Received: February 1, 2023. Revised: April 21, 2023. 12

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Copy-Move Image Forgery Detection Using Modified SURF Features and A-KAZE Detector

Shreenath Kannughatta Narasimhamurthy[1]* Vasantha Kumara Mahadevachar[2]
Ram Kumar Thayur Narasimhamurthy[3]

[1]*Department of Computer Science & Engineering, Siddaganga Institute of Technology, Tumkur, India*
[2]*Department of Computer Science & Engineering, Government Engineering College, Hassan, India*
[3]*Department of Computer Science & Engineering, Ramaiah Institute of Technology, Bengaluru, India*
* Corresponding author's Email: shreenathk_n@sit.ac.in

Abstract: Copy-move forgery detection (CMFD) is a well-known digital image forgery technique that is used in detecting forgery regions of images. The copy-move forgery in images occurs when a specific section of an image is attached to a new component of the same image to replicate the forged image parts as an original. The forgery appears to be realistic because even after being forged in the objective region, the image acquires all the basic qualities of the original image. Some post-processing functions, such as scaling or rotation invariant, noise handling, hybrid image manipulation, etc., limit the capability of CMFD models. To overcome these limitations, the features are extracted from the Hybrid feature extraction using modified speeded up robust feature (M-SURF) with accelerated KAZE (A-KAZE) feature description and detection algorithm. The main advantages of the SURF descriptor are: the SURF features are resistant to several post-processing attacks and use Laplacian of gaussian to differentiate background and foreground features clearly. The A-KAZE descriptor is robust in detecting scale-invariant of forged regions and poorly localized key points of objects. A-KAZE constructs the invariant scaling levels using nonlinear diffusion filtering. It smooths the image while preserving the edges and decreasing speckle noise. As a result, it captures the precise location of features during the feature extraction process. Following the feature extraction, the matched features are compared, and removed false matches by applying random sample consensus (RANSAC) technique. The performance evaluation of the proposed Hybrid MSURF with A-KAZE CMFD method is validated on MICC-F220, MICC-F2000, CoMoFoD datasets and surpasses the existing CMFD methods. The proposed CMFD achieved better results compared to existing methods such as when CMFD based on DHE-SURF features along with mDBSCAN clustering and CMFD based on SURF, BRISK features along with DBSCAN clustering measured in terms of Precision of 99.93%, Accuracy of 99.46%, F1-score of 98.21%, true positive rate (TPR) of 99.93%, and false positive rate (FPR) of 4.67%.

Keywords: Copy-move forgery detection, Feature descriptor and detector, Hybrid features, Modified speeded up robust feature, Random sample consensus.

1. Introduction

With recent advancements in image processing, people can easily modify and tamper images by using image editing software tools such as Corel Paint Shop, PhotoScape, GNU Image Manipulation Program (GMIP), and Photo plus, etc. In the era of digitalization, one of the significant communication tools is images that are used all over the world among people. Forgery images have become common in the media and day-to-day life over the past few years. The negative consequences of these forgery images have sparked widespread concern.

The most prevalent type of image forgery is called copy move forgery of images in which one or more image regions are copied and attached to other regions of the same image. [1, 2]. The forgery regions can be identified by exposing the selected forged image to rotations, translation, adding noise, illumination change, and so on, making obtained image extremely difficult to identify. High-quality forged images are difficult to recognize with the bare

eye, so an appropriate method must be employed to distinguish the forged regions [3]. The image authentication methods are categorized into active and passive, in which digital watermarking and digital signatures fall into the first category and copy-move forgery falls into the second category. The drawback of the digital watermarking method is; it depends on the specially created information watermark to authenticate an image. Similarly, the disadvantage of digital signatures is, it depends on digital signatures to authenticate an image. The copy move forgery operations are categorized into two types namely: block-based methods and key based methods. In block-based method, the input image is divided into a fixed size of overlapped circular or square shaped blocks. In the key point based approach, the execution time of the block based method is addressed, which is usually of long durations. Key points represent points of interest in an image and do not change even if the image has undergone geometric transformations such as rotation, scaling, and so on [4, 5].

The CMFD framework commonly consists of five stages known as preprocessing, feature extraction, matching stage, false match removal, and refining stage. Preprocessing is an optional process in which the Red, Green, and Blue (RGB) color images are converted into grayscale images like Green (Y), Blue (Cb), and Red (Cr) (YCbCr) or hue saturation value (HSV) to minimize the input images' dimensionality. The main process in CMFD is feature extraction, where the extracted features must be invariant to scaling, and rotation, as well as robust in handling post-processing attacks such as blurring, compression, and noise addition [6]. SURF, scale invariant feature transform (SIFT) and Histogram of Oriented Gradients (HOG) are three commonly used feature descriptors in extracting images' key points of interest with different scales and rotations. SURF is the most commonly used fastest feature extraction technique compared to SIFT and HOG used in CMFD, where the image features are arranged to identify common portions to minimize computational unpredictability and enhance false recognition accuracy. SURF feature extraction involves two operations namely SURF detection and SURF description [7]. The idea of extracting SURF features is to divide the image into blocks and perform a matching process between each block. The third stage in CMFD is Matching features where the features-wise classification is performed to label an image. The matching process between the block of interest and its complementary images generates features in the form of a distance vector. For this vector, a correlation matrix is constructed, and singular value decomposition is utilized to extract the final set of features for classification [8]. Many researchers have focused on feature extraction tools combined with SURF. For example, SURF based exponent-fusion moments (EFM), corner detector with Polar cosine transform (PCT) descriptor, SURF based Polar complex exponential transform (PCET) descriptor. These algorithms have common limitations like a computational burden, which is primarily due to the matching of a large number of image blocks (approximately between 10^5 to 10^6) [9,10].

