested technique needed an average of 4.64 s for feature extraction and 63.38 s for feature matching and mismatched pair detection Because more feature points were extracted and more iterations were needed, the method suggested in [41] took longer to extract features and resulted in a longer detection time. Using the CoMoFod dataset, the average detection and identification time was 99.25 seconds. The approach suggested in [1] used a two-feature detector (SURF and accelerated KAZE and density spatial clustering to remove mismatching pairs, which surely enhanced the computing cost of the process. As a result, the average processing time for this approach on the CoMoFoD dataset was 54.23s. In summary, the suggested method surpassed the two comparison techniques according to temporal complexity by merging SURF and Harris corner which has the benefit of two detectors complementing one another as in Table IV.

TABLE IV.
COMPARISON IN COMPLEXITY OF TIME.

Dataset	Guiwei et al. [1]	Aydin et al [41]	Proposed method
CoMoFoD	54.23s	99.25s	53.43s
MICC	——	—-	75.12s
IMD	——	—-	59.14s

In the comparison of the state-of-the-art methods related to our algorithm, table V. shows the features and metrics that are used.

2) Post-Processing Forgery Detection

The main focus of this study is on post-processing techniques for image tampering detection using noise and Gaussian blur. The influence of visual detection was compared to the binary picture provided in the dataset to compare and assess the detection outcomes. Gaussian blur forgery detection: We chose two blur factors, = 0.75 and = 2, to test the effectiveness of the proposed technique in detecting Gaussian blur counterfeit. The detection results are shown in Fig. 9. The first line of the figure displays the original photos; the second line displays the binaries truth images. and the third row shows the results of the suggested approach's detection. A comparison between the binary images from the dataset and the detection results of the proposed technique, where the Gaussian blur factor is set to = 2, shows that no detections were missed and that the suggested method accurately found the tampered regions in the binary images. To evaluate the efficacy of the proposed technique for identifying Gaussian white noise tampering and Gaussian white noise forgery detection,

To the images in the dataset, we applied Gaussian white noise (AGWN) with variance values of 0.0005 and 0.001, and mean values of $m = 0$. The paper's detection results, in both noise and Gaussian blur forgery detection, bear striking similarities to the binary images included in the dataset. This demonstrates how well the proposed method works for post-processing tasks such as Gaussian white noise and Gaussian blur forgeries. Overall, the proposed method finds tampered locations more accurately and yields more precise detection results, especially when the noise variation and blur factor are

TABLE V.
COMPARISON OF THE STATE-ART METHODS

Reference	Key Features	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Comments
Diwan et al., 2023 [42]	Superpoint Keypoint Architecture	97.8	96.5	97.2	96.8	A novel approach with advanced keypoint detection (SpringerLink)
Yang et al., 2023 [40]	Gradient-Hash Matching	96.4	95.0	96.0	95.5	Emphasizes gradient-hash features for robust matching
Wang et al., 2024 [43]	Adaptive key points with FQGPCET-GLCM	97.0	95.7	96.8	96.2	Combines adaptive key points with advancedfeature extraction
Dhillon et al., 2020 [44]	SURF + SVM Supervised Learning	95.2	94.0	95.0	94.5	Integrates machine learning with SURF for detection
This Work	Proposed Method (SURF + Harris + DBSCAN)-(MICC data set)	——	97.0	98.0	97.5	High accuracy and robustness

small.
Fig. 10 displays the F1 score results for the two comparison algorithms as well as the suggested approach. As illustrated in the image, the suggested approach provides a notable benefit in.

The proposed algorithm improves upon the high temporal complexity and edge detection challenges of conventional copy-move forgery detection approaches by:

1. Reducing Temporal Complexity: Due to the correct choice of descriptors, reducing the dimensions while preserving the maximal amount of information, the right choice of the clustering algorithm and the feature matching, the time needed for the processing is minimal without declining the accuracy.

2. Improving Edge Detection: It also reduces the edge artifacts due to nonlinear diffusion, edge-aware clustering, and the geometric consistency check all help to improve the chance of detecting forgeries even near the edges and boundaries.

