RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt26312

Copy-Move Image Forgery Detection via Weighted Multi-Similarity Matching and Adaptive Thresholding

Chalamalasetty Sai Pratheek [a, *], Giduturi Srinivasa Rao [b]

[a] Department of Artificial Intelligence and Data Science, GITAM School of Computer Science and Engineering, GITAM, Visakhapatnam, Andhra Pradesh 530045, India.

[b] Department of Computer Science and Systems Engineering, GITAM School of Computer Science and Engineering, GITAM, Visakhapatnam, Andhra Pradesh 530045, India.

* Corresponding Author Email: schalama@gitam.edu

DOI: https://doi.org/10.54392/irjmt26312

Received: 04-12-2025; Revised: 16-04-2026; Accepted: 27-04-2026; Published: 15-05-2026

Abstract: One popular digital image forgery technique for identifying regions of image forgery is Copy-Move Forgery Detection (CMFD). Copy-move forging is the procedure of attaching a specific section of an image to a new element of an identical image to replicate the forged image elements as an original. The fake appears realistic because the image preserves all the fundamental characteristics of the original image, even after its creation in the target region. Because editing tools and image capture have been more widely available, the quantity of phony photographs on the internet has exploded. Further, social media and other networks have emerged as the primary means of distributing modified photos, rumors, fake news, and other such content. Therefore, creating efficient methods for identifying these forgeries has become crucial. The Copy Move Forgery (CMF), which uses the patches inside the image to change it, is among the most prevalent kinds of forgeries. Deep structured learning-based methods generally perform better but have a focus on generalization. Besides feature matching, this paper also proposes a new deep-learning algorithm to detect forgeries. First, the images from the standard dataset are collected. Preprocessing methods include Retinex and Contrast Limited Adaptive Histogram Equalization (CLAHE) are applied. Further, each of the collected images is subjected to post-processing to improve image effectiveness. The pre-processed images are then fed into an Efficient Convolutional Transformer with Spatial Attention Network (ECT-SANet) for feature extraction. Then we perform the feature matching operation using the Weighted Multi-Similarity Check (WMS) method. The Adaptive Threshold is optimized by Randomized Improved Orca Predation Algorithm (RE-OPA). The matched features are then filtered for false-positives using a Random Sample Consensus (RANSAC) algorithm. The performance of the proposed approach is evaluated in terms of the CMFD.

Keywords: Copy-Move Forgery Detection, Contrast Limited Adaptive Histogram Equalization, Efficient Convolutional Transformer with Spatial Attention Network, Weighted Multi-Similarity Check and Adaptive Thresholding, Randomized Enhanced Orca Predation Algorithm.

1. Introduction

Photoshop, 3D Max and other editing programs have made manipulation of images easy to with the assistance digital graphics tools freely available today. Digital communicative media such as images are an integral part of our daily lives [1]. Because they are easy to modify, this raises the question questioned, especially when it is used as evidence in court cases, to pursue insurance claims, or in scientific research [2]. Fake numbers are common, however, according to some publications, serious doubts have been raised about image alteration [3]. Different algorithms have been proposed to determine whether a given image has been modified from its original form, on detecting CMF, which is the result of pasting and copying a part of one image to another [4].

To detect forgeries two types of visual forensic methods are used: active detection and passive detection [5]. In passive procedures the image itself is not known in advance, active strategies do such as digital signatures [6] or integrated watermarks [7], common passive watermarking techniques have been considered in many contexts [8]. In particular, CMF is one of the most often used forms of image alteration [9]. Both the forged and unaltered information appear the same and hence it can be challenging to do forensics on these images. Block-based or keypoint-based methods are also used. In customary CMF detection methods [10], computing the Discrete Wavelet Transform (DWT)

or the Discrete Cosine Transform (DCT) the image's data is split into smaller parts and features are extracted in a block by block process approaches [11]. In contrast, keypoint-based approaches detect keypoints first and then use their features to classify similarities [12]. These methods cannot cope with more complex forgeries or more advanced post-processing techniques, irrespective of whether they perform well [13].

Customary block-based and keypoint-based methods have a number of advantages such as being able to achieve a higher degree of detecting identical regions by identifying matching key features, and easily separate images into smaller sections [14]. These methods are simple, yet these techniques struggle to detect more subtle or elaborate changes, such as those in complex forgeries with integrated components or post-processing steps [15]. These restrictions can be exploited by an alternative option that resolves problems with existing proposals, while improving their benefits, is also presented. [16]. This approach can benefit from many of the advantages of the standard methods with added assurance. To detect and locate identical areas in complex and post-processed images in this way [17]. Therefore, CMF is successfully improved and a more reliable and thorough image forensics method is developed in this work.

1.1 Contribution

Deep learning model-based advanced techniques to detect copy-move image forgeries in digital images is presented in this research. The model successfully identifies overlapping areas even after new feature extraction and learning methods are applied. This method improves digital forensics overall by providing reliable evaluation and timely detection of the modified content.

- To model the highly unpredictable reconfiguration patterns in CMFD, a deep learning-based approach is adopted. High-dimensional images are useful for the system to learn its own nonlinear properties, spatial feature, redundancy and contextual signals, the system efficiently discovers duplicated regions, and can easily adapt to any post-processing changes, as well as the efficiency, flexibility and precision of the forgery detection systems. Resilience, accuracy, precision, flexibility in a range of imaging contexts are greatly enhanced.
- To improve the effectiveness of CMFD, an ECT-SA Net is used in the feature extraction step, which combines convolutional layers with transformer-based attention to identify local as well as global features. It improves detection accuracy, reduces computational load, and enables real-time image recognition that is both scalable and transformation-resilient. forgery detection by focusing on critical regions.
- To promote better matching of features in CMFD, we have developed a novel search technique called RE-OPA. To create equilibrium between exploration and exploitation, the algorithm can correctly detect the rehearsed regions in randomized optimization. It allows for a reduction in computational burden while verifying the true location of the forgery efficiently identifying the most appropriate matching regions in the modified image.
- To improve the feature matching process, the WMS-AT technique is employed in CMFD. For a reliable comparison, it leverages adaptive weighting to integrate several similarity measures. By constantly adjusting in response to image properties, adaptive thresholding improves the detection of subtle or modified duplicate regions, reduces false positives, and provides accurate forgery localization.

1.2 Organization

The organization of the research work is explained in this section. The literature review is presented in Section II. Section III motivates the significance of detecting copy-move image forgery along with the novel depiction of the developed approach; Section IV shows the explanation of the hybrid image pre-processing and spatial attention-based feature extraction process on the collected images; Section V elaborately elucidates the Multi-Similarity check-based feature matching using the randomized optimization algorithm infused with false match detection, and Section VII provides the conclusion of the research.

2. Literature Survey

2.1 Related Works

In 2023, Maashi *et al.* [18] have proposed a Reptile Search Algorithm with a Deep Transfer Learning (RSADTL)-based CMFD method using Neural Architectural Search Network (NASNet) to effectively extract features for CMFD. Extreme Gradient Boosting (XGBoost) was integrated to determine whether a portion of an image is legitimate or not. Hence, the model's efficacy is improved, providing precise forgery detection.

In 2023, Khalil *et al.* [19] proposed an innovative method to improve digital image forgery detection by deploying a Deep Neural Network (DNN) to detect two types of forgeries. The method depended on determining the compression quality of forged and original portions. Therefore, experimental results

demonstrated that the usage of pre-trained models performed better than state-of-the-art techniques.

In 2024, Diwan and Roy *et al.* [20] have detected and localized copy-move fraud in digital images by combining Convolutional Neural Network (CNN) architecture with CenSurE keypoint (CSK) detection. This adequately handled geometrical transformations by integrating key points with CNN characteristics. Hence, the proposed model provided a strong and dependable solution for multimedia forensic applications.

In 2023, Diwan *et al*. [21] proposed a CMFD method based on the SuperPoint keypoint detector. This method Dependability traits were also present in numerous facially intrusive images, where facial features remained constant across multiple images, making them useful for image forensics. and authenticity verification because it presented a practical method for identifying forgeries in a broad spectrum of digital images.

In 2023, Rao *et al*. [22] presented an image tampering detection approach which integrates Transformer Decoding. Residual Network layers (RN-TD) were utilized. The model was tested on the NIST, CASIA, and IMD2020 datasets. As a result, it was concluded that they were highly accurate and reliable in identifying image fraud.

In 2023, a thorough literature review of CMF was conducted by Abdulwahid *et al.* [23], with an emphasis on Principle Component Analysis (PCA). This method is often used to hide data in an image by copying a section of an image into another area. the rising challenges posed by image legitimacy, indicating that these outcomes could be useful in strengthening the privacy of images in connection with forensic and safeguarding the public

In 2023, Alhaidery *et al*. [24] proposed a fast multi-stage method by incorporating Speeded-Up Robust Features (SURF) and Histogram of Oriented Gradients (HOG) detection on Simple Linear Iterative Clustering (SLIC) segmentation. This indicated superior CMFD, localization, and classification performance. Ultimately, this outcome highlights the importance of adaptability, rapidity, and efficiency of cybercrime detection.

In 2024, Al-Shamasneh and Ibrahim *et al*. [25] proposed a hybridization detection approach based on convex sets and deep features derived from Sonine functions. It was based on Support Vector Machine (SVM) classification, extraction, distinguishing between real and fake images, producing better detection rate of the quality of the produced images which in turn improving overall accuracy.

2.2. Problem statement

CMFD is a pixel-based digital forensic method using advanced pattern recognition techniques to detect manipulation. It identifies more complex manipulations, including small ones, in contrast to customary detectors, by verifying the reliability of digital images and reduces the hazards associated with undiscovered forgeries. This technology is employed in numerous industries including forensics.

- Transformations and proximity of replicated parts make CMFD detection difficult. Deep learning networks have decreased the necessity for human feature engineering by automatically removing discriminatory characteristics from data. These models enable accurate identification of manipulated locations by improving detection trustworthiness and flexibility.
- Other problems may arise because they are sometimes hard to detect, due to their shape and/or the condition of the forged parts. The attention approach gives important portions of the image weights, thus enabling the model to focus on specific parts that seem problematic. This targeted emphasis improves the model's ability to distinguish between areas of tampered images and original ones, thus improving the generalization, reliability and precision of localization.
- Global dependencies are essential for finding forgeries but are difficult to model using customary approaches effective at identifying local patterns; the convolutional layers are combined to create transformer blocks to address this problem. This hybrid design improves the system's tolerance to forging problems by identifying redundant information under complex transformations.
- Local minima and low convergence speed make training deep models for forgery detection challenging. Optimization techniques solve this via adjusting the learning rate with the first and second moments of the gradients. Thus, these techniques improve the quality of detection results by making the network more sensitive to generalize within a variety of forging patterns.

In this study, a deep structured learning-based method is developed for the suggested detection system to tackle these issues.

