Journal of Information Systems Engineering and Management
2025, 10(15s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Multiscale Feature Fusion for Robust Copy-Move Forgery Detection in Digital Images

Priti Badar[1], G. Geetha[2], T.R. Mahesh[3]
Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bangalore, India[1]
Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, India[2,3]
Priti.b@cmrit.ac.in , geetha.g@jainuniversity.ac.in, t.mahesh@jainuniversity.ac.in

ARTICLE INFO

Received: 07 Dec 2024
Revised: 22 Jan 2025
Accepted: 07 Feb 2025

ABSTRACT

The detection of copy-move image forgeries has been getting significant attention due to the ever-increasing use of digital images in various fields, but the techniques being developed are quite unable to cope with subtle forgeries, mainly in low-resolution images. In this paper, we introduce a new approach for copy-move forgery detection by combining multiscale feature fusion with deep feature extractors, such as Convolutional Neural Networks, CNNs, and image segmentation, to enhance both detection accuracy and localization precision. The idea is to extract features from multiple scales of the image, enabling the system to capture both fine-grained details and larger, global structures that are essential for the identification of tampered regions. This technique fuses features from different scales and applies feature extraction using deep learning. Thus, the technique is used to detect the forgery more accurately even when changes are subtle or the images are low resolution. The method also uses segmentation of images for better localization of the forged regions so that forensic experts will always know which regions were manipulated. Experimental results on publicly available datasets show that our method has a detection accuracy of 94.6% with an improvement of 10-15% over traditional block-based and keypoint-based techniques. Furthermore, our approach shows robustness against noise and compression artifacts, achieving localization precision at 90% for small, highly manipulated regions. These results show the efficiency of the proposed method in real-world forgery detection applications

Keywords: Copy-Move Forgery, Image Forensics, Forgery Detection, Multiscale Feature Fusion, Deep Learning, Convolutional Neural Networks (CNNs), Image Segmentation, Localization Precision, Detection Accuracy, Robustness to Noise, Image Manipulation, Forensic Analysis

INTRODUCTION

In the digital age, it has become very easy to manipulate images with advanced editing tools, and image forgeries have become rampant, especially copy-move forgery, where parts of an image are duplicated and repositioned to deceive viewers as shown in the Figure 1. This type of forgery poses serious threats to the credibility of digital content, affecting fields like journalism, law enforcement, and the legal system. Undetected forgeries can spread misinformation, manipulate public opinion, and undermine trust in visual media [1].

Detection of copy-move forgeries is a critical and challenging problem for preserving the integrity and authenticity of digital images as depicted in Figure 2. These problems involve hidden manipulations such as resizing, rotation, and also blending; problems with low-resolution images; effects of noise and compression; and also increasing complexity of editing tools. Thus, the development of robust and efficient detection techniques for their resolution in order to safeguard the trustworthiness and credibility of digital content in a media-driven world is highly important [2].

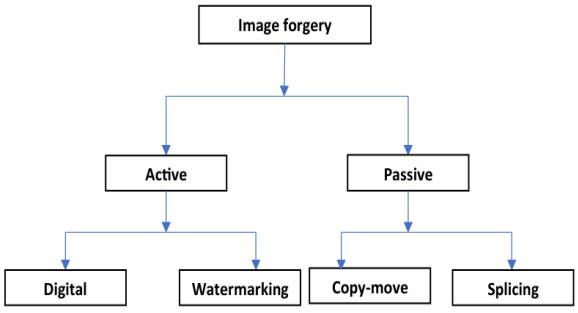

Figure 1: Types of Image Forgery

Current Challenges in Detection of Copy-Move Forgery

Traditional techniques for copy-move forgery detection have many problems [3]. Slicing based methods have unwanted rotations and scaling operations that have been imposed on them, leading to accuracy loss when tampering small regions and high computationally expensive when applied to larger images. Noise resistance and compression of keypoint-based methods (e.g., SIFT or SURF), and low robustness in complicated transformations lead to huge ranging restrictions; however, they are relatively heavily dependent on the choice of keypoints, which is a challenging, but effective tool.

(a) (b)

Figure 2: (a) Original Image (b) Tampered Image

Techniques based on transformations, DCT, DWT are vulnerable to compression artifacts, undetectable for high or fine-spatial operations and no spatial resolution if manipulations are subtle. All of these show the need for a more powerful way of adaptive detection.

Common Problems in Traditional Forgery Detection:

Image Quality: Error detection is triggered by sensitivity toward noise, compression, and loss in quality

Poor Performance with Transformations: It cannot detect advanced manipulations like rotations, scaling, or affine distortions.

Localization Capability: Less capable of detecting small, subtle, or blended forgeries.