VI. DISCUSSION

A. This method can contribute to the following points:

1- Improved Accuracy and Reliability
- SURF and Harris Corner Detection: Stress that using the speeded-up robust feature combined with Harris corner detection to extract features improves the detection of copy-move forgeries. SURF is quite immune to distortions that are evident in forged images such as scaling and rotation. Harris Corner detection does this to a finer level by only looking at particular points of interest that will enhance the reliability of the detection.
2- HDBSCAN Clustering: There is more to be gained out of HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise) than DBSCAN or k-means. It is more suitable for working with data of different densities that, by and large, are found when investigating forgery so clustering will be more effective for identifying the forged areas.
3- Reduction of False Positives
- Combination of Techniques: Our method minimizes false positives with the integration of SURF, Harris Corner, and HDBSCAN. In traditional approaches, we have faced difficulties in considering several regions as either genuine or forged; however, our approach of using feature extraction along with density-based clustering provides a sound mechanism for such detection.
4- Scalability and Applicability
Efficiency in Large Datasets: Our method can be well-applied to big data or images that are high-resolution. The effectiveness of using the SURF in feature extraction Plus is enhanced by the processing effectiveness of HDBSCAN, our proposal method is ideal in applications where quick detection

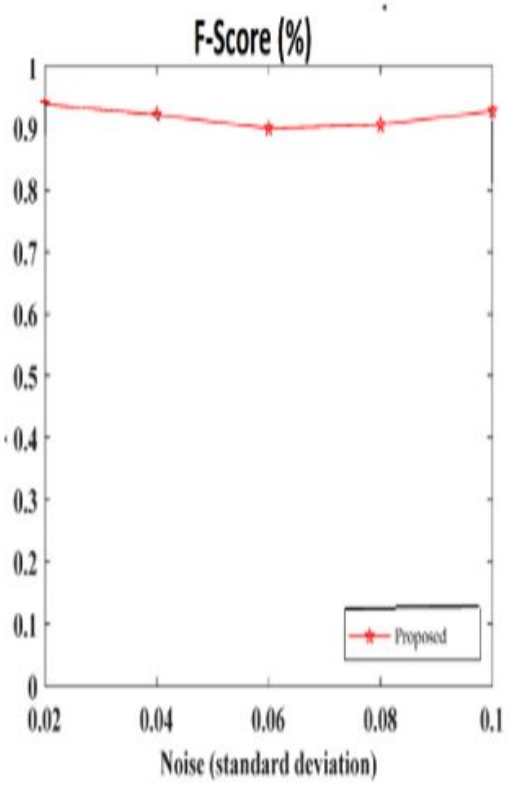

Fig. 10. Score for noise addition attack

is paramount.

B. Limitations

However, as with any method that we presented, the proposed algorithm here also has some drawbacks that are worth mentioning. Firstly, the choice of features and the training algorithm more or less fail when it comes to handling forgeries with affine or perspective transformations. These transformations can distort the forged regions in such a manner that can put to test the feature extraction as well as the clustering algorithm. Continuation of this work should involve the development of improvement to feature extraction techniques or the utilization of other geometric transformation models that can help overcome this problem.

Finally, it may be worth enhancing the computational efficiency of the constructed algorithm. At present, the algorithm is computationally demanding, and more so when dealing with high-resolution images or large data sets. This is so because the model has a limitation of not being able to be utilized in real-time conditions. It might be improved by optimization techniques like a fine tune of the algorithm or using parallel processors to accelerate the computations.

C. Future Directions

In the future work, we can discuss potential future directions as follows:

1- Expanding the Dataset: Opportunities for future work may include an elaborate data set to test the proposed system. It would also be possible, also, to try to take more complex images, images in different lighting conditions, and images with different kinds of forgeries to test the robustness of the system. This could benefit the later parts of this research by providing ways to generalize the model to increase its probability of performing well in many situations.

2- Exploring Different Neural Network Architectures: The current work employs the classic image processing approach Hence, there is a possibility that the subsequent studies could incorporate neural networks like the CNNs or the transformers for better extraction of features and classification. There may be other how better structures can be chosen or improved and these can form better forgeries if found in the complicated and subtle forgeries cases.

3- Testing the System in Clinical Settings: Another possible evolution is to apply the system in clinical or real environments where the identification of forged documents and confidence in the system are paramount. It might include working with forensic professionals or using it as a tool where an image's genuine provenance is relevant, like in legal proceedings or media credibility systems. Because of that, evaluation of the system performance in such environments may be beneficial and help to identify additional capacity to improve it.

4- Integration with Other Forensic Tools: Another research area for future works can also investigate how the proposed system can be integrated with other forensic analysis tools. Researchers have tried to combine one or several techniques, for instance, when the system utilizes metadata analysis or steganalysis and so on, the accuracy for forgery detection could then be improved, so expanding the range of positive methods in steganalysis.