Table I lists the properties and limitations of conventional copy-move image forgeries

Table 1. Features and Challenges of Traditional Copy Move Image Forgery

Author [citation]	Methodology	Features	Challenges
Maashi *et al.* [18]	RSADTL-CMFD	• It employs deep models to learn complex features, focusing on detection of subtle and sophisticated forgeries. • It reviews multiple benchmark datasets and metrics giving a structured evaluation to compare various CMFD techniques.	• Majority of the methods performed well on synthetic data and performed poorly when subjected to real-world data with varied transformations. • There is no uniform evaluation strategy or consistent dataset annotation making comparison even tougher.
Khalil *et al.* [19]	DNN	• They proposed a hybrid real world model which detects CMFD and splicing at same time. • The model uses transfer learning approach which reduces training time and computation cost, offering higher detection rates.	• The employed deep models require significant CPU, memory leading to resource limitations. • The overall accuracy reduced slightly when multiple forgery types are detected
Diwan and Roy *et al.* [20]	CNN-CSK	• It uses a 2-stage hybrid model using CenSurE key point detection coupled with CNN. • It effectively handled geometric transformations and post-processing operations.	• The proposed model slightly struggled when combined and complex attacks were involved. • The model proved sensitive to the texture parameters of the images employed.
Diwan *et al.* [21]	Superpoint	• It is adaptable to a variety of forgery types due to its resilience to attacks like rotation and scaling. • It improves localization by producing dense and stable key points.	• It may be overlooked if training does not include representative tampering patterns. • Its features must be carefully scaled and matched to classification layers.
Rao *et al.* [22]	RN-TD	• It is made easier by modeling long-distance relationships across widely distant image portions. • The large-scale manipulation pattern is done by capturing the global context.	• It requires a lot of memory and computing power. • It is still challenging to distinguish genuine recurring patterns in complicated settings from fake ones.
Abdulwahid [23]	SVM-PCA	• It points out the field's present problems and unmet research needs, directing future advancements and enhancements. • It helps with comparison and the proper choice of methods by combining a variety of CMFD techniques.	• It does not provide any novel computational innovations or new research results. • It might become outdated as deep learning methods for detecting forgeries advance.
Alhaidery *et al.* [24]	SLIC-SURF	• It is designed to be robust against the effects of various image deteriorating and manipulating scenarios. • It renders it valuable in forensic applications because it offers both forgery detection and precise location.	• The problems with border localization can result from slight variations in region alignment. • It uses an extensive amount of processing resources, especially when interpreting high-resolution images or intensive localization.

Al-Shamasneh and Ibrahim [25]	SVM	• It enhances deep learning features by capturing tiny textural variations. • It increases the detection accuracy for splicing forgeries.	• The mixing of several feature categories may result in high-dimensional or redundant representations. • It performs worse if the features are not appropriately adjusted.

3. Significance Of Detecting Copy-Move Image Forgery along with the Novel Depiction of the Developed Approach

3.1 Significance of Detecting Copy-Move Image Forgery

In the period from 2023 to 2025, the new CMFD approaches mainly focused on deep learning models, particularly on transformer-based models to capture the global context and hybrid feature matching schemes due to the ability to capture long-range dependencies. For example, the work of Rao et al. leveraged these benefits and built upon this capability, and subsequent work such as TransCMFD have been successfully implemented. Hybrid approaches like ECT-SANet-combine convolutional neural networks with transformer attention to combine different methods of feature extraction and structural inference to improve detection performance.

However, they have high computational costs and low robustness against composite transformations (rotation, scale changes, compression, etc.) with no ability to behave differently when natural repetitive patterns are present in the images. Diwan and Roy proposed a new hybrid feature matching approaches that combine local descriptors with deep representations, such as CNN-keypoint fusion approaches based on graph-matching or optimization, still suffer from texture variability, low discrimination power, and a high false-positive rate with fixed (or suboptimal) similarity measures. Our proposed pipeline consists of the efficient convolution-transformer for fusion (ECT-SANet), a new weighted multi-similarity adaptive thresholding (WMS-AT) method to compute the suitability score based on multiple complementary similarities, the new optimization-driven parameter adaptation (RE-OPA) algorithm for fine-tuning the matching parameters to optimize the convergence and stability of the proposed method, and the geometric verification using the RANSAC to reject the false matches. The proposed modules tightly cooperate to improve the performance of the whole pipeline. The proposed solutions fill in many of the major deficiencies found in recent CMFD works such as robustness, false positives, and real-world complex attacks, linking transformer based global modeling and accurate hybrid feature matching for practical forensic CMFD applications.

This model has been developed and refined in the light of the increasing number of manipulated digital images and demand for accurate CMF detection. These demands exist due to CMF degrading the dependability of digital content, in fields like media, legal investigations, and digital forensics. Traditional methods may fail to identify complex forgeries. We can overcome these limitations with modifications in scale, rotation and compression. It can therefore be applied to combining reliable feature extraction techniques with deep learning, with the main goal of correctly identifying identical regions while minimizing false positives, particularly when the image is subject to heavy transformations. The detection results are easier to interpret and improves forgery localization by learning contextual and spatial relationships. The model achieves efficiency, and adaptability makes it a useful tool for ensuring the validity and reliability of visual data. Because it increases criminal accountability and social reliance are centered around image-based communication, making it vital for digital security.

3.2 Systematic Novel Depiction of the Developed Approach

The proposed model outperforms others in detection accuracy, resilience, and efficiency through a systematic and innovative approach. The input images taken out from a dataset should be meaningful as they influence the localization efficiency in CMFD and diverse examples of counterfeits were pre-processed using CLAHE and Retinex to improve contrast and visibility of the manipulated area of the image. Extraction of deep features of preprocessed images go through ECT-SANet for segmentation. The ECT-SANet identifies less obvious forging evidence by focusing on specific regions of the image using spatial attention. The retrieved features are subsequently combined using the WMS-AT to match extracted features by facilitating region correlation. To improve performance, the parameters such as weights and thresholds are optimized. In addition, the RANSAC technique is employed to detect false matches, verify geometric uniformity, and remove inaccurate or misleading matches. Therefore, the suggested model enhances forensic reliability and accuracy in the legitimacy of digital images by providing accurate detection, localization, and resilience to forgeries in CMD. The pictorial visualization of the proposed CMFD architecture is represented in Figure 1.

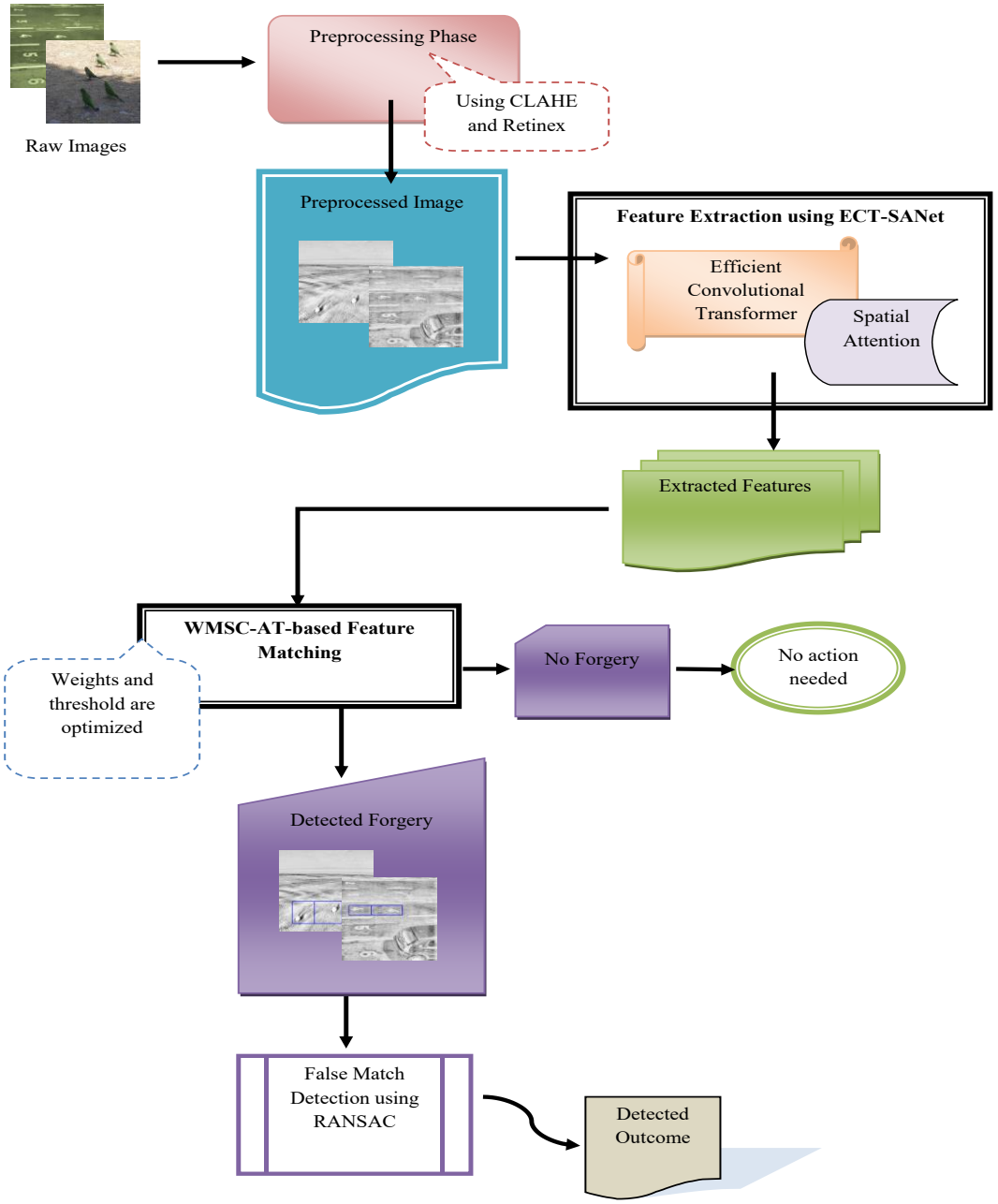


Figure 1. Schematic Illustration of Proposed CMFD Architecture

4. Hybrid Image Pre-Processing And Spatial Attention-Based Feature Extraction Process on the Collected Images

4.1 Collection of Images

The following section presents the dataset for the creation of the CMFD model.

Dataset 2 ("Copy-Move Forgery Detection"): The images related to forgery detection are obtained from the link http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/. Accessed on 2024-10-15. This dataset comprises both interfered and original images for the detection of fake images. Dataset-2 ("CoMoFoD - Copy-Move Forgery Detection Dataset"): The dataset can be accessed via the link below: "https://www.vcl.fer.hr/comofod/. Access date: 2025-10-15". This dataset offers original and forged images with ground truth, covering multiple forgery types and post-processing conditions. It is widely used for benchmarking copy-move forgery detection techniques.

The sample images of CMFD are portrayed in Figure 2. The raw image is depicted as D_F

4.2 Image Pre-processing

Initially, prevalent standard datasets were utilized to collect the raw images, D_F as input. By dividing the image into small parts and applying equalized histograms to each, CLAHE enhances the contrast of these input images without amplifying noise. This boosts transparency in low-light conditions and increases regional contrast.