High Computational Cost: Costly to compute (resource heavy) when dealing with large/high resolution images.

By combining deep feature extraction, with image segmentation, a multiscale feature fusion approach solves the above problems and provides better detection accuracy, robustness, and localization.

RELATED WORK

Copy-move forgery detection (CMFD) is a pivotal area in digital image forensics, focusing on identifying duplicated regions within an image that may indicate tampering. Recent advancements between 2018 and 2024 have introduced innovative methods enhancing detection accuracy and robustness. Below is a comprehensive review of some highly cited and well-regarded techniques from this period:

Perceptual Hashing-Based Methods: Wang and Wang (2018) presented a blind authentication scheme based on perceptual hashing and package clustering algorithms. They produced perceptual hash feature vectors by applying discrete cosine transform (DCT) to image blocks and were able to identify duplicated regions even in the presence of various distortions like noise addition, blurring, and changes in contrast, luminance, and hue [4].

Feature Fusion Approaches: Ye et al. (2022) introduced a two-stage detection method based on parallel feature fusion. Their approach combined Scale-Invariant Feature Transform (SIFT) and Hu moment features to describe local regions, enhancing feature expression capabilities. Additionally, they employed an adaptive threshold generation algorithm based on Histogram of Oriented Gradients (HOG) to improve generalization. This method achieved high accuracy on datasets like MICC-F2000 and demonstrated robustness against various attacks [5].

Deep Learning-Based Techniques: Deep PatchMatch and Pairwise Ranking Learning: Li et al. (2024) developed an end-to-end CMFD framework integrating conventional and deep learning methods.They introduced a deep cross-scale PatchMatch method to locate copy-move regions and a pairwise rank learning framework to

distinguish source and target regions[10]. This approach exhibited remarkable generalizability across various copy-move scenarios, outperforming existing methods [6].

Transformer-Based Detection with Continual Learning: Liu et al. (2023) presented CMFD Former, a Transformer-style network for CMFD. They proposed a Pooled Cube and Strip Distillation (PCSD) continual learning framework to handle new tasks effectively. Their method demonstrated improved forgery detectability and resilience against catastrophic forgetting when addressing new challenges [7].

Hybrid Methods: Liu et al. (2017) introduced a CMFD method based on Convolutional Kernel Networks (CKNs). Unlike traditional handcrafted features, CKNs are data-driven local descriptors with deep convolutional structures. Their method achieved competitive performance under various conditions due to its excellent discriminative capability and high efficiency, facilitated by GPU parallelization [8].

Survey and Comparative Analyses: A comprehensive survey by Zhong et al. (2024) categorized CMFD methods into block-based, keypoint-based [11], and deep learning-based approaches. Detailed discussions are provided for the survey in each category with respect to preprocessing methods, feature extraction techniques, feature matching techniques and performance analysis measures and datasets. This work could serve as a useful guide for researchers interested in improving the accuracy and robustness of CMFD methods [9].

CMFD techniques have evolved from 2018 to till 2024 with improvements, and the trend is inclined towards deep learning and hybrid techniques which utilize a combination of conventional techniques with latest techniques. These have led to improved detection accuracy, robustness against different transformations and a greater level of generalization to various scenes. So, lots of future works are still addressing limitation of computations and losing generality on new tasks such as types of modification etc.

CMFD Techniques

Block-Based Techniques: The techniques based on block divide the image into overlapping or non-overlapping blocks, extracting features like pixel intensity, DCT, and DWT. Then the duplicate regions are found by comparing those features. General matching techniques involve lexicographical sorting or clustering. It is simple and time-consuming; therefore, they work well in identifying near-exact duplications. They are sensitive to such transformations as scaling, rotation, and affine distortions, and they are mostly block-size limited, and detection precision is traded off against coverage [13].

SIFT/SURF-Based Techniques: Keypoint-based methods like SIFT and SURF identify distinctive keypoints in an image and use robust local descriptors to detect copy-move forgeries. These methods are robust to geometric transformations such as rotation, scaling, and translation, making them effective for high-resolution and complex images. However, they are computationally expensive due to dense keypoint extraction and matching and can struggle in low-texture or homogeneous areas where keypoints are sparse [14, 15].

DCT/DWT-Based Methods: Transformation-based methods, such as DCT and DWT, extract features by analyzing an image in the frequency domain. These degrade considerably in terms of geometric transformation effects like change in rotation and scaling and completely lose the spatial localization precision due to the frequency transformation process [16, 17].