5- Real-Time Detection: Another way for future research is in the direction of building real-time forgery detection mechanisms. Improving the system's performance and the time taken to process the information could make the system ideal in real-time applications like real-time video analysis or surveillance systems where forgery detection is critical as it happens

VII. Conclusion

In this research, we first merged the Harris corner detector and SURF detector, and then we matched features using HDBSCAN clustering. The HDBSCAN clustering technique was used to eliminate false positives and erroneous matches to increase localization accuracy. The experimental findings demonstrate the suggested method's effective detection capabilities. In smooth areas, SURF and Harris corners can extract useful feature points, while the HDBSCAN clustering algorithm can eliminate erroneous matches, lowering the number of false alarms. The suggested technique achieves increased detection accuracy in smooth areas and shows significant resilience to many kinds of manipulation, such as scaling and rotation. This approach performs well for detection when tampering procedures involve tiny blur factors and noise variances.

Declaration

We certify that We have read, comprehended, and accepted the journal's submission procedures, policies, and submission statement. The manuscript's author also states that it has no disclosed conflicts of interest. The manuscript is the author's original work; it has not been published before and is not currently being considered for publication elsewhere.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] G. Fu, Y. Zhang, and Y. Wang, "Image copy-move forgery detection based on fused features and density clustering," *Applied Sciences*, vol. 13, no. 13, p. 7528, 2023.

[2] A. Bensaad, K. Loukhaoukha, and S. Sadoudi, "Keypoint-based copy-move forgery detection in digital images: a survey," in *2022 7th International Conference on Image and Signal Processing and their Applications (ISPA)*, pp. 1–6, IEEE, 2022.

[3] S. Paul and A. K. Pal, "A fast copy-move image forgery detection approach on a reduced search space," *Multimedia Tools and Applications*, vol. 82, no. 17, pp. 25917–25944, 2023.

[4] R. Anushree, V. K. SB, and B. Sachin, "A survey on copy move forgery detection (cmfd) technique," in *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, pp. 439–443, IEEE, 2023.

[5] A. K. Venugopalan and G. Gopakumar, "Copy-move forgery detection-a study and the survey," in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, pp. 1327–1334, IEEE, 2022.

[6] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection.," *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[7] J. Fridrich, D. Soukal, J. Lukas, *et al.*, "Detection of copy-move forgery in digital images," in *Proceedings of digital forensic research workshop*, vol. 3, pp. 652–63, Cleveland, OH, 2003.

[8] A. Kumar, K. U. Singh, C. Swarup, T. Singh, L. Raja, and A. Kumar, "Detection of copy-move forgery using euclidean distance and texture features.," *Traitement du Signal*, vol. 39, no. 3, 2022.

[9] S. A. Fattah, M. Ullah, M. Ahmed, I. Ahmmed, and C. Shahnaz, "A scheme for copy-move forgery detection in digital images based on 2d-dwt," in *2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 801–804, IEEE, 2014.

[10] F. I. Rahma, E. Utami, and H. Al-Fatta, "Gaussian pyramid decomposition in copy-move image forgery detection with sift and zernike moment algorithms," *Telematika*, vol. 15, no. 1, pp. 1–13, 2022.

[11] M. Sabeena, L. Abraham, and A. Varghese, "Digital image forgery detection using local binary pattern (lbp) and harlick transform with classification," in *2021 IEEE International Power and Renewable Energy Conference (IPRECON)*, pp. 1–6, IEEE, 2021.

[12] J.-C. Lee, C.-P. Chang, and W.-K. Chen, "Detection of copy–move image forgery using histogram of orientated gradients," *Information Sciences*, vol. 321, pp. 250–262, 2015.

[13] W. Ye, Q. Zeng, Y. Peng, Y. Liu, and C.-C. Chang, "A two-stage detection method of copy-move forgery based on parallel feature fusion," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 30, 2022.

[14] C. Qin, X. Chen, D. Ye, J. Wang, and X. Sun, "A novel image hashing scheme with perceptual robustness using block truncation coding," *Information Sciences*, vol. 361, pp. 84–99, 2016.

[15] S. Kumar, S. Mukherjee, and A. K. Pal, "An improved reduced feature-based copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 82, no. 1, pp. 1431–1456, 2023.

[16] C. Wang, Z. Huang, S. Qi, Y. Yu, G. Shen, and Y. Zhang, "Shrinking the semantic gap: spatial pooling of local moment invariants for copy-move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1064–1079, 2023.

[17] M. Salman and A. Uhl, "Countering anti-forensics of sift-based copy-move detection," in *2020 25th International Conference on Pattern Recognition (ICPR)*, pp. 2701–2707, IEEE, 2021.

[18] M. Samel and A. M. Reddy, "An empirical study on copy-move forgery detection techniques in images," *Mathematical Statistician and Engineering Applications*, vol. 71, no. 3, pp. 183–193, 2022.

[19] N. Kumar and T. Meenpal, "Salient keypoint-based copy–move image forgery detection," *Australian Journal of Forensic Sciences*, vol. 55, no. 3, pp. 331–354, 2023.

[20] 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.

[21] G. Fu, Y. Zhang, and Y. Wang, "Image copy-move forgery detection based on fused features and density clustering," *Applied Sciences*, vol. 13, no. 13, p. 7528, 2023.

[22] J. Zheng and K. Zhang, "Copy-move forgery detection algorithm based on feature point clustering," in *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*, vol. 6, pp. 775–780, IEEE, 2022.

[23] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, pp. 91–110, 2004.

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

[25] X. Wang, W. Chen, P. Niu, and H. Yang, "Image copy-move forgery detection based on dynamic threshold with dense points," *Journal of Visual Communication and Image Representation*, vol. 89, p. 103658, 2022.

[26] Y. Liu, H. Wang, Y. Chen, H. Wu, and H. Wang, "A passive forensic scheme for copy-move forgery based on superpixel segmentation and k-means clustering," *Multimedia Tools and Applications*, vol. 79, pp. 477–500, 2020.

[27] X.-Y. Wang, C. Wang, L. Wang, L.-X. Jiao, H.-Y. Yang, and P.-P. Niu, "A fast and high accurate image copy-move forgery detection approach," *Multidimensional Systems and Signal Processing*, vol. 31, pp. 857–883, 2020.

[28] B. Fatima, A. Ghafoor, S. S. Ali, and M. M. Riaz, "Fast, brief and sift based image copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43805–43819, 2022.

[29] J. Sujin and S. Sophia, "Copy-move geometric tampering estimation through enhanced sift detector method.," *Computer Systems Science & Engineering*, vol. 44, no. 1, 2023.

[30] T. Ouyang and X. Shen, "Online structural clustering based on dbscan extension with granular descriptors," *Information Sciences*, vol. 607, pp. 688–704, 2022.

[31] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (surf)," *Computer vision and image understanding*, vol. 110, no. 3, pp. 346–359, 2008.

[32] 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.

[33] P. F. Alcantarilla and T. Solutions, "Fast explicit diffusion for accelerated features in nonlinear scale spaces," *IEEE Trans. Patt. Anal. Mach. Intell*, vol. 34, no. 7, pp. 1281–1298, 2011.

[34] B. Borah and D. K. Bhattacharyya, "An improved sampling-based dbscan for large spatial databases," in *International conference on intelligent sensing and information processing, 2004. proceedings of*, pp. 92–96, IEEE, 2004.

[35] P. Berba, "Understanding hdbscan and density-based clustering," *Pepe Berba*, 2020.

[36] Y. Tang, Y. Chang, and K. Li, "Applications of k-nearest neighbor algorithm in intelligent diagnosis of wind turbine blades damage," *Renewable Energy*, vol. 212, pp. 855–864, 2023.

[37] Z. Yang and S.-i. Kamata, "Fast polar harmonic transforms," pp. 673 – 677, 01 2011.

[38] S. Ganguly, S. Mandal, S. Malakar, and R. Sarkar, "Copy-move forgery detection using local tetra pattern based texture descriptor," *Multimedia Tools and Applications*, vol. 82, no. 13, pp. 19621–19642, 2023.

[39] R. Dhanya and R. Kalaiselvi, "Critical study of the copy-move forgery datasets," *International Journal of Engineering Research & Technology (IJERT)*, vol. 12, April 2023.

[40] J. Yang, Z. T, and e. a. Jianqing, "A novel copy–move forgery detection algorithm via gradient-hash matching and simplified cluster-based filtering," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 37, no. 06, 2023.

[41] Y. Aydin, "Comparison of color features on copy-move forgery detection problem using hsv color space," *Australian Journal of Forensic Sciences*, vol. 56, no. 3, pp. 294–310, 2024.

[42] D. DeTone, T. M, and A. R., "Superpoint: Self-supervised interest point detection and description," in *CVF Open Access*, 2023.

[43] X.-y. Wang, X.-q. Wang, P.-p. Niu, and H.-Y. Yang, "Accurate and robust image copy-move forgery detection using adaptive key points and fqgpcet-glcm feature," *Multimedia Tools and Applications*, no. 1, pp. 2203–2235, 2024.

[44] S. Dhivya, J. Sanyeetha, and B. Sudhaka, "Copy-move forgery detection using surf feature extraction and svm-supervised learning technique," *Soft Computing*, vol. 24, 2020.