Terms	Image-1	Image-2	Image-3	Image-4	Image-5
Dataset-1					
Image					
Dataset-2					
Image					

Figure 2. Sample Images of CFMD

The next phase is Retinex-based enhancement, which balances colour and brightness by estimating lighting and reflectance. In addition to enhancing visual clarity, this phase gets images ready for efficient feature extraction and therefore serves further image enhancements in the preprocessing process. The preprocessed Thus, by enhancing contrast and lighting balance, the integrated usage of CLAHE and Retinex improves image quality, thereby rendering image forgery analysis detection less inaccurate and consistent.

The pre-processed image results of CMFD are displayed in Figure 3. The pre-processed image is represented asPp_F.

4.3 Feature Extraction using ECT-SANet

The proposed feature extraction module incorporates the Efficient Convolution Transformer (ECT) and Spatial Attention Network (SANet) to facilitate rich local-global feature representation and spatial concentration. By using deep structured learning algorithms, this improves the accuracy of defect identification and anomaly categorization, enabling reliable, efficient CMFD.

Novelty: The preprocessed image, P_F obtained from the pre-processing phase, is fed into the ECT-SANet for the process of feature extraction. Here, the ECT [26] integrates CNN's local feature extraction with Transformer's global context modeling to increase the accuracy of classification tasks while reducing their computational cost. CNNs are essential to computer vision and are used extensively in fields including image identification, autonomous driving, and medical imaging. A basic CNN model was developed that begins with a Conv2D layer that extracts low-level features using 32 filters. In Eq. (1), the 2D convolution operation is represented.

$$Jk(h,v) = \sum\sum H(h+d, v+r) \cdot Kk(d,r) + gk \quad (1)$$

Here, the term H is the input, Kk is the convolutional kernel, gk is the bias, and Jk is the output feature map. The spatial dimensions are decreased via a max pooling layer, represented in Eq. (2).

$$W(h,v) = max\, J\, k(h+d, v+r) \quad (2)$$

Here, the term $W(h,v)$ represents the pooled output via selecting the maximum value in the area. More intricate patterns are captured by later layers with 64 and 128 filters.

After being flattened, the output is regularized by passing it through a dropout and a dense layer. 1D convolution is used to tabular data using Eq. (3).

$$Jh = \sum X\,(h+d, v+r) \times Ker(v) + bias \quad (3)$$

Here, the term Jh represents the output and$X$ represents the input vector. The transformers use self-attention to capture long-range dependencies; they were first developed for natural language processing. The definition of the unified multi-head attention is denoted in Eq. (4) and (5).

$$Mh(F,B,D) = [A(F_1, B_1, D_1), .. A(F_m, B_m, D_m)]W^s \quad (4)$$

$$A(F,B,D) = sftmx\left(\frac{FB^S}{\sqrt{l}}\right) \quad (5)$$

Here, the terms$F$,B, and Drepresent the query, key, and value metrics, F_1 , B_1 , and D_1 suggest the learnable projection matrix, and W^s represent the projection matrix outcome. The ECT provides a potent hybrid framework that improves feature representation and dramatically boosts classification performance by combining CNNs for local feature extraction and Transformers for global context modeling. The SANet [27] improves feature representation by concentrating on the most informative spatial regions by allocating attention weights to various areas within an input. This approach enables the model to perform better on tasks like object detection and image classification by prioritizing important areas.

.

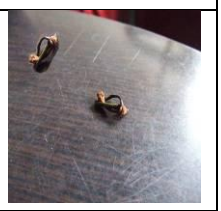
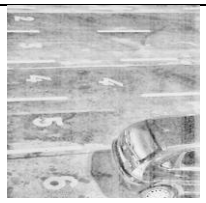
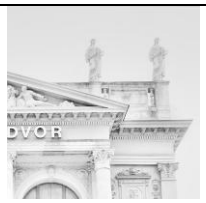
Terms	Image-1	Image-2	Image-3	Image-4	Image-5
Dataset-1					
Original Image					
Preprocessed Image					
Dataset-2					
Original Image					
Preprocessed Image					

Figure 3. Pre-processed Image Results of CFMD

As a result, the extracted feature, E_F are obtained from the ECT-SANet. The ECT-SANet architecture that results from integrating the ECT incorporates the use of the spatial emphasis from SAN, global context modelling from Transformers, and local feature extraction from CNNs Therefore, ECT-SANet is ideally suited for effective and reliable visual identification jobs since it offers high accuracy at a lower computational complexity. The schematic representation of feature extraction using ECT-SANet is depicted in Figure 4.

5. Multi-Similarity Check-Based Feature Matching Using the Randomized Optimization Algorithm Infused With False Match Detection

5.1 Development of RE-OPA

An improved RE-OPA is being developed to feature an innovative solution for CMFD detection optimization issues. The suggested method attempts to get over the limitations of traditional algorithms and improve the accuracy and robustness of duplicated region localization in complex images by effectively achieving a balance between exploration and exploitation.

Novelty: The established RE-OPA heuristic technique serves a significant role in improving the optimal parameter tuning for copy-move picture fraud detection. By updating the random number, the RE-OPA outperforms the conventional Orca Predation Algorithm (OPA). By improving the detection accuracy, resilience, and convergence in real-time image forgery identification tasks, these modifications tend to normalize the trade-off between exploration and exploitation.

The OPA [28] is a metaheuristic optimization algorithm inspired by the socio-behavioral, echolocation, and hunting activities of cooperative hunting tactics of orcas. The OPA mimics the orca's high level of intelligence, group cooperation, and sonar-based navigation capability that directs the search process in difficult solution spaces. To balance the exploration/exploitation trade-off, the algorithm incorporates a thorough set that simulates group behavior such as formation, communication through sonar clicks, and hunting techniques to obtain food enhancing the accuracy and convergence speed of the optimization algorithm. It is perfect for nonlinear fractional optimization. Hybridization with other methods, due to its simple structure and high degree of adaptability. To resemble communal behavior and initiate the optimization process.

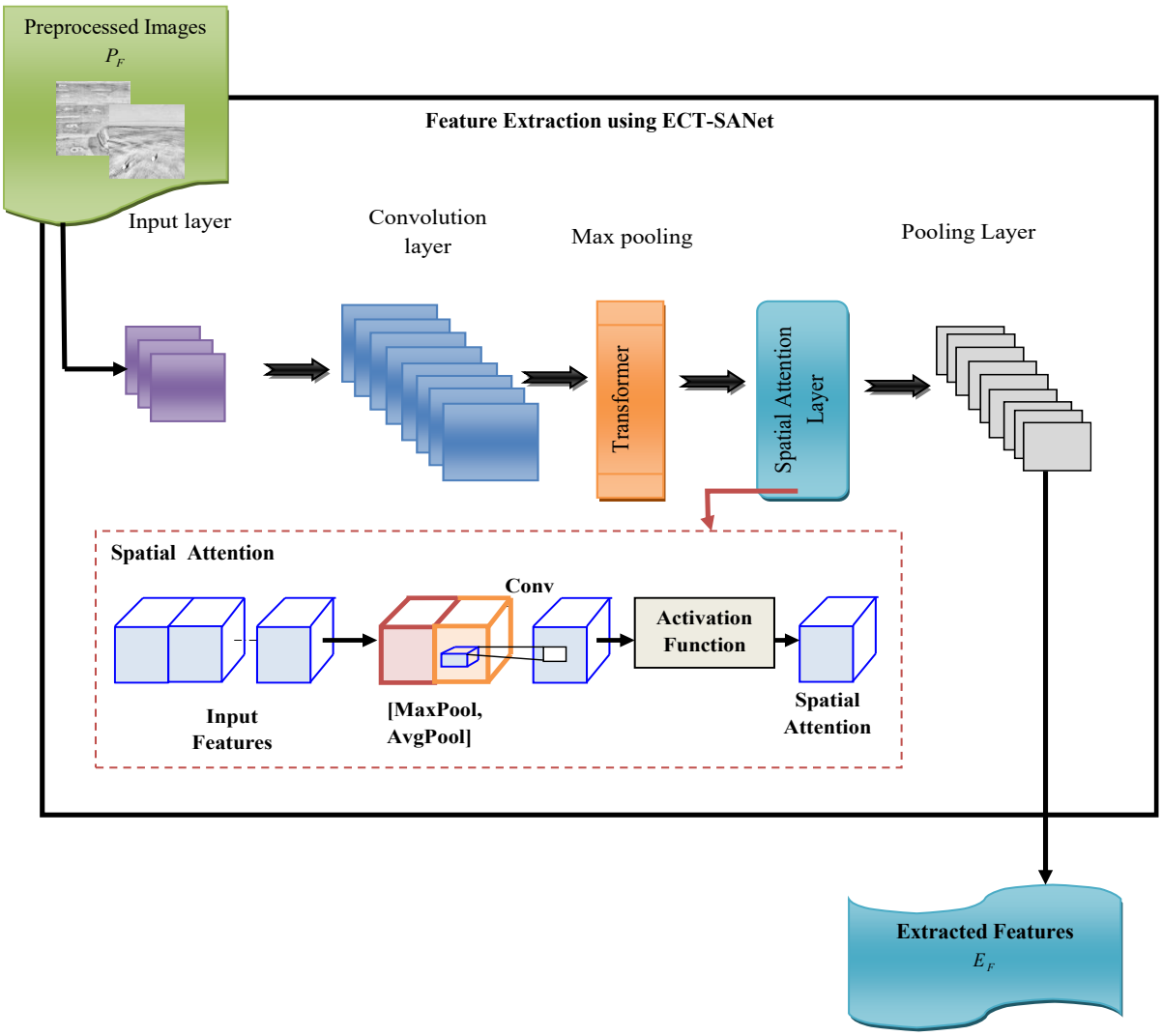


Figure 4. Schematic Representation of Feature Extraction using ECT-SANe

To this end, the movement of every orca is numerically determined by Eq. (6).

$$\delta_{ch,2,n} = rand \times (K_b - K_n) \quad (6)$$

Here, the term $\delta_{ch,2,n}$ Represents the chasing speed of the n^{th} orca, the term $rand$ denotes the random number between$[0,2]$, and the terms K_b and K_n represent the best solution position and the current position of the n^{th} iteration, respectively. The OPA can efficiently search the space owing to this movement, which guides orcas toward the best solution. Premature convergence, a major issue with the original OPA, is commonly brought on by the static random variable $rand \in [0,2]$ in Eq. (6), which restricts exploration in the early phases. To tackle this problem, the random value, $rand$in Eq. (6) is adaptively updated in the RE-OPA, and it is mathematically expressed in Eq. (7).

$$\delta_{ch,2,n} = \frac{Cf}{Bf+Wf} \times (K_b - K_n) \quad (7)$$

Here, the terms Ct, Bt, and Wt, illustrate the current fit, best fit, and worst fit values that are adaptively updated, respectively. The RE-OPA improves the original algorithm by eliminating premature convergence, strengthening search balance, providing better exploration and exploitation for faster, more accurate convergence to optimal solutions, and dynamically modifying control parameters. By accurately modifying random parameters, the proposed RE-OPA substantially improves detection performance in copy-move forging detection, providing reliable, real-time identification of modified regions while lowering computing overhead.

Therefore, it offers a dependable, flexible foundation for hybridization optimization in image forensics.

The pseudocode for the proposed RE-OPA is illustrated in Algorithm 1.