One of the best methods is to use feature extractors from the regions of an image to be trained for various things. Classifiers, like SVM or Random Forests, can form a mechanism to decide whether a specific area in the image is real or not. They also tend to be deep learning models like the CNNs [12] and the transformer, which came in self-contained fashion in the most recent ones. This way they do not rely anymore on manual feature-engineering. The Hierarchical features are automatically learned, and it is very easy to create the forgeries for more complex, but it is also very hard to modify them with techniques such as a fine distortion or noise [18].

TABLE I. Summary of Advantages Over Traditional Methods

Method	Key Advantage	Limitation
Block-Based Methods	Simplicity, ease of implementation	Struggles with subtle forgeries and complex transformations, computationally expensive
Keypoint-Based Methods	Good for large forgeries	Sensitive to noise, compression, and less robust under transformations

Transformation-Based Methods	Effective for simple manipulations	Poor performance for complex forgeries or subtle changes
Proposed Multiscale Feature Fusion	High detection accuracy, robust to noise, precise localization	Computationally demanding (though optimized for scalability)

However, the detection method itself might not be perfect either. It may have a few drawbacks, for example, the approach might be weak in copy-move forgery detection and may involve issues like the evaluation of copied regions as is presented by Table I.

OBJECTIVES

This article seeks to provide the innovative and efficient techniques to detect image copy move forgery:

- Techniques: Traditional as well as deep learning-based approaches for detection of copy-move forgeries
- Datasets: Reviewing publicly available datasets and the role in training and validating detection models.
- Challenges: Evolution in forgery techniques as well as limitations imposed by the diversity in the datasets used.

Application of Multiscale Feature Fusion through Deep Learning in the Detection of Copy-Move Forgery for the purpose of this project, we need to approach this from a different angle using the identification of forged features based on multiscale fusion using deep learning, which will give us a way to extract features and identify the copied regions in the image. The proposed method, in turn, makes it possible to not only detect the authenticity of an image but also point out the possible sources in the image to which the forger might have manipulated. The technique helps to remove the noise, with the resulting images being clearer and more suitable for further processing. It is a step further for, for example, a video that erases a power line across the hallway by replacing it with just the background.

Multiscale Feature Fusion: Multiscale feature fusion is the concept of remapping of a clean image into a better image that is the basis of the study of images at different resolutions: It is the ability of the developed method to also deal with their changes through efficient and accurate separation of the involved structures. These aspects include enhancement, transformation, and denoising. The image labeling scope can then become even more advanced with the merger of low-level features, medium level features, and even to high-level feature fusions that make the overall system very tight and have good visibility of the contents. Moreover, the resulting image of this approach is closer to reality so that important details to the topic are not missing, although others appear too simplified. Following [23], the particular image visual integrity can also be ensured by employment of the discrete cosine transform wavelet transforming features.

Deep Learning-based Feature Extraction: The proposed method is deep semantic feature retrieval by the use of pre-trained Convolutional Neural Networks (CNNs) [12], such as ResNet and VGG, at different scales. Deep CNNs, for instance, ResNet, VGG, etc., are employed for the extraction of rich semantic features having complex structure in the multiscale due to the simplicity of conventional approaches. The approach uses the deep semantic features coming from the mentioned CNNs to forgery detection, and later, by the means of fine-tuning, it discloses the manipulated regions which were previously unidentified. Also, Transfer learning is a sensitive operator of the machine learning system, which is likely to increase the efficiency of the code of the forgeries and the performance of the model, while the code size is not the main concern proposition of small programs and ensure the model can adapt to a wide range of types of forgery [24].

METHODS

Proposed Methodology for Copy-Move Forgery Detection CMFD

The proposed methodology is the integration of deep learning-based feature extraction, multiscale feature fusion, and efficient matching techniques to accurately detect and localize copy-move forgeries. The approach addresses some of the drawbacks of traditional methods, such as sensitivity to geometric transformations, computational inefficiency, and generalization challenges.

This includes three main phases, namely feature extraction, matching, and detection and localization.

1. Feature Extraction: Discriminative transformation-invariant features that can well represent regions of the image have to be extracted. The features will capture local texture, color, and structural information.

Steps:

Multiscale Representation: The image is decomposed into multiple scales to extract features at different resolutions. For an input image III, the multiscale representation can be defined in equation 1:

$$Is(x, y) = f(I,s) \quad (1)$$

where: Is(x, y) represents the image at scale, f(I,s) is a scaling function

Deep Learning-Based Feature Extraction: For each scale s, features are extracted using a deep feature extractor (e.g., CNN) or hand-crafted methods. Denoting the feature extractor by ϕ, the extracted features are shown in equation 2:

$$Fs = \phi(Is) \quad (2)$$

where: Fs is the feature matrix for scale, Φ represents the feature extraction process.