Most of the existing CMFD methods used BRISK, HOG, SIFT and SURF feature extraction methods. The drawbacks of these feature extraction methods are: detecting a high number of false matches, less accuracy in detecting forged regions, and less robustness in handling high scaling, noise, and compression. Hybrid feature extraction can overcome these drawbacks with MSURF and A-KAZE.

The major contributions of the proposed work are listed below:

- The false matches caused by copy-move forgery are minimized by implementing MSURF Hybrid feature extraction with A-KAZE feature descriptor and detection algorithm.
- The objects catalog is created to cluster the images using the Connected Components Labelling (CCL) technique and further performs open and close morphological operations that help in feature extraction. The CCL technique is used in processing high-dimensional color images and also helps in finding interconnecting between images.
- An affine transformation is used to handle both scaling and rotation simultaneously, and also a RANSAC algorithm is applied to extracted features in the feature-matching stage. The advantage of using the RANSAC algorithm is that its processing time is less even if the input data size is more.

The rest of the manuscript is structured as follows: Section 2 summarizes the related works of existing CMFD methods. Section 3 describes the proposed CMFD method. Section 4 illustrates the results and performance evaluation of the proposed method and section 5 provides the conclusion.

2. Literature review

Muhammad Bilal, [11] proposed a CMFD method that uses dynamic histogram equalization (DHE) to adjust the input images' contrast. The

performance of this method was evaluated on three specific standard datasets, such as MICC-F2000, MICC-F220, and CoMoFoD. For extracting manipulated image features, the SURF descriptor was used and matched with Euclidean distance. A clustering application was employed to the similar features with a novel method of modified density based clustering of applications with noise (mDBSCAN) which creates a binary mask and detects CMF regions. The experimental results have surpassed the existing CMFD methods in terms of precision and recall. The continuous phase of improvement and refinement caused more complexity in handling post-processing attacks which was the drawback of this method.

Muhammad Bilal, [12] proposed a novel CMFD method which was robust in detecting various forged regions of images and overcoming post-processing attacks. The performance of the proposed CMFD was validated on some specific standard datasets like MICC-F220, MICC-F2000, and CoMoFoD. descriptors like Binary invariant scalable key-points (BRISK) and SURF were used for feature extraction in CMFD. The proposed CMFD method surpasses the state-of-the-art methods in terms of TPR and FPR. The experimental results have shown that more false matches were detected, which is a limitation of this method.

Mohamed A. Elaskily, [13] proposed a deep learning based CNN for automatic CMFD. Standard datasets namely: MICC-F220, MICC-F2000, SATs-130, and MICC-F600 were used in this research, which consist of original and forged. The performance evaluation of the proposed method was measured in terms of computational cost, accuracy, TPR and FPR. High scaling issues has resulted in poor quality of image, which is a limitation of this work. In the future, more challenging datasets may be used with the deep CNN approach, which can also detect other digital image forgeries. Yohanna Rodriguez-Ortega, [14] proposed two deep learning approaches to address generalization issues with appropriate hyperparameter selection from eight datasets, such as the copy move forgery dataset, MICC-F2000, MICC-F220, Coverage, CG-1050 v1, CG-1050 v2, CASIA v1, and CASIA v2. Custom design and transfer learning are the two approaches based on CNNs used in the detection of copy move forgery. A CNN to the fully connected (FC) network was considered as the first approach, and a VGG-16 network was considered for image classification in the second approach. The second approach achieved the highest performance compared to the first one in terms of precision, recall, and F1 score. The robustness of this framework was low due to long execution approaches, which is alimitation of this work. In the future, domain transformation techniques like discrete-wavelet transform (DWT), discrete cosine transform (DCT), and discrete fourier transform (DFT) can be used by considering extending the training dataset.

H. Kasban et aI [15] proposed an image forgery detection method which was tested on seven open access datasets such as CASIA-v1, CASIA-v2, MICC-F2000, MICC-F220, MICC-F600, and CoMoFoD. This method was proposed to present a robust detection method in image forgery by converting an RGB image into YCbCr space. This method used the Hilbert-huang transform (HHT) to extract chrominance red (Cr) component features and three classifiers support vector machine (SVM), K-nearest neighbors (KNN), and artificial neuron networks (ANN). The accuracy of this image forgery detection method was measured in terms of the structural similarity index measure (SSIM). The proposed method was vulnerable to post-processing attacks, which was a limitation of this work, and this can be avoided further by optimizing the SSIM value with the attack parameters or verification parameters like cross-correlation.

Aya Hegazi, [16] proposed an improved key point based CMFD, which was validated on two benchmark datasets, namely MICC-F220 and the image manipulation dataset. By evaluating the performance metrics of this method, it was concluded that the proposed detection method was resistant to post-processing attacks, geometric attacks, and multiple cloning. Limited dataset has resulted in the poor performance of the model, which is a limitation of this work. This method was effective in detecting image-forged regions with the fewest false matches and can even reduce to less number of false matches in the future, using Gaussian noise comparison techniques.

Faten Maher Al_azrak, [17] proposed a robust CMFD method by combining key-based and block-based detection techniques. A modified Fuzzy C-means (FCM) algorithm was considered to extract image features from each block, and an emperor penguin optimization (EPO) was considered to improve the process of segmentation by optimizing the influential degree. The performance of this method was validated on the MICC-F600 dataset and obtained better performance in terms of F1-score, precision, and recall. The accuracy of this method in detecting forged regions is unknown which is a major drawback. The robustness of this approach can be improved in future by considering an optimized deep fully resolution convolutional neural network (CNN).

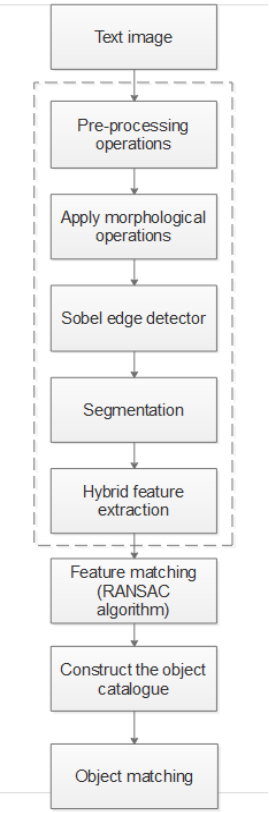

Figure. 1 Flowchart of improved proposed CMFD method

To overcome the limitations of existing CMFD methods like handling post-processing attacks like excessive scaling, rotation, and adjusting brightness, the M-SURF with A-KAZE feature descriptor and detection algorithm is proposed. The proposed method is fast and robust in detecting tampered regions in the tampered images, handles pre-processing attacks, and removes false matches using the RANSAC algorithm.

3. Methodology

The proposed CMFD method performs image segmentation using connected components labelling (CCL) and feature extraction using modified SURF with A-KAZE detection and descriptor algorithm. The tested image is first segmented into objects, and the objects catalog is created to extract features from each labeled region with modified SURF descriptors. In the end, the object catalog is created using these descriptors and a matching process takes place to compare similar attributes of the objects within the catalog. The proposed CMFD includes two stages in which the primary stage includes detecting original images and copy-move forgery in the images.

The second stage includes verifying the original image's integrity and checking whether CMF regions in the image exist. Fig. 1 illustrates the flowchart of identifying CMF regions from the original image and applying morphological operations along with image segmentation and feature extraction processes. The other processes like object catalog, object detection, and edge detection are described briefly below sections.

3.1 Dataset description

The standard datasets namely MICC-F220, MICC-F200 and CoMoFoD is considered for evaluating the proposed CMFD approach. The MICC-F220 incorporates a total of 220 images with 722×480 to 800×600 pixel resolution. Out of 220 images, 110 are the original images and the remaining 110 are forged images with 1.2% of the image portion being forged. The MICC-F2000 consists of 2000 images. The CoMoFoD dataset consists of 200 tampered images with 512×512 pixels. The patched regions of rectangular or square shape are pasted randomly over the original image to create forged images from this dataset. Original image samples with a comparison of tampered regions from the MICC-F220 dataset are shown in Fig. 2.

3.2 Object detection

Object detection is a process of three stages namely: close morphological operation, edge detection, and image segmentation. For labeling image regions and detecting various object locations in the image, a CCL technique is applied to the images. CCL is a unique method used in a wide range of applications including pattern recognition, image analysis, computer vision, image understanding, and eliminating false alarms on masked images. CCL involves blob discovery and extraction as a method of image segmentation where regions with constant properties are represented by the blob. These regions indicate the presence of objects which is then used for detecting and tracking objects. The three object detection stages are described below:

3.2.1. Close morphological operation (CMO) application

The CMO application involves an essential morphological operation that closes small gaps and blinds tiny cracks in an object's boundaries. The primary objective of this application is to analyze images based on their shape by using a set of nonlinear image processing techniques. These operations include edge detection, skeletonization, noise reduction, and other methods. The closing

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

Figure. 2: (a) and (c) original images and (b) and (d) CMF images

-1	0	1
-2	0	2
-1	0	1

G_x

1	2	1
0	0	0
-1	-2	-1

G_y

Figure. 3 Convolutional kernels of Sobel edge detector

operation is carried out on a binary image and a structuring element of fixed size. By filling in tiny, thin gaps in an object's boundaries and reducing tiny projections, the closing operation displays object outlines [18]. An object's foreground pixels tend to increase as its borders or contours are smooth. To make the borders of the regions more distinct, background holes or points are also minimized.

3.2.2. Edge detection

Edge detection is accomplished in a three-stage process namely: noise reduction, enhancing edges, and edge localization. To detect edges, Sobel detector is used in this work by calculating gradient pixel intensity in the image. By analyzing the changes in image orientation from light to dark pixels, the detector determines whether the pixel represents edges or not. Previous steps along with edge detection are intended to make the image ready for the segmentation process and contour tracking using CCL.

The Sobel detector measures the gradient intensity of an image using 3×3 convolutional kernels as shown in Fig. 3.

The Magnitude of Gradient intensity of pixels in orientation x and y is given by Eq. (1).

$$|G| = \sqrt{G_x^2 + G_y^2} \tag{1}$$

Where, $|G|$is the Gradient intensity magnitude, G_x is the gradient component in x direction, and G_y is the gradient component in the y direction.

Both gradient components can be measured individually as shown in Eq. (2), by applying these kernels to the input image. The approximate magnitude can be calculated using the below Eq. which is the fastest way of computing.

$$|G| = |G_x| + |G_y| \tag{2}$$

The change in the angle of edge orientation ultimately leads to the spatial gradient and it is represented as shown in Eq. (3).

$$\theta = arctan\left(\frac{G_y}{G_x}\right) \tag{3}$$

3.2.3. Image segmentation using contour tracking

A CCL labelling technique is adopted for image segmentation which is an important task in the object

detection process. The integrated pixel regions are detected by performing scanning phenomena to the edge-detected binary pixel using CCL from top to bottom and left to right. Based on the intensity value, each pixel is labeled as either foreground or background. If a pixel is not in the background, it is considered to be an object, and it is allocated in the object table after performing a connectivity check. Object bounding boxes are displayed after allocating each pixel particular foreground object or background region.

3.3 Hybrid feature extraction

The modified SURF algorithm is employed to the gray level images in this step to obtain object features. For each candidate region, SURF descriptors are obtained. The SURF is a local feature detector and descriptor that is fast, robust, and dependable. In each region, the point of interest is detected first, and later a 64-dimensional vector of features for each interesting point is computed. Rotation, scaling, translation, and lighting changes do not affect SURF descriptors. Finally, an object catalog is built by linking the extracted objects to their SURF descriptor. A modified SURF with an A-KAZE descriptor is proposed in this work to extract hybrid features. Initially, the A-KAZE descriptor is used in Hybrid feature extraction and secondly, a modified SURF descriptor will be employed.

3.3.1. Modified SURF descriptor

A Modified SURF descriptor (MSURF) is used in building a feature descriptor by considering a rectangular grid of $24\sigma_i \times 24\sigma_i$ size. The grid size is divided into 4×4 overlapping sub-regions of size $9\sigma_i \times 9\sigma_i$. For each key point, the derivatives of the first order, Lx and Ly are determined with a size of σ_i. A Gaussian Kernel is used to weigh the derivative responses, and each sub-region is added together to form a descriptor vector as shown in E Eq. (4).

$$v = \left\{\sum L_x,\ |\sum L_x|, \sum L_y,\ \left|\sum L_y\right|\right\} \tag{4}$$

The feature detector detects features directly and if the feature locations are chosen incorrectly, considering the influence of speckle noise, the error will be propagated to the subsequent steps of image registration. This step has been allocated to the A-KAZE and the descriptor, on the other hand, defines how the detector is interpreted. If this description is sensitive to the exact pixel values, the effect of noise is directly accepted. Therefore, choosing a good feature description is very important. The proposed MSURF descriptor achieves better feature extraction by handling noise with its weighted Gaussian kernel.

3.3.2. A-KAZE feature detection and descriptor algorithm

A) Feature detection:

The accelerated version of KAZE is A-KAZE which significantly improves the feature extraction and description phases of KAZE. KAZE constructs a nonlinear scale space as opposed to applying Gaussian blurring, much like SIFT extraction. When A-KAZE is smoothened to an equal level of noise and detail, it also increases localization accuracy and uniqueness. A Hessian matrix is introduced in extracting A-KAZE features and it is mathematically represented as shown in Eq. (5) and its scaling factor is given in Eq. (6). Hessian matrix is a symmetric matrix that holds some key information about the function being optimized and its dimension is always equal to the number of variables in a function. For example, the Hessian matrix will be a 3×3 dimension matrix, if the function consists of 3 variables.

$$L^i_{Hessian} = \sigma^2_{i,norm}(L^i_{xx}L^i_{yy} - L^i_{xy}L^i_{xy}) \tag{5}$$

$$\sigma^2_{i,norm} = \frac{\sigma_i}{2^{o^i}} \tag{6}$$

Where, $\sigma^2_{i,norm}$=normalized scale factor is given by Eq. (5), L^i_{xx}=horizontal derivatives, L^i_{yy}=vertical derivatives and L^i_{xy}= second-order cross derivatives.

The extreme points of this matrix are detected in the $3 \times 3 \times 3$ neighborhood between both the 3×3 rectangle windows and the current scale. If the identified point value and its Hessian value are more than the pre-threshold TA-KAZE, it is considered a key point. To ensure that A-KAZE features are rotation invariant, the principal orientation can be discovered by searching a radius of $6\sigma_i$ along with a sampling step σ_i. This method uses the extreme point as the neighborhood's centrality. The first-order differential values of all the nearby points will be applied with a Gaussian weighting in a circle centered on the interesting point. These weighted values are considered the image's pixel response values. These total response values are added together with a sector region of $\pi/3$ in the sliding window. The orientation of the sector region with the highest value after completing the circle gives the primary orientation of the feature points.

B) Feature descriptor

The local difference Binary (LDB) is modified to describe features in the feature description phase. The

modified-local difference Binary (M-LDB) is used to ensure the rotation is invariant, the grids were subsampled in steps as a feature function instead of all pixel's mean value in each sub-division of the grid. A feature point-centered image patch is chosen and then divided into $q \times q$ grids of equal size to extract information from each grid that is representative. These pair of grids undergo binary test operation as shown in Eq. (7).

$$\bar{\omega}(F_{function}(i), F_{function}(j)) = \begin{cases} 1, & if\ \left((F_{function}(i) - F_{function}(j)\right) > 0, i \neq j \\ 0, & otherwise. \end{cases} \quad (7)$$

Where, $\bar{\omega}$ is binary constant.

$F_{function}(i)$ is the function used in extracting information from grade unit i as shown in Eq. (8).

$$F_{function}(i) = \{F_{intensity}(i), F_{dx}(i), F_{dy}(i)\}, \quad (8)$$

The gradient function $F_{dx}(i)$ for grid unit, i in region x is represented as shown in Eq. (9)

$$F_{dx}(i) = Gradient_x(i) \quad (9)$$

The gradient function $F_{dy}(i)$ for grid unit i in region y is represented as shown in Eq. (10)

$$F_{dy}(i) = Gradient_y(i) \quad (10)$$

Where, $Gradient_x(i)$ is the gradient of grid unit i in region x, and $Gradient_y(i)$ is the gradient of grid unit i in region y.

$F_{function}(j)$ is the function used in extracting information from grade unit j which is identified as shown in Eq. (11).

$$F_{function}(j) = \{F_{intensity}(j), F_{dx}(j), F_{dy}(j)\}, \quad (11)$$

The gradient function $F_{dx}(j)$ for grid unit j in region x is represented as shown in Eq. (12)

$$F_{dx}(j) = Gradient_x(j) \quad (12)$$

The gradient function $F_{dy}(j)$ for grid unit j in region y is represented as shown in Eq. (13)

$$F_{dy}(j) = Gradient_y(j) \quad (13)$$

The pixel values of both grid units i, j for the $F_{function}(i)$ and $F_{function}(j)$ are represented as shown in Eq. (14).

$$F_{intensity}(i) = F_{intensity}(j) = \frac{1}{m}\sum_{k=1}^{m} Intensity(k) \quad (14)$$

Where, m is the number of total pixels in grid units i and j, $Intensity(k)$ is the pixel value.

3.4 Feature matching

To match the corresponding extracted features, RANSAC algorithm is employed in the feature matching stage. The affine transformation is then applied to determine the homographic matrix parameters as described in the 3.4.1 section. Because the matched points are generally more, compared to the amount of matrix unknown parameters, then an overdetermined matrix is formed. Singular value decomposition (SVD) is used to solve this matrix, and the right singular matrix value is considered as the final homographic matrix coefficients. Affine transformation is only one of several feature-matching techniques available, including projective transformation, sparse, and guided local features. In fact, as a linear transformation, affine mapping can handle translation, rotation, and scaling at the same time.

3.4.1. Affine transformation:

The attached forged regions are continuously exposed to scaling and rotation which are said to be distortions techniques, before moving from one region to another region within the same image. The distortion is represented as an affine transformation of image coordinates in the mathematical form. $x = (x, y)^T$ and $\tilde{x} = (\tilde{x}, \tilde{y})^T$ are represented as copied region coordinates and pasted region coordinates. The relation between these two coordinates is represented in Eq. (15).

$$\begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \rightarrow \begin{pmatrix} \tilde{x} \\ \tilde{y} \\ 1 \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & x_0 \\ t_{21} & t_{22} & y_0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \rightarrow \tilde{X} = TX \quad (15)$$

Where (x_0, y_0)=shift vector, (x, y)=coordinates of the copied region, $(\tilde{x}, \tilde{y})$=coordinates of the pasted region, $t_{11}, t_{12}, t_{21,}\ and\ t_{22}$ are the affine transformation parameters. A commonly used

approach to calculate the affine transformation matrix T is RANSAC, which accomplishes high accuracy even when the input data contains many mismatched pairs. T requires minimum of three corresponding non-collinear coordinate pairs. After feature extraction, using the mismatched features, the below-listed steps are performed for N times.

- The three non-collinear coordinates are considered randomly and based on these chosen point pairs, the T value is estimated by minimizing the objective function as shown in Eq. (16).

$$L(T) = \sum_{i=1}^{N} \left\| \widetilde{X}_i - TX_i \right\|_2^2 \quad (16)$$

- Using this estimated matrix T, all the obtained matched point pairs are divided into outliers and inliers. If $\left\| \tilde{X} - TX_i \right\|_2 \leq \varepsilon$, the matched point pairs $\{x, \tilde{x}\}$ belongs to the inlier group. The iterations (N) and the evaluation error (ε) are set to a maximum of N=1000 and $\varepsilon = 10^6$.

3.5 Objects catalog

The forged regions are tested on the original images and are categorized into different objects in this catalog. The objects catalog is a type of profile that consists of different image attributes like height, pixel size etc. The objects are profiled based on their similar attributes and this process is carried out after hybrid SURF feature extraction following image segmentation. A CCL approach is used for image segmentation, where the image is segmented to detect the objects and categorize them.

3.6 Object matching

Following the creation of the items' catalogue, the copy-move forgery is found via a matching process. There are two stages to the matching process. All of the objects in the objects' catalogue are compared to one another in the initial matching step to find comparable objects. All images labeled as original are subjected to the refine matching test to ensure image originality, with a second stage set aside to further refine the results.

3.6.1. Matching stage

The objects are compared to one another during the matching stage. These comparisons are carried out using a similarity threshold of 0.6 and the Euclidean distance among the extracted features that were matched. A copy-move forgery object table is formed when two or more similar items are discovered [19, 20]. All possible copied and relocated objects are listed in this table. These CMFD images are either real, or their resemblance is the result of their intersection zones. To find crossed items, the object table of copy-move forgery is searched. To see if there is an intersection between these items, the position (x, y) of each object's four corners is compared to the four corners of other objects. These intersecting items are consequently taken from the table.

If the table still has candidate items after the intersected objects have been removed, the image is recognized and labeled as a forged image, and the table's remaining objects are the forged areas. If not the image is designated as an original and undergoes the process of refining matching stage.

3.6.2. Refine matching stage

The images that have been put forth as being original are now put through a second matching process. This is a refining stage, in which the system performance is enhanced by applying an originality check to the images.

The candidate original images are subjected to different close and open morphological treatments. The boundaries of objects are smoothed using both closed and open morphological techniques. By removing small and thin parts, open morphological operations tend to smooth the outlines of the objects [21]. Additionally, it eliminates the shadowed pixels along object borders. While near morphological operations tend to enhance and fill in the tiny, thin holes that exist along the margins of the objects, smoothing their features. The approach of using CCL is employed in identifying objects individually in both closed and opened images. The intersected and nearby items are then combined when the two segmented images are linked. By combining regions produced by the two morphological procedures, the suggested algorithm will add more spatial regions to the image.

Following the extraction of SURF descriptors from the identified objects, a new objects catalogue is created. All of the items in the new catalogue reach the matching stage, and the related items are arranged in a copy-move object table. The tested image is classified as original if the table is empty. Otherwise, if there are any crossovers among the identified objects in the table, those objects are again investigated and will be eliminated from the table. The image is unquestionably original if the copy-move objects table is empty; otherwise, the detected objects table is once more examined to see if there is

any object intersection. If an intersection exits, those objects are removed from the table and the copy-move forgery table is once again examined. If the table is empty, the image is said to be original, otherwise, it is designated as forgery, with the fraud regions remaining in the table.

4. Results

The evaluation of the proposed CMFD method in terms of performance metrics like precision, accuracy, F1-score, TPR, and FPR are illustrated in this section. The implementation is done on a system with Intel core i7, a 64 bits' processor, and 8 GB RAM, and operates with the software tool MATLAB R2018a.

Precision is the most important performance measure that calculates the similarity measure of the obtained values and is calculated using Eq. (17)

$$Precision = \frac{TP}{TP+FP} \times 100 \quad (17)$$

Accuracy is the ratio of prediction of true observations to the total observations as shown in Eq. (18)

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (18)$$

F1-score is determined as the harmonic mean value of methods' recall and precision as shown in Eq. (19)

$$F1-score = \frac{2TP}{2TP+FP+FN} \times 100 \quad (19)$$

TPR is the possibility of predicting accurate positive class as shown in Eq. (20)

$$TPR = \frac{TP}{TP+FN} \times 100 \quad (20)$$

FPR is the possibility of predicting incorrect positive classes which is calculated mathematically as shown in Eq. (21)

$$FPR = \frac{FP}{FP+TN} \times 100 \quad (21)$$

Where, TP, FP, TN, and FN represent True Positives, False Positives, True Negatives, and False Negatives.

4.1 Quantitative evaluation

The proposed CMFD method uses modified SURF with A-KAZE feature descriptor on the MICC-F220, MICC-F2000, and CoMoFoD datasets. Various feature extraction was used in the existing research, out of which some of the feature extractors like SURF (speeded up robust feature), A-KAZE (accelerated KAZE), SIFT, and BRISK (Binary robust invariant scale key points) are compared in this section with the proposed Hybrid MSURF and A-KAZE feature extractor. Table 1 represents the effectiveness of these techniques in terms of accuracy, precision, and F1-score. The proposed feature extraction achieves better results compared to the other feature extraction techniques. The SURF feature extractor achieved an accuracy of 96.30%, precision of 95.64%, and F1-score of 94.35%. A-KAZE achieved an accuracy of 97.91%, precision of 96.45%, and F1-score of 97.56%. SIFT achieved an accuracy of 98.23%, precision of 97.76% and F1-score of 96.39%. BRISK achieved an accuracy of 98.76%, precision of 97.45% and F1-score of 96.21%. The graphical representation of table 1 parameters is shown in Fig. 4.

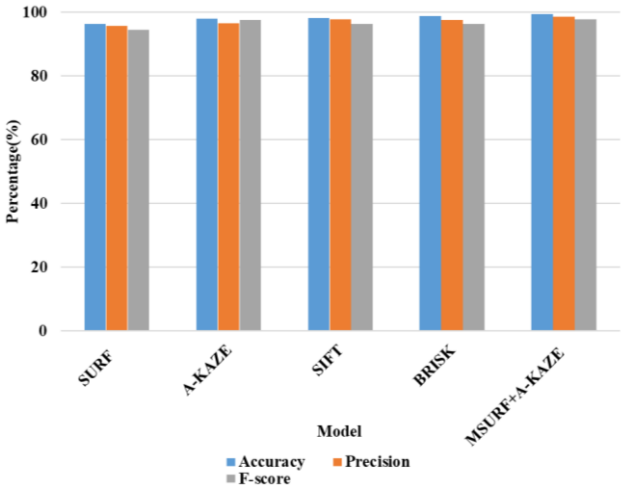

Figure. 4 Performance metrics analysis of various CMFD methods

The comparison of TPR and FPR of existing feature extraction methods are compared with the proposed feature extraction method on the MICC-F220 data and represented in Table 2. The graphical representation of these results is shown in Fig. 5. The proposed method MSURF and A-KAZE shows better results with TPR of 99.93%, and FPR of 4.67%. Whereas, the existing method SURF shows TPR of 82.73%, FPR of 10.71%, and A-KAZE shows TPR of 87.16%, and FPR of 9.96%. Other approaches like SIFT achieved TPR of 92.05%, and FPR of 7.71% and BRISK achieved TPR of 97.94%, and FPR of 6.02%.

Table 1. Comparison of different feature extraction algorithms on MICC-F220 dataset

Method	Dataset	Accuracy (%)	Precision (%)	F1-score (%)
SURF	MICC-F220	96.30	95.64	94.35
A-KAZE		97.91	96.45	97.56
SIFT		98.23	97.76	96.39
BRISK		98.76	97.45	96.21
MSURF+A-KAZE		99.46	99.93	98.21

Table 2. Comparative analysis of prediction outcomes with existing methods on MICC-F220 dataset

Method	Dataset	TPR (%)	FPR (%)
SURF	MICC-F220	82.73	10.71
A-KAZE		87.16	9.96
SIFT		92.05	7.71
BRISK		97.94	6.02
MSURF+A-KAZE		99.93	4.67

Table 3. Comparative analysis of existing CMFD methods on MICC-F220 dataset

Method	Dataset	Precision (%)	F1-score (%)
mDBSCAN [11]	MICC-F220	98.35	97.13
DBSCAN [12]		95.64	95.96
MSURF + A-KAZE		99.93	98.21

Table 4. Comparative analysis of existing CMFD methods on MICC-F2000 dataset

Method	Dataset	Precision (%)	F1-score (%)
mDBSCAN [11]	MICC-F2000	96.83	96.03
DBSCAN [12]		99.90	94.33
MSURF + A-KAZE		99.93	98.21

Table 5. Comparative analysis of existing CMFD methods on CoMoFoD dataset

Method	Dataset	Precision (%)	F1-score (%)
mDBSCAN [11]	MICC-F2000	98.35	93.36
DBSCAN [12]		95.98	93.54
MSURF + A-KAZE		99.93	98.21

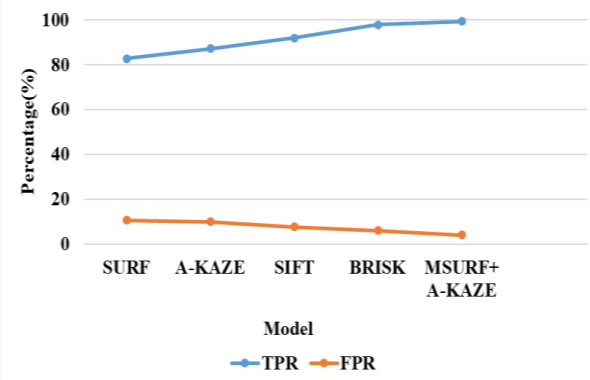

Figure. 5 Performance metrics analysis for prediction outcomes

4.2 Comparative analysis

The comparison of existing CMFD methods with the proposed CMFD method on the MICC-F220 data are represented in Table 3. The graphical representation of these results is shown in Fig. 6. The proposed CMFD method shows better results with the precision of 99.45% and F1-score of 98.21%. The evaluation of proposed method on MICC-F2000 is compared with existing methods in Table 4. The graphical representation of these results are given in Fig. 7. And also, the performance evaluation of the proposed on CoMoFoD dataset is compared with the existing methods in Table 5. These results are graphically represented in Fig. 8.

The proposed CMFD method over comes the limitation of existing CMFD method based on DHE-SURF features along with mDBSCAN clustering [11] and CMFD method based on SURF, BRISK features along with DBSCAN clustering [12]. In reference 11, the continuous phase of improvement and refinement caused more complexity in handling post-processing attacks which was the drawback of this method. In reference 12, the experimental results have shown that more false matches were detected, which is a limitation of this method. To overcome the continuous refinement and to obtain les false matches, a Modified Hybrid SURF is proposed with A-KAZE feature descriptor and detector which achieved high performance and less computing.

Table 6. Analysis of prediction outcomes with existing methods on MICC-F220 dataset

Method	Dataset	TPR (%)	FPR (%)
mDBSCAN clustering [11]	MICC-F220	98.26	6.03
DBSCAN clustering [12]		98.05	7. 31
MSURF +A-KAZE		99.93	4.67

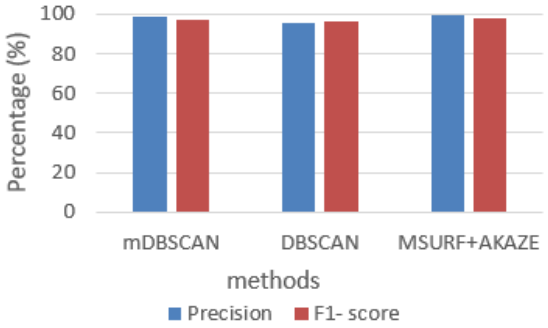

Figure. 6 Performance metrics analysis of various CMFD methods on MICC-F220 dataset

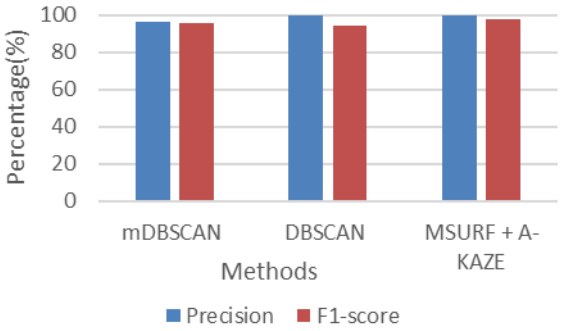

Figure. 7 Performance metrics analysis of various CMFD methods on MICC-F2000 dataset

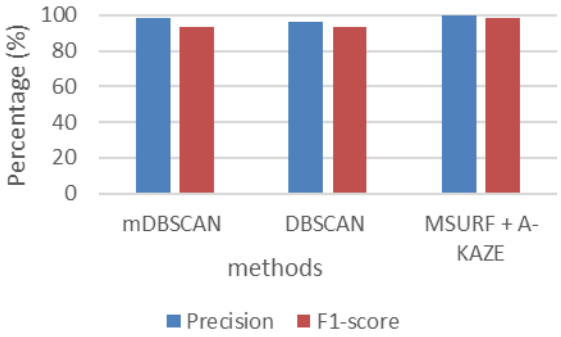

Figure. 8 Performance metrics analysis of various CMFD methods on CoMoFoD dataset

The comparison of TPR and FPR of existing CMF methods are compared with the proposed CMFD method on the MICC-F220 data and represented in Table 6. The graphical representation of these results are shown in Fig. 9. The proposed method achieves better results with TPR of 99.93%, and FPR of 4.67%. Whereas, the existing method referecnce 11 shows 98.26% shows TPR of 98.26%,

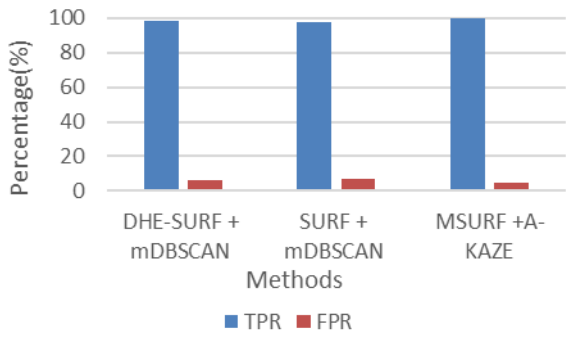

Figure. 9 Performance metrics analysis for prediction outcomes

and FPR of 6.03% and reference 12 shows TPR of 98.05% and FPR of 7.31%.

5. Conclusion

A novel hybrid feature extraction using MSURF features with an A-KAZE descriptor and detector algorithm is implemented in the proposed CMFD method. The required points in the smoothened regions are acquired by adjusting the lowest threshold values rather than A-KAZE and SURF's default values. This method can detect tampered regions within a forged image, even in smooth regions. The performance evaluation of the proposed CMFD method is validated on MICC-F220 and surpasses the existing DNN method of CMFD. The proposed method achieved the highest values in terms of Precision of 99.93%, F1-score 95.96%, TPR of 99.93%, and FPR of 4.67%. The proposed method is validated only on MICC-F220 dataset which consists of 110 tampered images and 110 original images. Another dataset like MICC-F2000 consists of more tampered and original images, which can be used for future research to check the effectiveness of the proposed CMFD method for large-size dataset.

Notation list

Parameters	Notation
G_x and G_y	Gradient intensity of pixels in orientation x and y
L_x and L_y	First order derivatives of greyscale image L
$F_{function}(i)$	function for extracting information from grade unit i
$F_{dx}(i)$	The gradient function for grid unit i in region x
$F_{dx}(j)$	The gradient function for grid unit j in region x
m	number of total pixels in grid units i and j
$Intensity(k)$	pixel value.
(x_0, y_0)	shift vector
(x, y)	coordinates of the copied region
$(\tilde{x}, \tilde{y})$	coordinates of the pasted region
$t_{11}, t_{12}, t_{21,}$ and t_{22}	affine transformation parameters.
T	Estimated matrix
ε	Evaluation error
N	Maximum iterations

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

References

[1] M. A. Elaskily, H. A. Elnemr, M. M. Dessouky, and O. S. Faragallah, "Two stages object recognition based copy-move forgery detection algorithm", *Multimedia Tools and Applications*, Vol. 78, No. 11, pp. 15353-15373, 2019.

[2] J. Yang, Z. Liang, Y. Gan, and J. Zhong, "A novel copy-move forgery detection algorithm via two-stage filtering", *Digital Signal Processing*, Vol. 113, p. 103032, 2021.

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

[4] G. Tahaoglu, G. Ulutas, B. Ustubioglu, and V. V. Nabiyev, "Improved copy move forgery detection method via L* a* b* color space and enhanced localization technique", *Multimedia Tools and Applications*, Vol. 80, No. 15, pp. 23419-23456, 2021.

[5] G. S. Priyanka, and K. Singh, "An improved block based copy-move forgery detection technique", *Multimedia Tools and Applications*, Vol. 79, No. 19, pp. 13011-13035, 2020.

[6] J. Y. Park, T. A. Kang, Y. H. Moon, and I. K. Eom, "Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram", *Symmetry*, Vol. 12, No. 4, p. 492, 2020.

[7] S. Dhivya, J. Sangeetha, and B. Sudhakar, "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique", *Soft Computing*, Vol. 24, No. 19, pp. 14429-14440, 2020.

[8] F. M. A. Azrak, Z. F. Elsharkawy, A. S. Elkorany, G. M. E. Banby, M. I. Dessowky, and F. E. A. E. Samie, "Copy-move forgery detection based on discrete and SURF transforms", *Wireless Personal Communications*, Vol. 110, No. 1, pp. 503-530, 2020.

[9] P. Niu, C. Wang, W. Chen, H. Yang, and X. Wang, "Fast and effective Keypoint-based image copy-move forgery detection using complex-valued moment invariants", *Journal of Visual Communication and Image Representation*, Vol. 77, p. 103068, 2021.

[10] R. Agarwal, and O. P. Verma, "An efficient copy move forgery detection using deep learning feature extraction and matching algorithm", *Multimedia Tools and Applications*, Vol. 79, No. 11-12, pp. 7355-7376, 2020.

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

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

[13] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. E. Banby, O. A. Elshakankiry, A. A. M. Khalaf, H. K. Aslan, O. S. Faragallah, and F. E. A. E. Samie, "A novel deep learning framework for copy-moveforgery detection in images", *Multimedia Tools and Applications*, Vol. 79, No. 27, pp. 19167-19192, 2020.

[14] Y. R. Ortega, D. M. Ballesteros, and D. Renza, "Copy-move forgery detection (CMFD) using deep learning for image and video forensics", *Journal of Imaging*, Vol. 7, No. 3, p. 59, 2021.
[15] H. Kasban, and S. Nassar, "An efficient approach for forgery detection in digital images using Hilbert–Huang transform", *Applied Soft Computing*, Vol. 97A, p. 106728, 2020.
[16] A. Hegazi, A. Taha, and M. M. Selim, "An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal", *Journal of King Saud University-Computer and Information Sciences*, Vol. 33, No. 9, pp. 1055-1063, 2021.
[17] R. Agarwal, and O. P. Verma, "Robust copy-move forgery detection using modified superpixel based FCM clustering with emperor penguin optimization and block feature matching", *Evolving Systems*, Vol. 13, No. 1, pp. 27-41, 2022.
[18] J. L. Zhong, C. M. Pun, and Y. F. Gan, "Dense moment feature index and best match algorithms for video copy-move forgery detection", *Information Sciences*, Vol. 537, pp. 184-202, 2020.
[19] J. Varghese and C. S. Kumar, "Robust copy-move forgery detection algorithm using singular value decomposition and discrete orthonormal Stockwell transform", *Australian Journal of Forensic Sciences*, Vol. 52, No. 6, pp. 711-727, 2020.
[20] 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, No. 3, pp. 857-883, 2020.
[21] M. U. Devi, and U. R. Babu, "Grey wolf assisted SIFT for improving copy move image forgery detection", *Evolutionary Intelligence*, Vol. 15, No. 2, pp. 1097-1108, 2022.