Algorithm: Pseudocode of the Developed RE-OPA

Begin RE-OPA

Input: Weights $E$and Threshold$C$

Output: Optimized parameters such as optimized weights E_o and optimized threshold C_o

Initialize position of orcas

Evaluate the fitness of every orca K_n

Identify current fitCt,best fit Bt, and worst fit Wt

Iterate the loop

For each orca $n = 1$to N:

The random number, $rand$ is updated using Eq. (7)

Compute adaptive chasing speed using Eq. (6)

Update position

Apply boundary constraints

Evaluate new fitness

End For

Update best and worst based on the new population

Store conventional metric

End loop

Return:

Best solution

Best fitness

End

5.2 *WMS-AT-based Feature Matching*

To improve CMFD, the weighted multi-scale evaluation and attention-based transformers are incorporated in the WMS-AT-based feature matching technique. It tackles difficulties, including noise, texturing similarities, and illumination fluctuations, aimed at improving matching resilience and precision. In practical fraud situations, this approach ensures accuracy and effectiveness.

Novelty: The proposed WMS-AT scheme, using an improved weighted multi-similarity technique, considers multiple aspects of similarity measures for the subsequent feature matching process such as assigning weights for the features, adaptive thresholds. Feature discrimination, reduction of false matches, and improvement of overall localization accuracy for forgery detection is done. The extracted features from ECT-SANet are fed as input into WMS-AT, a model that computes several similarity measures, including the Euclidean distance, Cosine similarity, Jaccard coefficient and Correlation coefficient. Each similarity metric is optimized for a given weight associated with the similarity type. The weighted multi-similarity score is then calculated using this weighted similarity tensor. The equation that calculates the weighted multi-similarity score is given by Eq. (8).

$$F = \underset{\{v_1,v_2,v_3,v_4,t\}}{\arg\min}\left(\left(\frac{1}{S}\right)*v_2\right)+v_1*E+\left(\frac{1}{J}\right)*v_3+\left(\frac{1}{C}\right)*v_4 \quad (8)$$

Here, in Eq. (8), the terms v_1, v_2, v_3, v_4, and t represent the optimized weight in Euclidean Distance, optimized weight in Cosine Similarity, optimized weight in Jaccard Coefficient, optimized weight in Correlation Coefficient, and match threshold, respectively. In the proposed model, similarities between each data point and every other data point are estimated. Its objective is to maximize Cosine Similarity S, Jaccard Coefficient J, and Correlation Coefficient C, which capture structural and semantic similarities that are essential for identifying duplicated regions while minimizing Euclidean Distance E, which maintains proximity in feature space. Furthermore, adjusting hyperparameters such as weights and thresholds increases the model's performance. The terms E, S, J, C are expressed in Eq. (9) to (12).

$$E = \sqrt{\sum_{v=1}^{b}(d_v - f_v)^2} \quad (9)$$

$$S = \frac{\sum_{v=1}^{b} d_v f_v}{\sqrt{\sum_{v=1}^{b} {d^2}_v^2}\cdot\sqrt{\sum_{v=1}^{b} {f^2}_v}} \quad (10)$$

$$J = \frac{|D \cap G|}{|D \cup G|} \quad (11)$$

Here, $|D \cap G|$and $|D \cup G|$denote the number of common terms and unique elements present across both sets of value of range 0 to1.

$$C = \frac{\sum_{v=1}^{b}(d_v-\overline{d})(f_v-\overline{f})}{\sqrt{\sum_{v=1}^{b}(d_v-\overline{d})^2}\cdot\sqrt{\sum_{v=1}^{b}(f_v-\overline{f})^2}} \quad (12)$$

Here, the terms d_v and f_v represent the vectors, the terms $\overline{d}$ and $\overline{f}$ represent the mean of vectors D and$G$, and the term v represents the number of features. Then, resultant pairs and their scores are stored for further analysis. The image is marked as forged if the scores are higher than the optimum threshold; if not, it is authenticated. When there is changing illumination and noise, this adaptive thresholding dynamically adapts to increase detection accuracy. As a result, the detected forgery outcome FD_F is obtained from the proposed WMS-AT, which requires false match detection. Therefore, WMS-AT enhances feature matching accuracy, allowing for accurate anomaly localization and lowering false detections by dynamically altering thresholds and weighting similarities in challenging CMF applications. The schematic representation of WMS-AT-based feature matching is illustrated in Figure 5.

5.3 False Match Detection using RANSAC

The RANSAC-based false match detection method improves CMFD through the removal of inaccurate feature correspondences. Geometric consistency between matched regions is ensured by iteratively fitting transformation models and eliminating outliers. By keeping only genuine matches, this improves accuracy and strengthens the system's resistance to noise and intricate counterfeits.

The forged features captured are fed into the RANSAC false match detector during feature matching. RANSAC [30] is a strong model that computes the geometric transformation model by randomly sampling a small subset of the matched feature pairs, to see if the

model matches with the full set of matched features. For matched feature pairs, best captures the huge majority of consistent matches and effectively separates false matches (outliers) from true matches (inliers), in this approach, since the model is improved iteratively, a large proportion of outliers are kept by RANSAC, classifying matches in accordance with their adherence to the expected transformation, but also making them suitable for precision-involved applications. Localization and verification of the CMF regions in a large image, making it stronger to outliers. Are essential for accurate CMFD and reliable forgery localization.

6. Results And Discussion

6.1 Simulation Design

A copy-move image forgery detection system was implemented using Python. It is leveraged with a population size of 10, a chromosome length of 5, and a maximum iteration of 50.Other deep model parameters include image size of 32x32x3, 512-dimensional feature map, 70-20-10 train-validation-test split, batch size of 32, learning rate set to adam default (0.01), epochs set to 200. The stopping criterion was set to 50 iterations. The data was pre-processed not augmented.

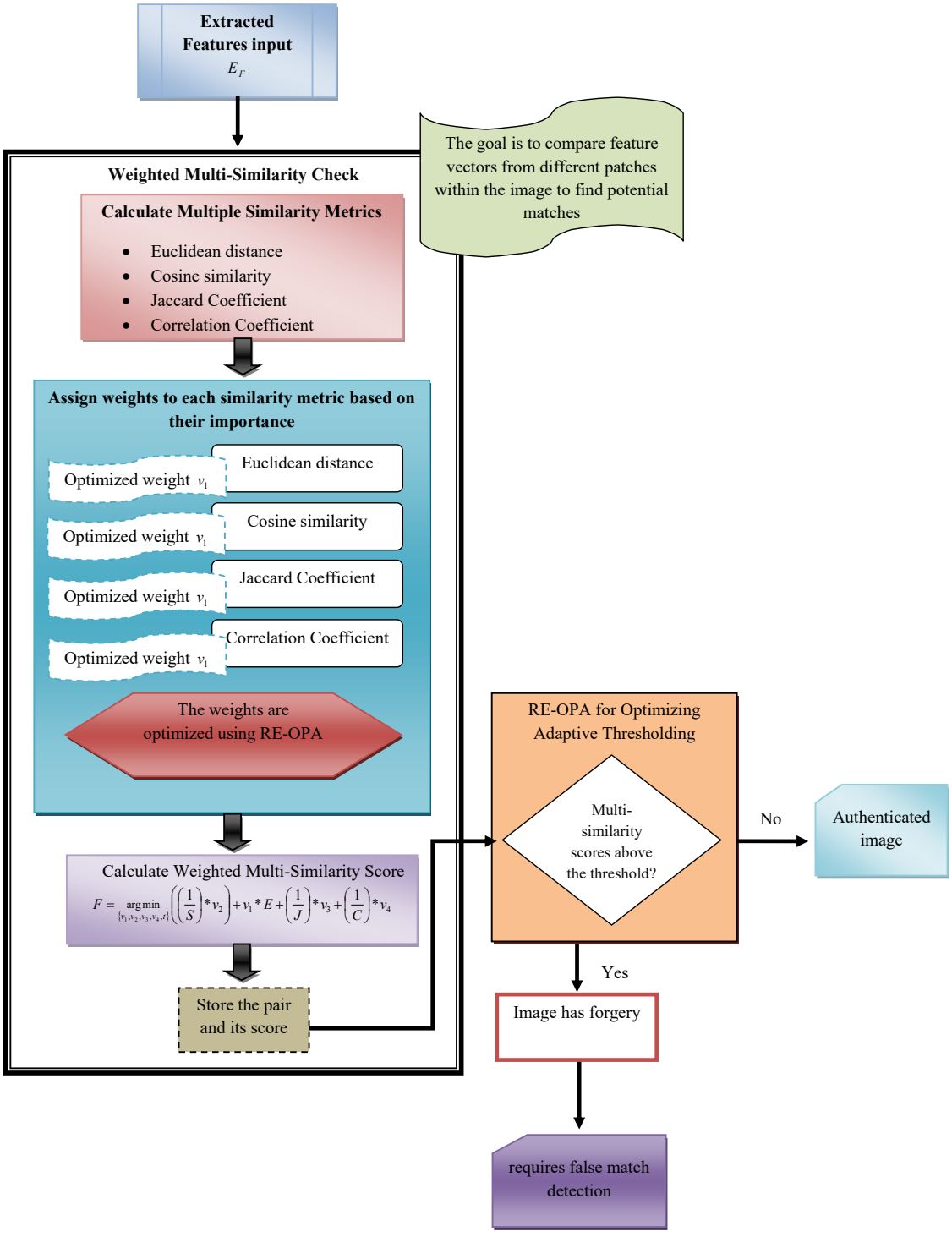


Figure 5. Schematic Representation of WMS-AT-based Feature Matching

The system requires a minimum configuration of intel core i3 processor and 512GB of disk space and performs well when run over GPU systems or T4-CPU configuration in Google colab environment. The effectiveness of the proposed copy-move image forgery detection model was compared with several classification models, including Orca Predation Algorithm (OPA) [28], Gooseneck Barnacle Optimization Algorithm (GBOA) [29], Actor Optimization Algorithm (AOA) [30], and Ship Rescue Optimization (SRO) [31].

6.2 Performance Metrics

This section provides an outline of the metrics employed for computational performance analysis.

(a) Accuracy:

$$C = \frac{L+G}{L+G+J+W} \quad (14)$$

Here, the terms L, G, J, and W represent the true positive, false positive, true negative, and false negative, respectively.

(b) Precision:

$$K = \frac{L}{L+G} \quad (15)$$

(c) F1 Score:

$$Hf = \frac{2\times L}{(2\times L)+G+W} \quad (16)$$

(d) Recall:

$$R = \frac{L}{L+W}$$

6.3 Resultant Images of Copy-Move Image Forgery Detection

The resultant images of copy-move image forgery detection are portrayed in Figure 6.