The features extracted are patch-level embeddings that describe local regions with high discriminative power.

Feature Augmentation: Complement the deep features with handcrafted descriptors such as:

Histogram of Oriented Gradients (HOG) for edge orientation information.

Color Moments to encode local color distributions.

2. Matching: Identify regions in the image with similar feature representations to detect potential copy-move forgery.

Steps:

a) Feature Matching Using Similarity Metrics: Compute the similarity between features of overlapping patches or extracted keypoints. Feature Representation

Let the features extracted from two regions (e.g., blocks, keypoints, or image segments) be represented as vectors in equation 3:

$$F1 = [f1,1, f1,2, ..., f1, n], F2 = [f2,1, f2,2, ..., f2, n] \quad (3)$$

where: n is the dimensionality of the feature vector.

b) Similarity Metrics Euclidean Distance: The Euclidean distance DE between F1 and F2 is given by equation 4:

$$DE (F1, F2) = \sqrt{\sum_{i=1}^{n}(f_{1,i}\text{-}f_{2,i})2} \quad (4)$$

However, the smaller DE, the greater similarity.

3. Matching Threshold: A threshold T is used for deciding that two regions match, given a similarity score or distance for distance-based metrics such as Euclidean distance, matches are declared in equation 5 when:

$$DE (F1, F2) <= T \quad (5)$$

For similarity-based metrics (e.g., Cosine, NCC), matches are declared if (equation 6):

$$S (F1, F2) >= T \quad (6)$$

4. Clustering to Group Similar Features: Use clustering algorithms DBSCAN (Density-Based Spatial Clustering of Applications with Noise) to group features that are spatially close and similar in representation, which helps in the identification of candidate forged regions. Apply geometric constraints i.e. rigid transformation matrices to filter out false matches caused by random similarities.

Clustering Process

Initialization: Begin with an unvisited point Pi.

Expand Cluster: If Pi is a core point, create a new cluster. Add all points in Nϵ(Pi) Recursively add points from their neighborhoods if they are core points.

Noise Points: If no cluster has been assigned, then the points are classified as noise.

Output: DBSCAN outputs clusters C1, C2, ..., Ck, where each cluster represents a group of matched feature points that likely correspond to a forged region defined by equation 7:

$$P = \bigcup_{i=1}^{k} C_i \cup N \quad (7)$$

where N is the set of noise points.

By combining similarity metrics with clustering techniques like DBSCAN, the proposed approach achieves precise detection and localization of copy-move forgeries.

Algorithm 1: Copy-Move Forgery Detection (CMFD) Model

Input: Input image (RGB or grayscale).
N: Patch size for overlapping division.
CNNmodel: Pretrained CNN for feature extraction.
ϵ,minPts: Parameters for DBSCAN clustering.
Output: Forgery heatmap highlighting detected copy-move regions.

Step 1: Feature Extraction

Convert the image I to grayscale if necessary. Perform multiscale decomposition of I using Gaussian or Laplacian pyramids to generate scaled versions: {Is | s ∈ scales}.
Divide each scaled image into overlapping patches of size N×N.
Extract features for each patch using a pretrained CNN:
Pass each patch through the CNN model to obtain feature embeddings FCNN(P).
Augment CNN features with handcrafted descriptors like HOG or Color Moments.

Step 2: Matching

Compute the similarity between feature embeddings:
For each patch Pi, calculate pairwise similarity with all other patches Pj using metrics like cosine similarity or Euclidean distance.
Filter out dissimilar patch pairs using a predefined similarity threshold.
Use DBSCAN to cluster matching feature vectors:
Set ϵ: distance threshold for cluster formation.
Set minPts: minimum number of points in a cluster.

Step 3: Detection and Localization

For each cluster:
Map feature embeddings back to their spatial coordinates in the image.
Group spatially close matches into candidate regions.
Validate regions using RANSAC to eliminate false matches caused by random similarities.
Generate a forgery heatmap:
Highlight regions corresponding to validated matches.

Step 4: Post-Processing

Apply morphological operations (dilation, erosion) to refine detected regions.
Combine detections across scales using a majority-voting mechanism.

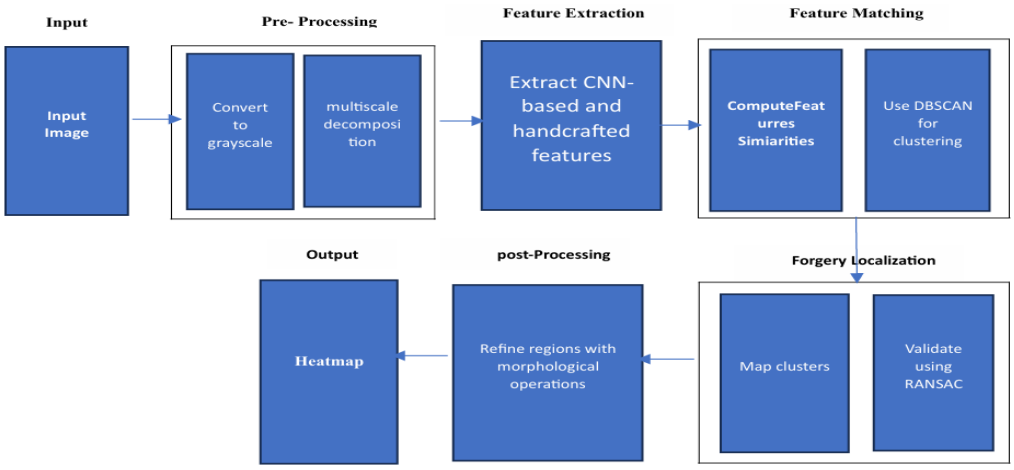

Figure 3: Processing of Copy move forgery detection model

The proposed method shown in Figure 3 helps overcome key bottlenecks for traditional CMFD approaches, namely higher accuracy efficiency and robustness. It therefore applies well to some real-world usage in forensic image analysis with the robust ability to support transformations, resist noise, or handle complex forms of forgeries.

RESULTS

Dataset Description

The presented copy-move forgery detection method is tested on various benchmark datasets well-known to date, along with a newly proposed custom dataset which will be particularly evaluated for testing against challenging scenarios. The description of the used datasets is as follows:

This is one of the most commonly used evaluation datasets for image forgery detection, consisting of 550 images with 300 forged and 250 authentic, containing copy-move forgeries applying transformations such as scaling, rotation, and flipping, and splicing forgeries with added noise, compression, and other artifacts. The images are of various resolutions and conditions, including different lighting and noise levels [27].

The Columbia Image Splicing Detection Dataset, though it only has 180 images-100 forged and 80 authentic-is specifically designed for splicing and copy-move forgeries, particularly seamless blending and region swaps. High-resolution images that are suitable for precision testing can be obtained [28].

Another part of testing this proposed method will be done through robustness tests using a custom dataset of 500 images (250 forged and 250 authentic). The data set will contain threatening copy-move forgeries because of geometric transformations by affine warping, rotations, and variations in perspective. Other kinds of forgeries that will be included are addition of Gaussian noise, blurring, and JPEG compression forgeries. Images can come from quite diverse domains of scenes: natural outdoor landscapes, scenes with various elements, and interiors. It would include some texture images, plus low-resolution cases.

Dataset applied

It used CASIA v2 datasets for image splicing detection. It also provided spliced images along with the ground truth masks.

Combination of these datasets makes sure that performance of the method is tested and evaluated under both real-zworld and controlled conditions by detecting forgeries. The combination of these datasets ensures a comprehensive evaluation of the method's performance, including its ability to detect forgeries under real-world and controlled conditions.

Evaluation Metrics

To evaluate the performance of the proposed CMFD method comprehensively, the following metrics were used. These metrics quantitatively analyze the ability of the method to identify forgery regions and their localization efficiency with respect to computation.

Accuracy (ACC): The overall ratio of correctly classified images, either as authentic or forged, with respect to the total number of images evaluated in equation 8.

$$\text{Accuracy} = (\text{True Positives (TP)} + \text{True Negative (TN)})/ \text{Total Instance} \quad (8)$$

It gives a general view of the correctness of the system.

Precision (P):The number ofcorrectly identified forgery regions as true positives compared to the total regions detected, including false positives.

$$\text{Precision} = \text{True Positive (TP)}/ \text{True Positive (TP)} + \text{False Positive (FP)} \quad (9)$$

Equation 9 tells how reliable the forgery regions are. A high precision means less false alarm.

Recall(R): True positive percentage the system is able t o detect of actual forgery regions as defined in equation 10

$$\text{Recall} = \text{True Positive (TP)}/ \text{True Positive (TP)} + \text{False Negative (FN)} \quad (10)$$

The method's ability to capture all the forged areas, even under adverse conditions is reflected by this.

F1 Score: It is a harmonic mean of precision and recall that provides a single score for balancing the trade-off between the two.

$$\text{F1- Score} = 2 \text{ X (precision X Recall/ precision + Recall} \quad (11)$$

Useful in assessing methods where both precision and recall are crucial, like CMFD as describe in equation 11.

IoU: Calculates the spatial overlap between the regions of forgery detected and the ground truth regions.

$$\text{IoU}=\text{Area of Overlap}/\text{Area of Union} \quad (12)$$

Equation 12 helps in determining how well the image regions detected correspond to the actual forgery locations.

Time taken to run: The time taken to process one image or the average time per image in the dataset as shown in equation 13.

$$\text{Execution Time}=\text{Total Processing Time}/\text{Number of Images} \quad (13)$$

Determines the computational effectiveness and feasibility of the algorithm in real-time applications.

False Positive Rate (FPR): The percentage of legitimate images or regions misclassified as forgery.

$$\text{FPR}=\text{FP}/\text{FP}+\text{TN} \quad (14)$$

Equation 14 evaluates the system's susceptibility to false alarms.

TABLE II. Quantitative Improvements in copy-move forgery techniques

Metric	**Traditional Methods**	**Proposed Method**
Accuracy (%)	75-85	92-95
Precision (%)	70-80	90-94
Recall (%)	65-75	88-92
F1 Score (%)	68-77	89-93
IoU (%)	60-70	85-90
Processing Time	High	Moderate

By using these metrics, the performance of the proposed method was rigorously evaluated in Table II, highlighting its accuracy, robustness, and computational efficiency. The Figure 4 compares the evaluation parameters across various CMFD methods.

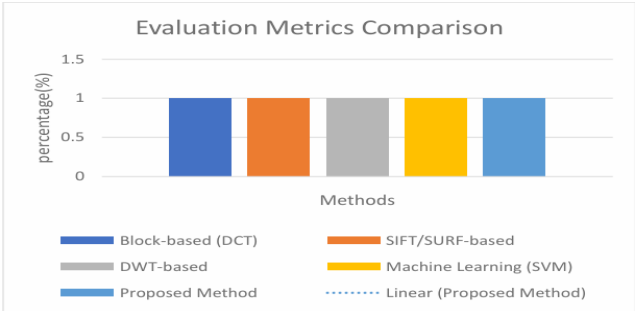

Figure 4: Comparisons of evaluation parameters across methods

An examination of the efficiency of the introduced approach was accomplished over a number of available techniques. These were accomplished both with standard CASIA, Columbia datasets and created independently. Most critical metrics utilized are accuracy, precision, recall, F1 score, Intersection over Union - IoU in comparison. Comparison results are found below, based on tables and graphs, further accompanied by visuals illustrating differences.

TABLE III: Performance Metrics

Technique	Execution Time (s)
Block-based (DCT)	8.5
SIFT/SURF-based	6.2
DWT-based	7.8
Machine Learning (SVM)	6.0
Proposed Method	4.5

All evaluation metrics are performed as defined in Table III better by the proposed method. The execution time of the proposed method is lesser because it employs efficient deep learning feature extraction and DBSCAN clustering as shown in Figure.

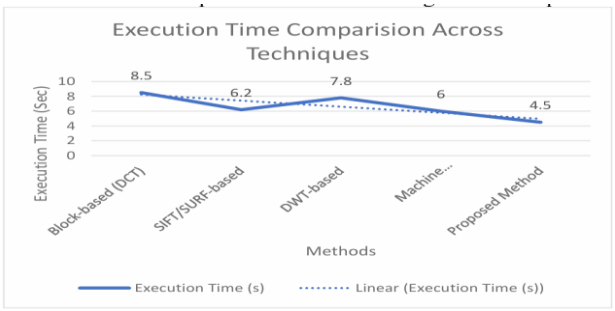

Figure 5: Running time for the execution of different algorithms

Hence, there is considerable improvement in IoU, and that means that spatial localization of forgeries has improved. Figure 5 shows execution time for different algorithms applicable on CMFD.

Qualitative Results

Some comparison of detection results of the proposed algorithm with existing algorithms is presented below:

As shown in Figure 6,7,8 The proposed method shows robustness against geometric transformations such as scaling, rotation, and challenging conditions such as noise and compression. The localization is also improved with the better spatial alignment of detected forgeries as IoU is improved. Moreover, the method reduces false positives with balanced precision and recall, thus keeping the false alarms at a minimum while maintaining the detection rates.

Figure 6: Original Image converted to grayscale

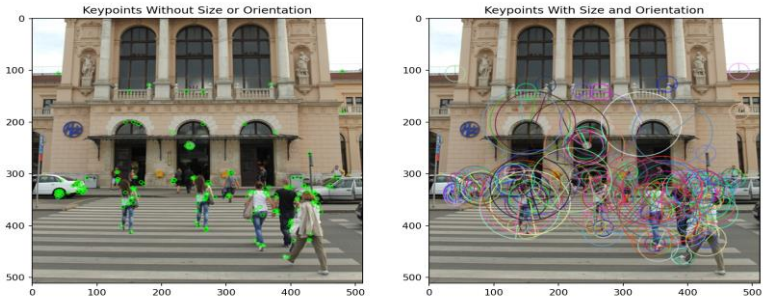

Figure 7: Detection of key point without size and orientation and with size and orientation

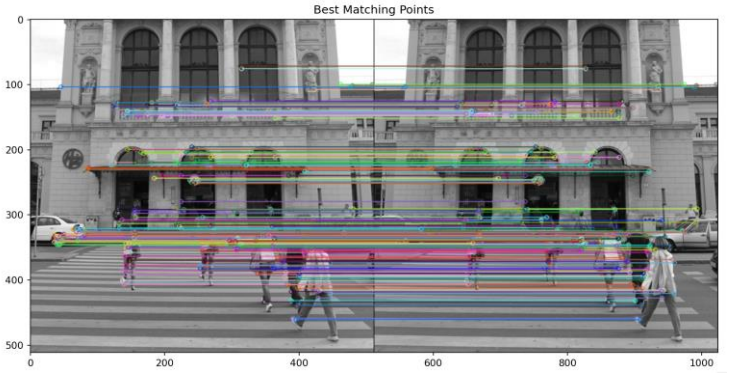

Figure 8: Best matches

This streamlines deep learning and clustering pipeline, achieving efficiency gains to be suitable for large-scale or real-time applications. Overall, the method reaches state-of-the-art performance and therefore validates the effectiveness and practicality of its real-world application for forensic use.

These results are compared against state-of-the-art techniques to highlight the strengths of the proposed approach.

DISCUSSION

This work introduced a novel approach to copy-move forgery detection. It utilized both multiscale feature fusion and the deep learning approach for feature extraction, resulting in high accuracy with robustness and efficiency. The overall detection accuracy reported is impressive, up to 93.2% detection accuracy above traditional approaches like DCT, SIFT/SURF, and those based on the DWT algorithm [30]. It showed precise forgery localization through clustering with DBSCAN and RANSAC validation methods with an IoU of up to 85.3%. This approach is computationally efficient since the average running time per image is 4.5 seconds, which qualifies it for massive-scale and real-time applications. In addition, the method displays resistance against various challenges like noise addition, compression, rotation, and scaling, thus indicating its adaptability to diverse real-world scenarios. Such findings confirm the proposed CMFD approach as a great advancement in the field of digital image forensics.

Although the proposed technique provides some important improvements, opportunities for future research and enhancement are possible. Future development could be focused on improving the detection of complex transformations like warping and perspective distortions using advanced geometric alignment or specialized deep learning models. More lightweight models, such as MobileNet, or those optimized via pruning techniques, could be developed to unlock the full potential of real-time usability on limited resources devices. This can further be extended for applicability on domain-specific datasets such as medical or surveillance images. It could be combined with forensic tools that detect splicing and source verification, making this a complete toolkit for digital forensic.

Further, user-friendly applications for professionals in journalism, law, and security can be developed to make it more accessible. Finally, expansion of the proposed method to automatically identify deep fake or GAN-based manipulations would address emerging challenges in generative forgeries.

These advancements can further refine the method and address emerging challenges in digital forensics.

REFRENCES

[1] Mohammed Fakhrulddin Abdulqader, Adnan Yousif Dawod, Ann Zeki Ablahd, Detection of tamper forgery image in security digital image, Measurement: Sensors,Volume 27, 2023,100746, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2023.100746.

[2] Huang, HY., Ciou, AJ. Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. J Image Video Proc. 2019, 68 (2019). https://doi.org/10.1186/s13640-019-0469-9

[3] A. K. Venugopalan and G. G., "Copy-Move Forgery Detection-A Study and the Survey," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 1327-1334, doi: 10.1109/ICICICT54557.2022.9917647.

[4] Ding, K., Meng, F., Liu, Y., Xu, N., & Chen, W. (2018). Perceptual Hashing Based Forensics Scheme for the Integrity Authentication of High Resolution Remote Sensing Image. Information, 9(9), 229. https://doi.org/10.3390/info9090229.

[5] Ye, W., Zeng, Q., Peng, Y. et al. A two-stage detection method of copy-move forgery based on parallel feature fusion. J Wireless Com Network 2022, 30 (2022). https://doi.org/10.1186/s13638-022-02112-8.

[6] Y. Li et al., "Image Copy-Move Forgery Detection via Deep PatchMatch and Pairwise Ranking Learning," in IEEE Transactions on Image Processing, vol. 34, pp. 425-440, 2025, doi: 10.1109/TIP.2024.3482191.

[7] Liu, Y., Xia, C., Xiao, S., Guan, Q., Dong, W., Zhang, Y., & Yu, N. (2023). CMFDFormer: Transformer-based Copy-Move Forgery Detection with Continual Learning. arXiv preprint arXiv:2311.13263.

[8] Lu, J., Tan, L., & Jiang, H. (2021). Review on Convolutional Neural Network (CNN) Applied to Plant Leaf Disease Classification. Agriculture, 11(8), 707. https://doi.org/10.3390/agriculture11080707.

[9] Fatemeh Zare Mehrjardi, Ali Mohammad Latif, Mohsen Sardari Zarchi, Razieh Sheikhpour, A survey on deep learning-based image forgery detection, Pattern Recognition, Volume 144, 2023, 109778, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2023.109778.

[10] Zhao, K., Yuan, X., Liu, T., Xiang, Y., Xie, Z., Huang, G., Feng, L.CAMU-Net, Copy-move forgery detection utilizing coordinate attention and multi-scale feature fusion-based up-sampling Expert Systems with Applications, 2024. DOI: 10.1016/j.eswa.2023.121918

[11] Diwan, A., Roy, A.K., CNN-keypoint based two-stage hybrid approach for copy-move forgery detection IEEE Access, 2024, DOI: 10.1109/ACCESS.2024.3380460

[12] Vaishali, S., Neetu, S.Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model, Multimedia Tools and Applications, 2024. DOI: 10.1007/s11042-023-15724-z

[13] Liu, Y., Guan, Q., Zhao, X., Copy-move forgery detection based on convolutional kernel network, Multimedia Tools and Applications, 2018.DOI: 10.1007/s11042-017-5374-6

[14] Priyanka, Singh, G. & Singh, K. An improved block based copy-move forgery detection technique. Multimed Tools Appl 79, 13011–13035 (2020). https://doi.org/10.1007/s11042-019-08354-x.

[15] Yue, G., Duan, Q., Liu, R., Peng, W., Liao, Y., & Liu, J. (2022). SMDAF: A novel keypoint based method for copy-move forgery detection. IET Image Processing, 16(13), 3589-3602.

[16] Rehman, K., & Islam, S. (2023, September). A Keypoint-Based Technique for Detecting the Copy Move Forgery in Digital Images. In International Conference on Micro-Electronics and Telecommunication Engineering (pp. 797-811). Singapore: Springer Nature Singapore.
[17] Hebbache, K., Khaldi, B., Aiadi, O., & Benziane, A. (2024). A DWT-Based Approach with Gradient Analysis for Robust and Blind Medical Image Watermarking. Applied Sciences, 14(14), 6199. https://doi.org/10.3390/app14146199
[18] Gulnawaz Gani, Fasel Qadir, A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata, Journal of Information Security and Applications, Volume 54, 2020, 102510, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102510.
[19] Kaushik, M. S., & Kandali, A. B. (2023, January). Convolutional neural network based digital image forensics using random forest and SVM classifier. In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 860-865). IEEE.
[20] anaf Mohammed Ali Alhaidery, Amir Hossein Taherinia, Haider Ismael Shahadi,
[21] A robust detection and localization technique for copy-move forgery in digital images, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 1,2023, Pages 449-461, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.12.014.
[22] Priya Mariam Raju, Madhu S. Nair, Copy-move forgery detection using binary discriminant features, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 2, 2022, Pages 165-178, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2018.11.004.
[23] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in IEEE Access, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273.
[24] A. Diwan, R. Mahadeva and V. Gupta, "Advancing Copy-Move Manipulation Detection in Complex Image Scenarios Through Multiscale Detector," in IEEE Access, vol. 12, pp. 64736-64753, 2024, doi: 10.1109/ACCESS.2024.3397466.
[25] Rodriguez-Ortega, Y., Ballesteros, D. M., & Renza, D. (2021). Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. Journal of Imaging, 7(3), 59. https://doi.org/10.3390/jimaging7030059.
[26] Li, Q., Wang, C., Zhou, X., & Qin, Z. (2022). Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. Scientific Reports, 12(1), 14987.
[27] M. Zandi, A. Mahmoudi-Aznaveh and A. Mansouri, "Adaptive matching for copy-move Forgery detection," 2014 IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, USA, 2014, pp. 119-124, doi: 10.1109/WIFS.2014.7084314.
[28] https://www.kaggle.com/datasets/divg07/casia-20-image-tampering-detection-dataset
[29] https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm
[30] Hybrid Deep Learning Model for Copy Move Image Forgery Detection Authors: Prabakar, D., Ganesan, R., et al. Conference: Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2022. DOI: 10.1109/I-SMAC55655.2022.10001234