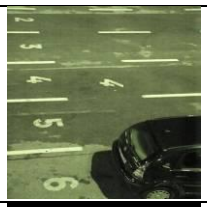
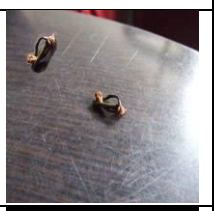
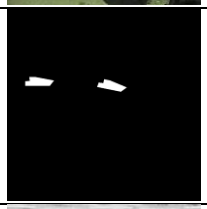
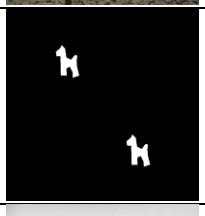
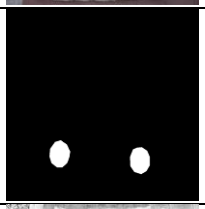
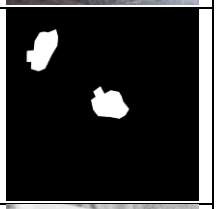
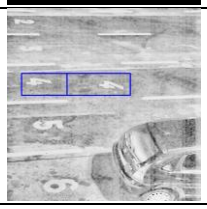
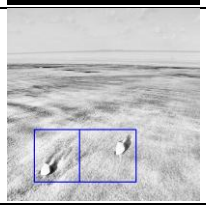
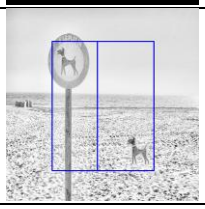
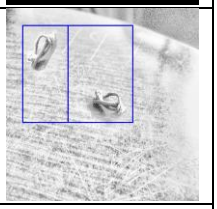
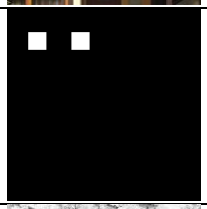
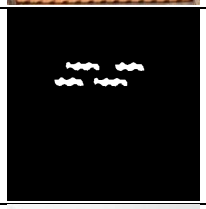
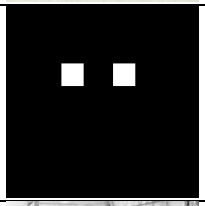
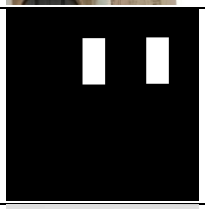
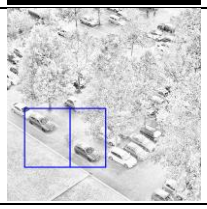
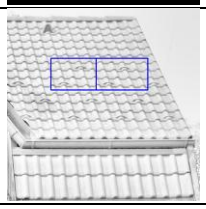
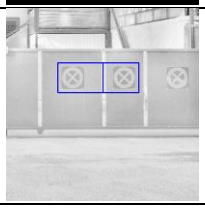
Image Classes	Image-1	Image-2	Image-3	Image-4	Image-5
Dataset-1					
Original Image					
Ground Truth Image					
Detected Image					
Dataset-2					
Original Image					
Ground Truth Image					
Detected Image					

Figure 6. Resultant Copy-Move Image Forgery Detected Images

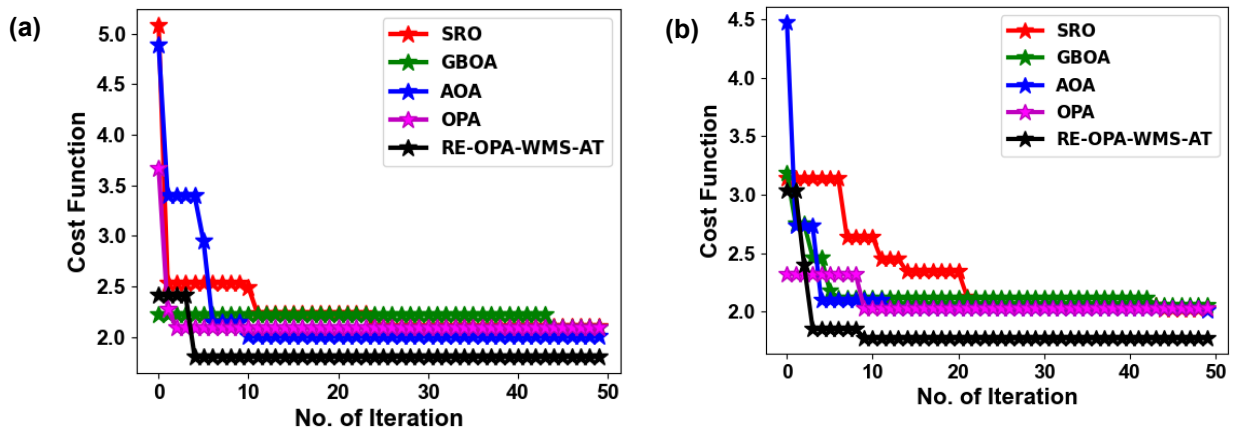


Figure 7. Convergence Validation of the Proposed Model on Dataset-1 and Dataset-2

6.4 Convergence Validation of the Proposed Model

Figure 7 illustrates the convergence validation of the proposed model for CMFD on Dataset-1 and Dataset-2. Convergence validation implies that the optimization process produces accurate and consistent results across time.

Superior convergence behavior was repeatedly shown by RE-OPA-WMS-AT, which outperformed SRO, GBOA, AOA, and OPA by 53.846%, 4.348%, 51.020%, and 35.135%, respectively.

Its adaptive optimization and improved feature matching greatly decreased false matches and increased detection accuracy. Therefore, the proposed model exhibits fewer computational complexity with supporting evidence from Figure 7 showing marginally faster convergence in comparison to benchmark optimizers representing lesser iterations and processing overhead, and is appropriate for a variety of high-resolution image datasets because of its robustness and dynamic parameter adjustment, which allow it to tackle complex forgeries with ease for CMFD.

6.5 Performance Evaluation of Proposed Model with Traditional Optimization Algorithms

Figure 8 presents the performance evaluation of the proposed model in comparison with traditional optimization algorithms on Dataset-1 and Dataset-2. The performance evaluation measures each method's capacity to produce reliable, consistent, and accurate detection results across a range of forgery scenarios. The suggested model continuously surpassed SRO, GBOA, AOA, and OPA in terms of detection accuracy and low false matches across several test datasets by margins of 14.458%, 11.765%, 13.095%, and 5.556%, respectively, on Dataset-1. Therefore, the proposed RE-OPA-WMS-AT works well with large-scale, complicated, and high-resolution picture datasets because of its improved feature matching and adaptive optimization, which enable accurate forgery localization for CMFD.

6.6 Performance Analysis of the Developed Model for Feature Matching

Figure 9 presents the performance analysis of the developed model using similarity measures such as Euclidean Distance, Cosine Similarity, Jaccard Coefficient, and Correlation Coefficient for feature matching in copy-move image forgery detection. The similarity and proximity of matched regions were assessed using these parameters individually. In the proposed model, Euclidean Distance, Cosine Similarity, Jaccard Coefficient, and Correlation Coefficient are used together to evaluate the similarity of matched regions. Durable matching accuracy and low false match rates were shown by the model's low Euclidean distances, cosine similarity, Jaccard, and correlation similarity scores of values 8.434%, 8.362%, 6.509%, and 3.448%, respectively, in Dataset-1. Therefore, this demonstrates that the proposed model can detect forged areas even when compressed and subjected to geometric changes. Its extensive similarity analysis helps greatly in the accurate detection of manipulated areas in a variety of image situations. The proposed methodology's resilience to complex image transformations is supported by constant detection performance across varied image manipulation demonstrated in Figures 8 & 9.

6.7 Performance Comparison of the Proposed Model with Existing Methods

Figure 10 shows the comparison with other existing CMFD methods for various datasets, which present the performance of our proposed model. Uses an advanced region-matching method and advanced feature representation to improve efficiency and reduce the time needed. Furthermore, the model is considerably better than RSADTL-CMFD, DNN, CNN-CSK, SVM-PCA, and RE-OPA-WMS-AT with F1 Score increased by 16.667%, 16.667%, 33.333%, 16.667%, and 16.667% respectively.

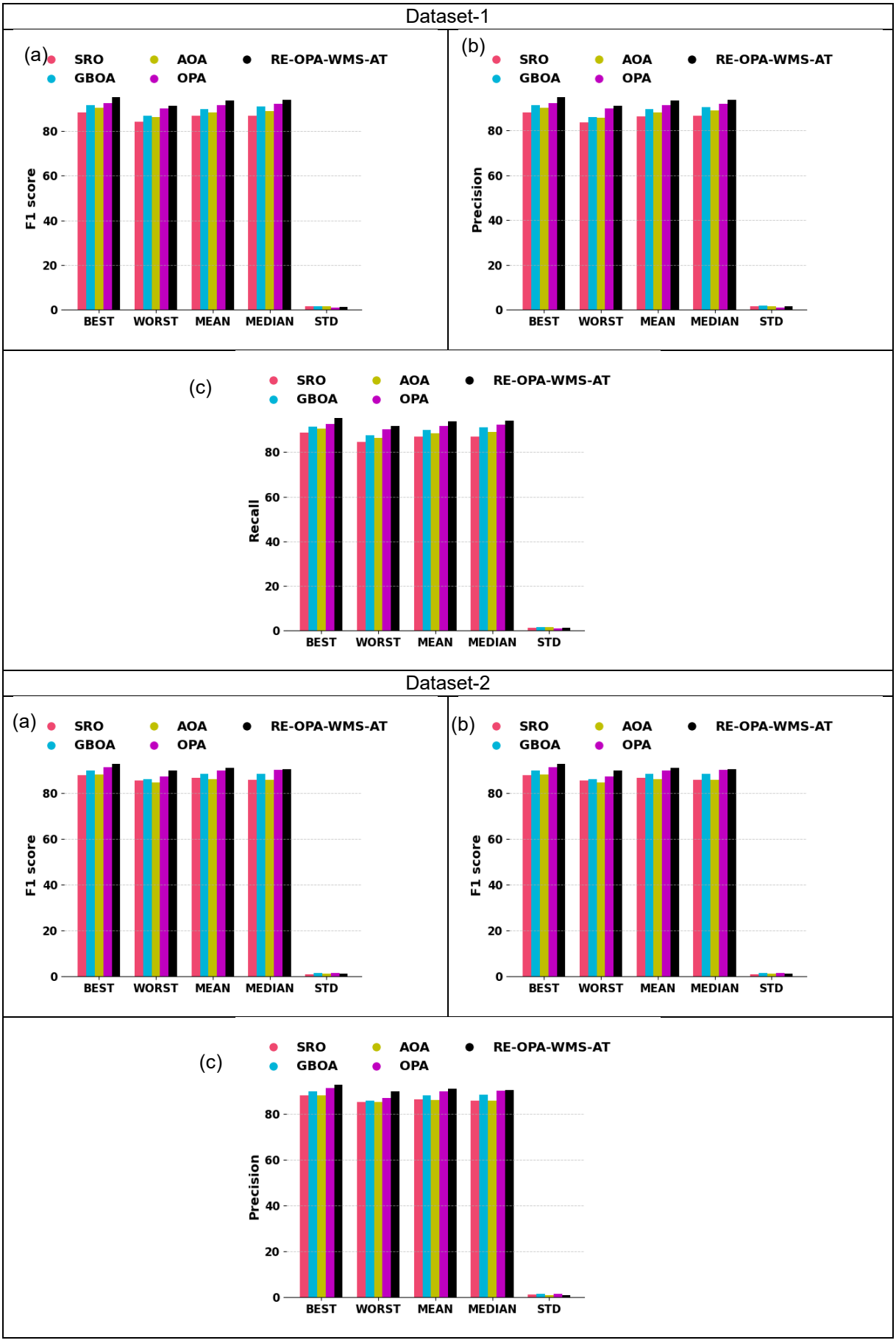


Figure 8. Performance Evaluation of Proposed Model with Traditional Optimization Algorithms regarding **(a)** F1 Score, **(b)** Precision, and **(c)** Recall on Dataset-1 and Dataset-2

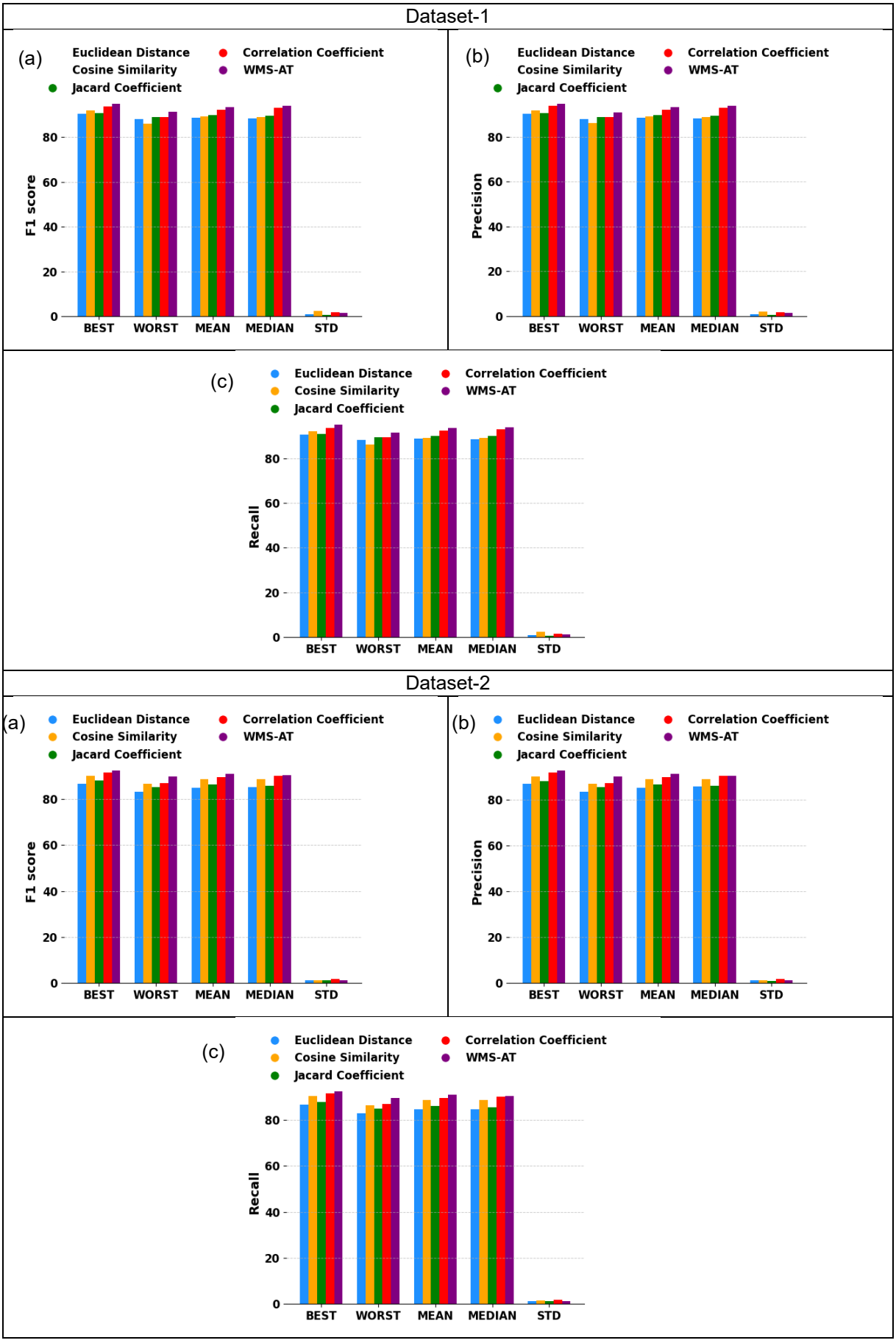


Figure 9. Performance Analysis of Developed Model for Feature Matching regarding **(a)** F1 Score, **(b)** Precision, and **(c)** Recall on Dataset-1 and Dataset-2

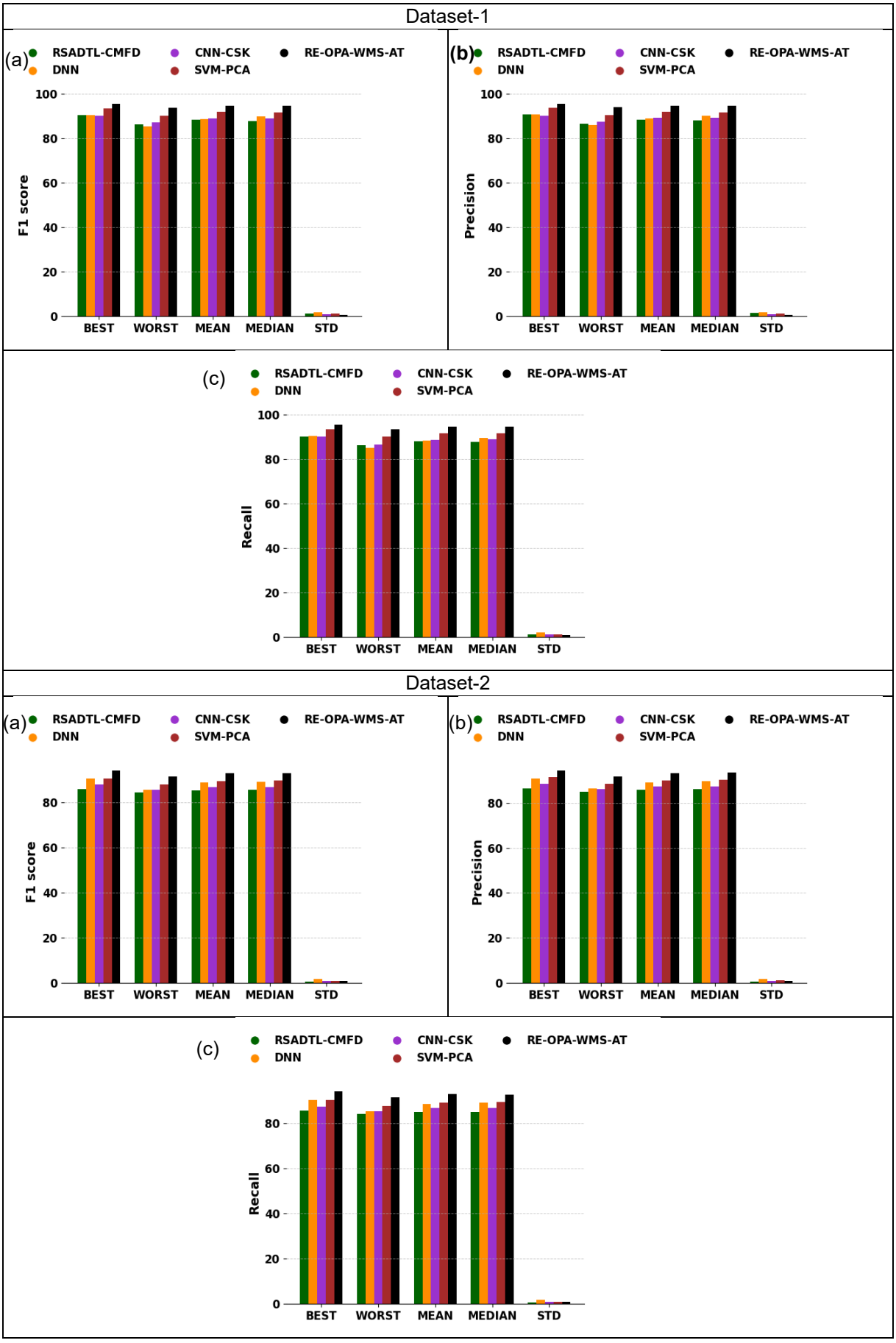


Figure 10. Performance Comparison of the Proposed Model with Existing Methods regarding **(a)** F1 Score, **(b)** Precision, and **(c)** Recall on Dataset-1 and Dataset-2

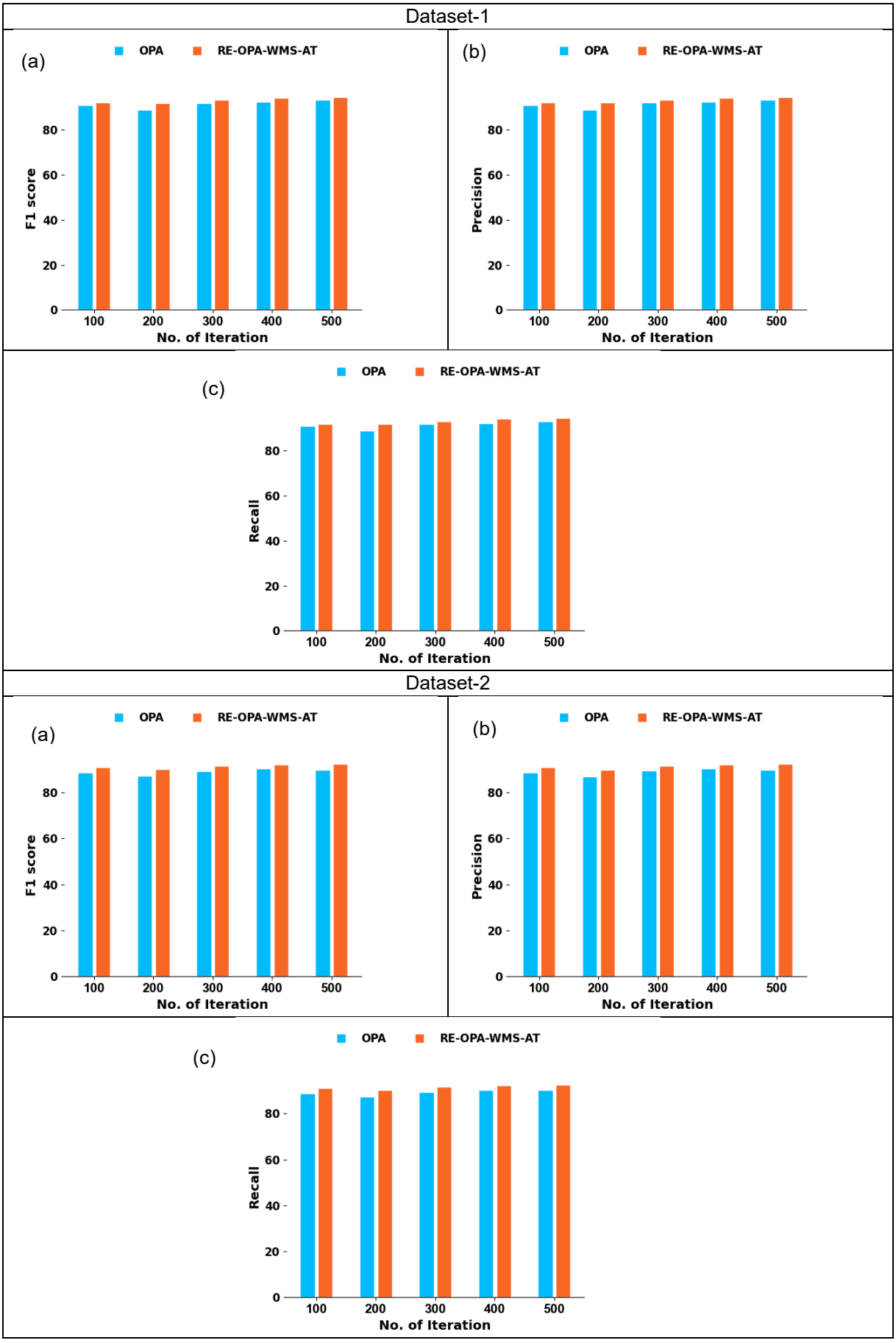


Figure 11. Performance Comparison of with Existing Optimization Algorithm vs. the Proposed Model regarding **(a)** F1 Score, **(b)** Precision, and **(c)** Recall on Dataset-1 and Dataset-2

The experimental results for Dataset-1 and the proposed heuristic method reflect the percentage of 11.364%, 13.953% and 8.889% model can detect fake areas even when there are changes of geometric, compression and scaling in the images. Therefore, REOPA- the WMS-AT model allows for accurate localization of changes and has demonstrated robustness in variable conditions. Difficult imaging scenarios in medical care.

6.8 Performance Comparison with Existing Optimization Algorithm vs. Proposed Mode

The performance comparisons between the existing optimization algorithm and the proposed model for CMFD are shown in Figure 11.

The proposed model considerably improves performance and robustness by jointly analyzing feature matching and adaptive optimization although OPA has a similar optimization ability.

Table 2. Comprehensive Evaluation of the Proposed Method

Optimization Algorithm					
Terms	**SRO [31]**	**GBOA [29]**	**AOA [30]**	**OPA [28]**	**RE-OPA-WMS-AT**
Dataset-1					
Accuracy	83.719	86.610	88.064	88.911	98.971
Recall	71.998	76.383	78.673	80.036	97.964
Precision	83.823	86.075	87.838	89.044	98.934
F1 - Score	13.589	10.908	9.750	7.028	0.987
Dataset - 2					
Accuracy	80.572	83.445	83.553	87.589	98.837
Recall	67.465	71.593	71.753	77.918	97.702
Precision	80.208	81.386	81.804	86.807	98.677
F1 - Score	11.650	10.742	8.453	6.035	0.987
Classifier					
Dataset-1					
Terms	**Euclidean Distance**	**Cosine Similarity**	**Jaccard Coefficient**	**Correlation Coefficient**	**WMS-AT**
Accuracy	80.350	80.927	83.110	84.551	98.971
Recall	67.154	67.964	71.102	73.237	97.964
Precision	80.343	80.392	82.551	84.157	98.934
F1 - Score	16.617	15.463	13.261	12.042	0.987
Dataset-2					
Accuracy	74.393	78.703	81.813	83.034	98.837
Recall	59.227	64.884	69.223	70.911	97.702
Precision	72.152	76.267	79.622	80.421	98.677
F1 - Score	16.493	14.082	12.817	10.541	0.987

In terms of accuracy, false match reduction precision, RE-OPA-WMS-AT outperformed other types of techniques to address complex high-resolution fake images, outperforming standard OPA by 1.052% in terms of the F1 Score on Dataset-1, thus verifying that CMFD is far more successful when combined with advanced similarity metrics and dynamic parameters.

6.9 Comprehensive Evaluation of the Proposed Model

Table 2 lists the performance of the proposed model for CMFD. The proposed RE-OPA-WMS-AT displayed its performance strength against detected forgeries on random textures, geometric transformations and noise, with an average resulting in improvements of 8.722%, 5.592%, 5.505%, and 1.342% in precision compared to existing methods SRO, GBOA, AOA, and OPA respectively.

RE-OPA have been compared against a standard model in Dataset-1 and have been shown to perform better effectiveness and computing economy by integrating adaptive optimization and thorough matching of features to provide more consistent detection across a wide range of datasets. The proposed methodology exhibits higher generalization parameter, faring consistent performance among benchmark datasets

with low variance, supported by the below-mentioned Table 2.

6.10 Statistical Analysis of the Proposed Model

The performance comparison of copy-move image forgery detection on Dataset-1 and Dataset-2 in terms of fitness value of the objective function up to 50 (stopping criterion) independent iterations on random seeds is shown in Table 3. The objective function optimized by RE-OPA is defined as maximizing the weighted multi-similarity score (Eq. 8), subject to minimizing false matches after RANSAC filtering. The best performance results of several algorithms, including the RE-OPA-WMS-AT model, are reported on dataset 2 exhibiting the highest effectiveness at 1.807%. Overall, RE-OPA-WMS-AT is considerably more effective than the other models with which it was compared. The best values obtained were 14.157% for SRO, 13.788% for GBOA, and 9.785% for BGGOA. Values (0.153%, 0.499%, 0.253%, 1.812%, 13.499% for OPA). The RE-OPA-WMS-AT algorithm obtains a trade-off of different metrics with the best results for Dataset-1. However, it does have advantages over standard techniques making it a more reliable method of CMF detection.

6.11 Attack-wise breakdown of the proposed Model

To evaluate the strength of the proposed RE-OPA-WMS-AT against varied forgery attacks, an attack-wise breakdown of the results is proposed for both the datasets, The MICC dataset does not present direct attacks unlike CoMoFoD dataset, and the images were categorised into various attack groups based on the dataset inference and corresponding literature. The attack groups for MICC dataset include plain copy-move, geometric, post-processed, noise-affected and complex transformations are listed in table 4.

The CoMoFoD dataset contains attack labels like compression, scaling, rotation, noise and complex transformations which include more than one of the above-mentioned attacks which are listed in table 5.

Table 3. Statistical Analysis of the Proposed Model

Terms		GBOA [29]	AOA [30]	OPA [28]	RE-OPA-WMS-AT
Dataset-1					
BEST	2.105	2.096	2.003	2.089	1.807
WORST	5.078	2.226	4.886	3.668	2.412
MEAN	2.283	2.210	2.203	2.124	1.855
MEDIAN	2.105	2.226	2.003	2.089	1.807
STD	0.431	0.042	0.549	0.222	0.164
Dataset-2					
BEST	2.0171	2.0588	2.0151	2.0312	1.7763
WORST	3.1391	3.1861	4.4723	2.3246	3.0330
MEAN	2.3133	2.1721	2.1298	2.0840	1.8485
MEDIAN	2.0525	2.1188	2.0280	2.0312	1.7763
STD	0.3824	0.2034	0.3736	0.1127	0.2578

Table 4. Attack-Wise Breakdown of Micc Dataset

Attack Type	Accuracy	Precision	Recall	F1 Score
Plain Copy-move	96.1	95.2	95.8	95.5
Geometric	94.6	93.4	94.1	93.7
Post-processed	95.0	94.0	94.6	94.3
Noise-affected	93.7	92.8	93.2	93.0
Complex transformations	92.9	91.5	92.0	91.7

Table 5. Attack-Wise Breakdown of Comofod Dataset

Attack Type	Accuracy	Precision	Recall	F1 Score
Compression	95.6	94.8	95.2	95.0
Scaling	94.3	93.1	93.8	93.4
Rotation	93.2	91.5	92.2	91.8
Noise	93.8	92.7	93.0	92.8
Complex Transformations	92.4	90.9	91.3	91.1

Table 6. Standarad Deviation & Confience Interval of the Proposed Re-Opa-Wms-At Method of Micc Dataset

Dataset-1			
Method	**Mean**	**Std**	**95% CI**
SRO	2.283	0.431	2.283 ± 0.122
GBOA	2.210	0.042	2.210 ± 0.012
AOA	2.203	0.549	2.203 ± 0.156
OPA	2.124	0.222	2.124 ± 0.063
RE-OPA-WMS-AT	1.855	0.164	1.855 ± 0.047

Table 7. Standarad Deviation & Confience Interval of the Proposed Re-Opa-Wms-At Method of Comofod Dataset

Dataset-2			
Method	**Mean**	**Std**	**95% CI**
SRO	2.3133	0.3824	2.313 ± 0.109
GBOA	2.1721	0.2034	2.172 ± 0.058
AOA	2.1298	0.3736	2.130 ± 0.106
OPA	2.0840	0.1127	2.094 ± 0.032
RE-OPA-WMS-AT	1.8485	0.2578	1.849 ±0.073

The proposed RE-OPA-WMS-AT model fared consistently high across all types of attacks, with its best performance observed under plain copy-move and compression attacks. The system slightly struggled to identify complex transformations due to varied distortions.

Further to ensure statistical reliability of the proposed RE-OPA-WMS-AT model, the key metrics were computer on 50 independent runs for which the mean and standard deviation were obtained. In addition, 95% confidence intervals were added using the t-distribution to quantify the uncertainty linked with the estimated means. The proposed method demonstrates slightly narrow confidence compared to benchmark algorithms depicting its higher stability across multiple seed runs on both the datasets which are listed in tables 6 and 7.

Table 8. Ablation study on MICC dataset

Variant	Accuracy	Precision	Recall	F1 Score
Without Preprocessing	91.22	90.05	89.60	90.18
Without SA	93.45	92.14	90.16	92.30
Without RE-OPA	94.88	93.76	90.58	93.84
Without WMS-AT	95.64	94.52	89.48	94.63
Without RANSAC	96.72	95.61	91.50	95.74
RE-OPA-WMS-AT	**98.97**	**98.93**	**97.96**	**98.70**

Table 9. Ablation study on CoMoFoD Dataset

Variant	Accuracy	Precision	Recall	F1 Score
Without Preprocessing	91.00	89.20	89.90	88.80
Without SA	92.88	93.14	91.20	93.20
Without RE-OPA	93.67	93.90	91.40	92.20
Without WMS-AT	95.80	94.20	90.80	93.60
Without RANSAC	96.68	96.40	92.00	96.40
RE-OPA-WMS-AT	**98.83**	**98.67**	**97.70**	**98.71**

6.12 Ablation Study of the Proposed RE-OPA-WMS-AT Method

The ablation studies show that every component contributes to the overall detection performance. Without preprocessing, both accuracy and F1-score gradually decrease, indicating that preprocessing helps extract better features under challenging conditions. Disabling spatial attention decreases precision and recall, indicating that spatial attention helps in accurately identifying salient forged regions of the image. The loss of RE-OPA was marginal, indicating that the adaptive optimization stabilizes the matching process.

The stronger influence of WMS-AT on precision and F1-score indicates that this algorithm is important to the separation of true matches from false ones. The largest drop in precision without RANSAC indicates that RANSAC rejects most of the geometrically inconsistent false matches. The trade-off of no RANSAC or other filtering is that result recall increases, but false positives are introduced and both accuracy and F1-score decrease.

Ultimately, the results show that the performance increase is achieved through the combination of the different components, i.e., preprocessing, hybrid feature learning, adaptive matching, optimization, and geometric verification, rather than being caused by a single component. The experiments presented in this paper directly answer the question of where the performance gain comes from as depicted in tables 8 and 9.

7. Conclusion

This study developed a novel CMFD architecture, combining deep learning with advanced feature matching-based methods. And optimization approaches that offer good accuracy and longevity in the field of digital image forensics. Firstly, benchmark datasets were utilized, which include identical, real, and altered images. For this, image preprocessing was carried out on the images and to bring them to a uniform scale. The ECT-SANet was trained on preprocessed images to extract regionally relevant information and high-dimensional features to assist in accurately identifying the forgery. The feature extraction process involves using a WMS-AT approach. The RE-OPA enabled this by improving feature correlations in the presence of target signal deviations and decreased false matches. It is then used to test the detected features for consistency using RANSAC the matched regions or intervals. The performance of conventional optimization approaches in these situations is such as SRO, GBOA, AOA, OPA, and others. The proposed RE-OPA-WMS-AT model showed a considerable reduction in error of 6.880%, 3.984%, 7.673% and 1.635%. This result shows that the proposed approach is an efficient method for detecting copy-move image forgeries with a strong suite of feature extraction capabilities and matching accuracy. The model's lower computational complexity is indirectly complimented by the algorithm's convergence.

8. Limitation of the Proposed Model

Beyond the reported success of ECT-SANet + WMS-AT + RE-OPA, there remain areas for potential improvement, which can be addressed in future research efforts. In the case of regions with repeated data, such as foliage, grass, bricks, and waves, this can lead to false positives due to the high similarity values assigned to these regions by the multi-similarity matching strategy, leading to over-segmentation. Very small duplicated patches or thin structures such as wires or edges may be missed. RANSAC method may not work well on real forgeries with non-rigid or perspective-based transformations, as matching features may be rejected or localization results may be fragmented. The gains are incremental not exponential as the optimizer shares modified features from its baseline OPA family, reason for RE-OPAs narrow gains.

9. Future Work and Directions

Future research works can be focused on developing semantic understanding of the advanced attention and transformer models yielding better results in the domain of vision-language models. Integration of advanced image pre-processing techniques coupled with multi scale sensitivity architectures can further strengthen the advanced CMFD models. False positive detection can stretch beyond RANSAC or similar techniques. Future advancements can address video copy-move and multi copy-move forgeries and optimization modules can explore novel Meta heuristic approaches.

References

[1] J. Desai, Detecting Digital Image Copy Move Forgery through Advanced Image Forensics. Journal of Emerging Technologies and Innovative Research, 11(2), (2024) 440-443.

[2] S.K. Narasimhamurthy, V.K. Mahadevachar, R.K.T. Narasimhamurthy, A Copy-Move Image Forgery Detection Using Modified SURF Features and AKAZE Detector. International Journal of Intelligent Engineering & Systems, 16(4), (2023). https://doi.org/10.22266/ijies2023.0831.02

[3] E. Liang, K. Zhang, Z. Hua, Y. Li, X. Jia, TransCMFD: An Adaptive Transformer for copy-Move Forgery Detection. Neurocomputing, 638, (2025) 130110. https://doi.org/10.1016/j.neucom.2025.130110

[4] E. Amiri, A. Mosallanejad, A. Sheikhahmadi, the Optimal Model for Copy-Move Forgery Detection in Medical Images. Journal of Medical Signals & Sensors, 14(2), (2024) 5. https://doi.org/10.4103/jmss.jmss_35_22

[5] V. Shinde, V. Dhanawat, A. Almogren, A. Biswas, M. Bilal, R. A. Naqvi, A. U. Rehman, Copy-move Forgery Detection Technique using Graph Convolutional Networks Feature Extraction. IEEE Access, 12, (2024) 121675 – 121687. https://doi.org/10.1109/ACCESS.2024.3452609

[6] J. Wang, J. Nie, N. Jing, X. Liang, X. Wang, C.H. Chi, Z. Wei, Copy-Move Forgery Image Detection based on Cross-Scale Modeling and Alternating Refinement IEEE Transactions on Multimedia, 27, (2025) 5452 - 5465. https://doi.org/10.1109/TMM.2025.3543057

[7] M.M.E. Eltoukhy, F.S. Alsubaei, A.M. Mortda, K. M. Hosny, an Efficient Convolution Neural Network Method for Copy-Move Video Forgery Detection. Alexandria Engineering Journal, 110, (2025). 429-437. https://doi.org/10.1016/j.aej.2024.10.030

[8] A. Diwan, R. Mahadeva, V. Gupta, Advancing copy-move Manipulation Detection in Complex Image Scenarios through Multiscale Detector. IEEE Access, 12, (2024) 64736-64753. https://doi.org/10.1109/ACCESS.2024.3397466

[9] Z. Zhang, E. Zhao, D. Niu, J. Nie, X. Liang, L. Huang, (2024) Copy-Move Forgery Detection and Question Answering for Remote Sensing Image. arXiv preprint. https://doi.org/10.48550/arXiv.2412.02575

[10] D.P. Timothy, A.K. Santra, Detecting Digital Image Forgeries with Copy-Move and Splicing Image Analysis using Deep Learning Techniques. International Journal of Advanced Computer Science & Applications, 15(5), (2024).

[11] G. Fu, Y. Zhang, Y. Wang, Image Copy-Move Forgery Detection based on fused features and Density Clustering. Applied Sciences, 13(13), (2023) 7528. https://doi.org/10.3390/app13137528

[12] M. Assiri, Synergy of Internet of Things and Software Engineering approach for enhanced Copy–Move Image Forgery Detection Model. Electronics, 14(4), (2025) 692. https://doi.org/10.3390/electronics14040692

[13] B. Chaitra, P.V.B. Reddy, Copy-Move Image Multiple Forgery Detection Based on Transit Flow Regime Algorithm-Enabled ShuffleNet. International Journal of Image and Graphics, (2025) 2750017. https://doi.org/10.1142/S0219467827500173

[14] S.B.G. Tilak Babu, C.S. Rao, Copy-Move Forgery Verification in Images using Local Feature Extractors and Optimized Classifiers. Big Data Mining and Analytics, 6(3), (2023) 347–360. https://doi.org/10.26599/BDMA.2022.9020029

[15] T. Qazi, M. Shah, M. Ali, F. Gul, M. Ahmad, A. Khan, Frequency Domain Manipulation of Multiple Copy-Move Forgery in Digital Image Forensics. PLoS One, 20(7), (2025) e0327586. https://doi.org/10.1371/journal.pone.0327586

[16] M. Zanardelli, F. Guerrini, R. Leonardi, N. Adami, Image Forgery Detection: a Survey of Recent Deep-Learning Approaches. Multimedia Tools and Applications, 82(12), (2023). 17521-17566. https://doi.org/10.1007/s11042-022-13797-w

[17] S.D. Dabhole, G.G. Rajput, Copy Move Image Tampering Genuine and Tampered Region Identification and Classification using various Residual Network Approaches. International Journal of Engineering Research & Technology (IJERT), 13(9), 2024.

[18] M. Maashi, H. Alamro, H. Mohsen, N. Negm, G.P. Mohammed, N.A. Ahmed, S.S. Ibrahim, M.I. Alsaid, Modeling of Reptile Search Algorithm with Deep Learning Approach for Copy Move Image forgery detection. IEEE Access, 11, (2023) 87297-87304. https://doi.org/10.1109/ACCESS.2023.3304237

[19] A.H. Khalil, A.Z. Ghalwash, H.A. Elsayed, G.I. Salama, H.A. Ghalwash, Enhancing Digital

Image Forgery Detection using Transfer Learning. IEEE Access, 11, (2023) 91583-91594. https://doi.org/10.1109/ACCESS.2023.3307357

[20] A. Diwan, A.K. Roy, (2024). Cnn-keypoint based Two-Stage Hybrid Approach for Copy-Move Forgery Detection. IEEE Access, 12, 43809-43826. https://doi.org/10.1109/ACCESS.2024.3380460

[21] A. Diwan, D. Kumar, R. Mahadeva, H.C.S. Perera, J. Alawatugoda, Unveiling Copy-Move Forgeries: Enhancing Detection with Superpoint keypoint architecture. IEEE Access, 11, (2023) 86132-86148. https://doi.org/10.1109/ACCESS.2023.3304728

[22] J. Rao, S. Teerakanok, T. Uehara, ResTran: Long Distance Relationship on Image Forgery Detection. IEEE Access, 11, (2023) 120492-120501. https://doi.org/10.1109/ACCESS.2023.3327761

[23] S. Abdulwahid, The Detection of Copy Move Forgery Image Methodologies. Measurement: Sensors, 26, (2023). https://doi.org/10.1016/j.measen.2023.100683

[24] M.M.A. Alhaidery, A.H. Taherinia, H.I. Shahadi, A Robust Detection and Localization Technique for Copy-Move Forgery in Digital Images. Journal of King Saud University-Computer and Information Sciences, 35(1), (2023) 449-461. https://doi.org/10.1016/j.jksuci.2022.12.014

[25] A.R. Al-Shamasnehm R.W. Ibrahim, Image Splicing Forgery Detection using feature-based of Sonine Functions and Deep Features. Computers, Materials, & Continua, 78(1), (2024) 795-810. https://doi.org/10.32604/cmc.2023.042755

[26] L. Yin, L. Wang, S. Lu, R. Wang, Y. Yang, B. Yang, S. Liu, A. AlSanad, S.A. AlQahtani, Z.Yin, Xi. Li, X. Chen, W. Zheng, Convolution-Transformer for Image Feature Extraction. Computer Modeling in Engineering & Sciences, 141(1), (2024) 87-106. https://doi.org/10.32604/cmes.2024.051083

[27] X. Zhang, C. Liu, D. Yang, T. Song, Y. Ye, K. Li, Y. Song, (2023). RFAConv: Innovating Spatial Attention and Standard Convolutional Operation. arXiv:2304.03198. https://doi.org/10.1016/j.patcog.2026.113208

[28] Y. Jiang, Q. Wu, S. Zhu, L. Zhang, Orca predation algorithm: A Novel Bio-Inspired Algorithm for Global Optimization Problems. Expert Systems with Applications, 188, (2022)116026. https://doi.org/10.1016/j.eswa.2021.116026

[29] S.C. Chu, T.T. Wang, A.R. Yildiz, J.S. Pan, Ship Rescue Optimization: a New Metaheuristic Algorithm for Solving Engineering Problems. Journal of Internet Technology, 25(1), (2024) 61-78. https://doi.org/10.53106/160792642024012501006

[30] M. Ahmed, M.H. Sulaiman, A.J. Mohamad, M. Rahman, Gooseneck Barnacle Optimization Algorithm: A novel nature Inspired Optimization Theory and Application. Mathematics and Computers in Simulation, 218, (2024) 248–265. https://doi.org/10.1016/j.matcom.2023.10.006

[31] K. Wu, Creating Panoramic Images using ORB Feature Detection and RANSAC-based Image Alignment. Advances in Computer and Communication, 4(40, (2023) 220–224. https://doi.org/10.26855/acc.2023.08.002

Authors Contribution Statement

Chalamalasetty Sai Pratheek: Conceptualization, Methodology, Investigation, Validation, Writing - Original Draft, Writing - Review & Editing. Srinivasa Rao Giduturi: Supervision. The authors read and approved the final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes