Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 10, 704-720
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i10.10525

Image integrity and tampering detection: A hybrid approach to copy-paste forgery detection using ORB-SSD and CNN

Priti Badar[1]*, Geetha G[2], Mahesh T. R.[3]
[1,2,3]Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bangalore, India; priti_badar@yahoo.co.in, Priti.b@cmrit.ac.in (P.B.).

Abstract: Digital image manipulation, especially copy-paste forgery, presents significant challenges to maintaining the authenticity and credibility of visual content in the digital age. As image editing techniques become increasingly sophisticated, there is a pressing need for effective and reliable methods to detect and localize manipulated regions within images. This study introduces an innovative approach that combines ORB (Oriented FAST and Rotated BRIEF) and SSD (Single Shot Detector) algorithms for key point detection and feature matching, complemented by a CNN-based image authentication process. The low-dimensional binary descriptors generated by the ORB method enhance computational efficiency, while the integration of SSD ensures precise localization of fraudulent areas. Experimental evaluations, using metrics such as precision, recall, and F1-score, demonstrate the proposed method's superior performance compared to existing state-of-the-art techniques, achieving a favorable balance between accuracy and processing speed. This approach effectively detects copy-paste forgeries, even in complex scenarios, providing a reliable tool for identifying altered digital images. The methodology has potential applications in digital forensics, copyright protection, and secure multimedia content verification.

Keywords: *Copy move, Oriented FAST and Rotated BRIEF, Scale-Invariant feature transform, Single shot detection.*

1. Introduction

Images hold considerable importance in multiple facets of contemporary life, frequently functioning as verification or evidence in various situations. The swift progress in computer networks and digital image processing technologies has simplified the management of digital photographs, even for those with less technical knowledge. The availability of freely available technologies allows individuals, irrespective of proficiency, to modify photos. Consequently, digital photographs may be altered either deliberately or inadvertently.

Image tampering denotes the intentional manipulation of an image to unlawfully or detrimentally modify its content. The deliberate modification of photographs for nefarious purposes is a prevalent definition of image tampering. This method can fulfill multiple functions, including comic effects, political propaganda, entertainment, or augmenting a subject's appeal, perhaps resulting in significant repercussions. Digital image tampering detection has become a crucial domain in image processing, concentrating on verifying the integrity of digital images. A principal objective of picture tampering detection is to ascertain the authenticity or deceitfulness of an image. The manipulation of images commenced in the early 1900s, mostly for political propaganda purposes. Image modification has become a prevalent phenomenon. The widespread accessibility of tools for picture enhancement, correction, modification, and recreation enables unlawful acts.

Digital images are essential to forensic investigations, criminal assessments, intelligence operations, medical imaging, insurance claims, and broadcasting. Thus, safeguarding and validating the authenticity of photographs has become increasingly important. In response to this demand, technologies for detecting image forgery have gained considerable societal significance. Over the past ten years,

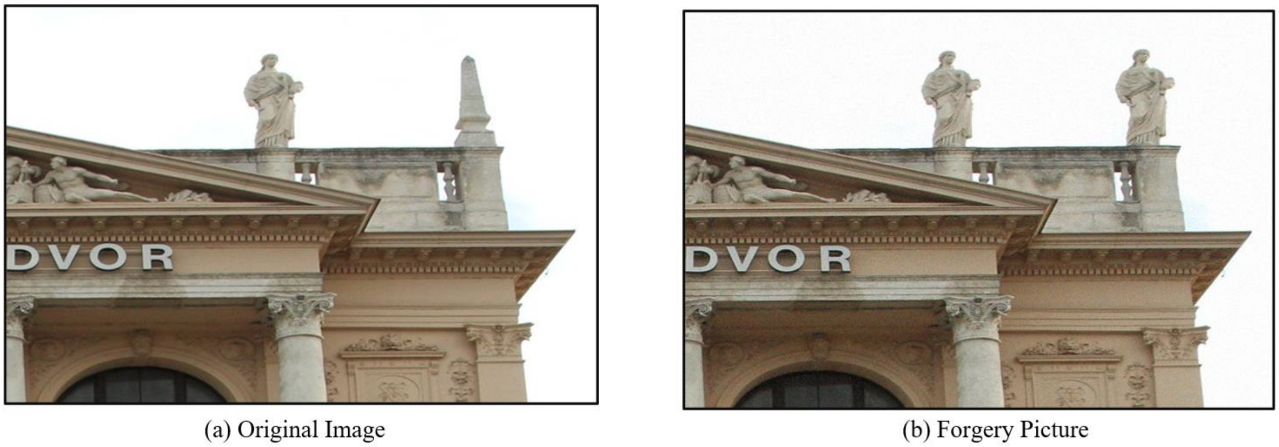
History: Received: 11 July 2025; Revised: 13 August 2025; Accepted: 18 August 2025; Published: 13 October 2025
* Correspondence: priti_badar@yahoo.co.in

significant progress has been made in methods for detecting image alterations.

1.1. Techniques for Detecting Image Manipulation

Two primary strategies for detecting picture tampering are active approaches and passive ones. Active approaches entail incorporating past evidence, such as a watermark or digital signature, into the image. These strategies seek to validate the integrity of the image. Nonetheless, a major constraint of this approach is its inapplicability to photographs from unidentified sources, as the embedded information must be pre-existing within the image. This constraint poses a considerable barrier when employing active methodologies [1].

Conversely, passive or blind image tampering detection techniques do not depend on any prior knowledge to ascertain the integrity of an image. Rather, these techniques employ picture statistics or certain image elements to detect discrepancies and alterations [2]. Among the myriad forms of tampering, copy-paste forgery, or cloning, is the most prevalent. Copy-paste forgery entails duplicating a segment of an image and inserting it into a different location within the same image. This technique is frequently utilized to obscure unwanted aspects, copy particular components, or augment the visual appeal of the image. The replicated regions may differ in dimensions and form and can be inserted repeatedly in various positions within the same image. To prevent the appearance of conspicuous artifacts in altered areas, image fragments are usually integrated seamlessly with the background. After an area is copied, it can be pasted into a new position either unchanged or modified by transformations such as rotation or scale. The duplicated and final images originate from the same source, resulting in the tampered areas exhibiting comparable qualities such as color palette, texture, dynamic range, and noise characteristics. This resemblance complicates the identification of frauds. Methods such as image splicing and copy-move forgery frequently belong to this classification of manipulation. Figure 1 represents an example of copy-paste forgery.


(a) Original Image

(b) Forgery Picture

Figure 1.
Example of Copy Paste Forgery.

With the progression of technology, various picture editing software applications have become accessible at no cost, enabling users to edit, enhance, correct, modify, and recreate photographs effortlessly. This growth engenders substantial apprehensions regarding the authentication of digital images. The simplicity of image manipulation has unintentionally enabled illegal activities, since several individuals exploit these tools to modify photographs and produce fraudulent evidence to mislead others. Under this mechanized and networked environment, the authenticity of digital photographs is increasingly under doubt. The imperative for a solution to authenticate photos and differentiate between authentic and counterfeit ones is paramount. Social media, although a potent medium for connection, discourse, and information dissemination, also presents dangers of propagating false propaganda and misleading content if not utilized judiciously. Deceptive visuals can induce confusion and even result in catastrophic consequences. Some edited photographs display evident pixilation that indicates their inauthenticity, while others are so well created that they seem completely authentic.

Digital photos are essential evidence in various domains, including forensic autopsy, criminal investigations, intelligence systems, healthcare imaging, insurance claims, and broadcasting. This highlights the essential requirement for effective techniques to maintain and authenticate photographs. As a result, the importance of picture tampering detection methods has markedly increased in society, leading to considerable progress in visual forensic approaches. While various methodologies in the literature tackle simple copy-move forging cases, many are unable to detect intricate manipulations efficiently. Block-based forgery detection techniques, which include partitioning the host image into overlapping segments and extracting information, are extensively utilized. Nonetheless, these methods encounter obstacles like protracted processing durations and failure to identify geometric modifications imposed on altered areas [3].

2. Literature Survey

A considerable body of work exists on digital picture manipulation, a critical domain within digital image forensics. Image tampering detection techniques can be categorized into two primary types: active (non-blind) approaches and passive (blind) methods. Active approaches involve the incorporation of supplementary information into the image, either during its creation or post-processing, thus requiring specialized equipment or software for detection. Conversely, passive approaches do not require embedding additional data, making them a more organic method for identifying tampering. This chapter examines numerous research studies related to image tampering detection, covering both active and passive methodologies, and presents fundamental principles in digital forensics, forgery detection in composite images, and copy-move image forgeries. Table 1 provides a summary of supplementary techniques for identifying copy-move frauds.

One notable contribution to the field involves a study that effectively conceals the original image within the LWT (Lifting Wavelet Transform) approximation band through perceptual mapping. The study underscores the necessity for robust concealment that renders tampering imperceptible to the human eye, while regions prone to detection are obscured with diminished intensity [4]. A significant study suggests an improved SURF-based method for detecting copy-paste manipulation. This method enhances the quick Hessian matrix to identify key locations, thereafter matched via the k-g2NN methodology. The study additionally estimates parameters for affine transformation, and by integrating R-RANSAC with SPRT, it eliminates disparities to identify copy-paste regions [5]. A unique CNN-based method is introduced for the automatic identification of copy-move forgeries. This model, evaluated on the MICC-F2000 benchmark dataset, exhibits enhanced efficacy over traditional techniques in detecting copy-move forgeries [6]. Another study emphasizes the comparison of extracted key points to identify copy-move frauds. It applies SIFT (Scale-Invariant Feature Transform) to extract invariant features from the image and subsequently utilizes PCA (Principal Component Analysis) to extract blocks for further analysis, thereby efficiently identifying altered regions [7]. Proposals have been made for real-time forgery detection systems, wherein the textural shape of the input image is originally eliminated. SIFT key points and descriptors are utilized to identify suspicious areas, while key point matching aids in determining if an image is manipulated. A Ciratef-based approach is subsequently utilized to localize the manufactured pixels [8]. A separate work introduces a splicing identification method utilizing the VGG-16 CNN architecture, which categorizes picture patches as genuine or fraudulent, thereby enhancing the precision of splicing detection [9]. An alternative method utilizes singular value decomposition (SVD) hashing to produce efficient hash vectors, facilitating the identification and location of picture alterations. This technique demonstrates significant sensitivity to modest structural alterations while remaining resilient to content-preserving adjustments [10]. A SIFT-based methodology for duplicate picture detection is introduced, utilizing invariant feature extraction techniques that are resilient to noise and transformations [11]. The paper presents an innovative similarity metric that integrates cosine and Jaccard indices to enhance feature matching. This method incorporates ORB (Oriented FAST and Rotated BRIEF) feature extraction, improving forgery detection efficiency through the matching of picture blocks and the assessment of similarity [12]. A novel approach utilizing the Blocking Artifact Characteristics Matrix (BACM) detects forgeries in JPEG retargeted images due to seam alterations, independent of the source image knowledge [13]. Another approach examines the application of texture descriptor-based algorithms to identify splicing and copy-move frauds. This technique enhances the focus on specific image characteristics and improves manipulation detection by converting an image to YCbCr format and applying higher-order texture descriptors and standard deviation (STD) filters to the Cb and Cr components [14]. A study introduces a deep learning-based hybrid model for identifying and pinpointing copy-paste frauds, merging densely connected networks (DenseNets) with generative adversarial networks (GANs). This hybrid model utilizes the artificial fish swarm algorithm (AFSA) to adjust the weight and bias parameters of the extreme learning machine (ELM) classifier, thereby enhancing detection accuracy [15]. Deep convolutional neural networks (CNNs) have been examined for visual forgery detection, focusing specifically on pre-processing methods and network structures. Transfer learning techniques utilized on the CASIA V2.0 dataset have been evaluated, demonstrating the efficacy of fine-tuned CNN models in identifying picture tampering [16]. A study examines the obstacles and potential solutions in deep learning-based passive picture forensic analysis, providing insights for the development of more effective tampering detection algorithms [17]. Finally, the proposed methodology in one research addresses CFA (Color Filter Array) artifacts resulting from the interpolation of acquired pixels. The technique evaluates the probability of pixel interpolation and employs the Discrete Cosine Transform (DCT) on designated regions to identify altered areas [18]. A framework for fusion feature extraction and forgery detection is proposed, incorporating various feature extraction techniques such as SURF, PCA, and HoG (Histogram of Oriented Gradients), which are subsequently input into an optimized convolutional neural network (CNN) to enhance detection accuracy [19]. Table 1 shows some additional papers specifying their datasets and the methodology used.

Table 1.
Copy-Move Forgery Detection Techniques.

Author	Method	Dataset	Remark
Kaushik and Kandali [20]	Hybrid features - NCA (Neighborhood Component Analysis) - SVM (Support Vector Machine) method	CASIA 1	This article suggests a highly accurate forgery detection method. The hybrid features-NCA-SVM technique has the highest accuracy of 98.00% on MICC-F220 and 97.62% on CASIA 1. These results demonstrate the method's reliability and versatility in detecting copy-move forgeries across datasets.
Fu, et al. [21]	Accelerated robust features (SURF) and KAZE (A-KAZE) are used to extract descriptive features. The density-based spatial clustering of applications with noise (DBSCAN) method reduces erroneous positives and incompatible groups.	CoMoFoD	Ardizzone and CoMoFoD datasets tested the suggested method. Results indicated that the technique was resistant to post-processing procedures such as alteration, scaling, and noise accumulation, and improved forgery detection by 95% in smooth regions while reducing computing cost.
Asghar, et al. [22]	Support Vector Machine (SVM) combined with FFT-DRLBP (Fast Fourier Transformation - Discriminative Robust Local Binary Patterns)	CASIA 1 + CoMoFoDS	This work extensively tests the approach using benchmark datasets to validate it. It achieved 99.21% accuracy on two challenging datasets.
Diaa [23]	Simple Linear Iterative Clustering (SLIC) algorithm, Speeded Up Robust Features (SURF) detector, Generative Adversarial Network (GAN)	CoMoFoD + MICC F220	The approach was tested against scaling, rotation, blurring, and JPG compression. Test results showed that the suggested method detected various CMFs with 91.41% accuracy. Finally, the proposed method was compared to cutting-edge methods.
Chaitra and Reddy [24]	Fractional Leader Harris Hawks Optimization (FLHHO)-based Deep Convolutional Neural Network (CNN)	Unknown	Deep CNN is qualified using pre-trained GoogLeNet parameters in this article to detect several forgeries. Additionally, Fractional Leader Harris Hawks Optimization (FLHHO) is created to alter Deep CNN bias and weights. The approach is evaluated using metrics like 93% testing accuracy.
Aydın [25]	Hessian and Raw patch feature extraction	GRIP and the image manipulation dataset (IMD)	This study used the Image Manipulation Database (IMD) and GRIP for detection and characterization. The data show that the approach achieved 100% F1 scores for the GRIP dataset and 92.13% for the IMD database.

Numerous methods and procedures have been suggested for identifying digital image tampering, each possessing distinct advantages and drawbacks. Although block-based and key point-grounded techniques demonstrate potential, they continue to face considerable obstacles. Block-based methods have difficulties in identifying geometric modifications because of overlapping block divisions, resulting in inefficiencies in both processing time and accuracy. Conversely, key point-grounded methodologies, while proficient in detecting geometric alterations, frequently exhibit inadequate localization abilities and subpar true positive rates (TPR). Moreover, numerous current approaches exhibit constrained computing efficiency and demand considerable resources, rendering them unfeasible for real-time and large-scale applications. Despite ongoing developments in machine learning and deep learning, these issues endure, highlighting the necessity for more robust, efficient, and scalable forgery detection techniques. Below are the major gaps identified in existing forgery detection methods.

1. Contemporary block-based methods encounter difficulties in detecting geometric alterations in

forging areas due to overlapping block divisions, resulting in inefficiencies in processing time and precision.

2. Numerous current methodologies exhibit insufficient localization proficiency for identifying forgery areas, especially in instances of intricate manipulations or geometric modifications.
3. The constrained computing efficiency and substantial resource demands impede the practical implementation of several forgery detection techniques.

This major contribution is the development of a novel forgery detection system that addresses the shortcomings of block-based and key point-based techniques. The suggested method improves both the true positive rate (TPR) and computational efficiency by merging the ORB algorithm for key point extraction with the SSD methodology for accurate localization. This method proficiently tackles the difficulties of identifying geometric modifications and large-scale forgery detection, providing a resilient and scalable solution. Primary contributions of the research work are as follows:

1. This research presents a solution to overcome the shortcomings of block-based and key point-grounded forgery detection methods. Although key point-grounded approaches are proficient in identifying geometrical changes, they exhibit inadequate localization capabilities and subpar true positive rates (TPR). The suggested methodology aims to enhance TPR data and computational efficiency.
2. The proposed system utilizes the ORB algorithm to identify salient points in an image and applies the SSD technique to pinpoint the altered region. This technique guarantees accurate detection of fraudulent areas while withstanding geometric alterations.
3. By incorporating these sophisticated methodologies, the suggested method attains a balance between precision and computational expense, providing a more efficient solution for forgery detection.

3. Methodology

This text presents a novel approach for identifying copy-paste forgeries in digital images. The method relies on key point detection, utilizing a combination of SSD and ORB for localization and key point extraction, followed by classification via CNN. The utilization of SSD and ORB reduces both the wrong matching rate and the computational and temporal complexity. Figure 2 illustrates the overall framework of the proposed methodology. The CoMoFoD dataset was utilized to evaluate the approach. The CoMoFoD collection contains images with dimensions of 512 by 512 pixels. Thirty copy-move manipulated photographs and their associated genuine ones were used to evaluate forgery detection. The initial phase involves capturing a picture and extracting features that can be used for forgery detection. Feature identification is the process of recognizing abstractions within visual data and evaluating the presence of a given feature at each location in the image. A notable region within an image is referred to as a feature. Our approach employs the ORB algorithm for rapid and precise key point extraction and the SSD algorithm for object detection. Point correspondences are frequently established by contrasting the key points of two distinct images. Key locations within a single image are supplied to a CNN classifier to detect copy-move frauds. Analogous points indicate regions of an image that have been modified. The fabricated regions can subsequently be derived by analyzing the vicinity of the designated places.

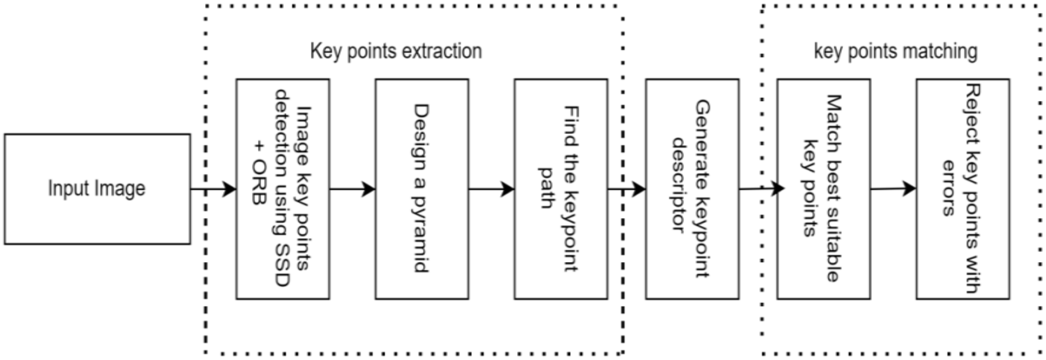

Input Image
Key points extraction
Image key points detection using SSD + ORB
Design a pyramid
Find the keypoint path
Generate keypoint descriptor
key points matching
Match best suitable key points
Reject key points with errors

Figure 2.
Image matching based on ORB and SSD algorithm

Detecting copy-move attacks with ORB and SSD in this study. SSDs' efficiency and speed are important benefits since they use one network. Due to their pre-trained base network, SSDs can access a multitude of tagged data for picture categorization. Even when trained on small datasets, they achieve high accuracy. SSDs have limitations. First, they are less accurate than R-CNN approaches. SSDs cannot benefit from the context and data provided by several networks when using a single network [26]. Another problem is that SSDs are sensitive to picture dimensions. SSDs may have problems detecting items that are significantly smaller or larger than the training dataset since the additional layers recognize objects at different scales.

The SSD algorithm provides the object's category probability and position coordinate value immediately and includes target location and prediction into the forward operation. One-step detection yields the final result. As detection speed increases, placement precision falls. SSD algorithm uses shallow high-resolution feature layer. This layer's lack of feature expression may cause missed and inaccurate detections of small targets. This work improves SSD object detection by using ORB to avoid the concerns above. The network structure is shown after fusing neighboring feature maps. A feature detection and description algorithm is ORB. A descriptor is computed for each corner of an input pyramid. It then returns each feature's bitstring descriptor and coordinates from the input's highest resolution base picture. ORB outperforms other detection and description methods because of its simplicity and computing efficiency.

3.1. Image Pre-Processing for Copy- Move Attack

The colored image is first grayscaled. A computer using RGB displays color. Most people use RGB, or Red-Green-Blue. The name implies that this paradigm represents colors with red, green, and blue values. Globally, most digital screens use RGB. Grayscale is the simplest way to express colors because it employs only brightness. Lightness runs from 0 (black) to 255 (white). RGB images are more informational than grayscale ones. Because grayscale images are faster and require less space, they are often employed in image processing, especially for complex computations. Consider a color as having the RGB value (R, G, B), where R, G, and B are integers between 0 and 255. Equation 1 calculates C, the grayscale weighted average.

$$C = 0.299R + 0.587G + 0.114B \quad (1)$$

3.2. Feature Extraction Module for Copy-Move

This module divides the pre-processed image into overlapping, pre-sized parts. Figure 2 shows how ORB (Oriented FAST and Rotated BRIEF) and SSD (Single Shot Detector) are fused to extract the relevant features [33SSD uses VGG16 for feature maps]. The Conv4_3 layer identifies objects. ORB combines the best of BRIEF descriptor and FAST key point detector with a few additional features to improve performance. Qualities from the Accelerated Segment Test (FAST) identify picture features. Pyramids generate multiscale features. The suggested method uses SSD and ORB fusion to extract accurate features for quick image manipulation detection. Pixel values range from 0-255 in the grayscale image array, with rows and columns denoted by m and n. The data is separated into 8 × 8 subarrays with severity values from 8 rows × 8 columns sequences. For finding picture interest key points, [27] suggested the FAST technique. Picture interest points are well-defined pixels that can be reliably identified. Interest points should be repeated in multiple images and contain lots of local information. Interest point detection is used in object recognition, tracking, and image matching. FAST compares the lighting of a pixel (p) in an array to the 16 pixels that form a trivial circle around it. From the circle pixels, three classes are created: similar to p, darker than p, and lighter than p.

Key features are pixels at least eight pixels lighter or brighter than p, as seen in Figure 3. Thus, rapid important spots reveal a picture's edges.

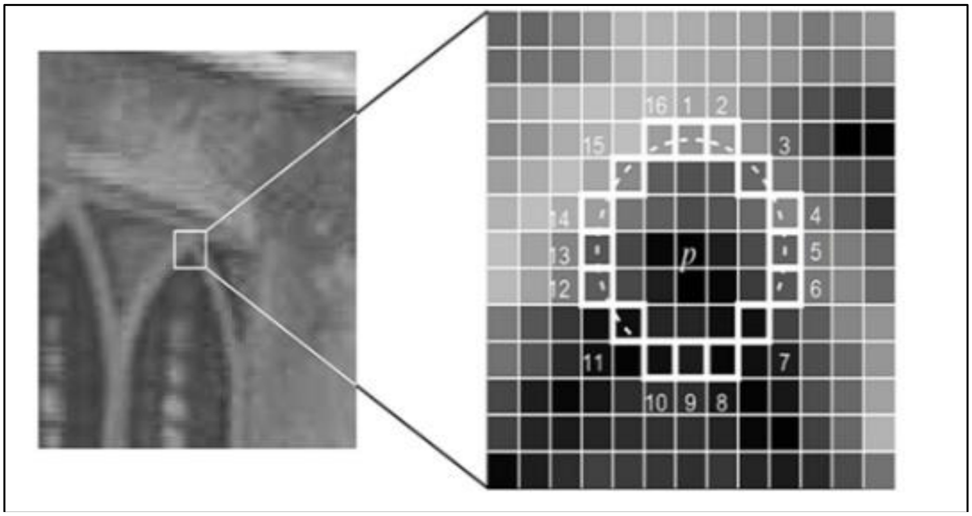


Figure 3.
FAST corner extraction diagram.

Multiscale and orientation elements are inattentive from FAST characters. The ORB method uses a multiscale photo pyramid. Picture pyramids are multiscale depictions of a single image made of many photos with different resolutions. A lower-resolution image is displayed for each pyramid tier. ORB produces a pyramid in Figure 3 and uses the quick approach to highlight key elements. ORB effectively finds crucial spots at a new scale by discovering them at every level. Thus, ORB is fractional scale invariant [28]. After identifying essential areas, assign a left or right orientation based on surrounding intensity. The intensity centroid helps ORB discern intensity changes. The intensity centroid vector assumes an orientation since corner intensity is different from center intensity.

Initially, a patch's occurrences are described as eq. 2:

$$m_{p,q} = \sum\nolimits_{x,y \epsilon B} x^p y^q \, I(x,y),\ p,q = (0.1) \tag{2}$$

The ORB descriptor - Patch's instant specification

Applying these instances, may identify the centroid, or patch's "center of mass," as given in eq. 3:

$$C = \left(\frac{m_{10}}{m_{00}}, \frac{m_{01}}{m_{00}}\right) \tag{3}$$

The ORB algorithm attribute represents the patch's center of mass. We can create a vector that goes from the centroid (OC) to the corner's center (O). Eq. 4 will provide the patch's orientation:

$$\theta = atan2\ (m_{01}, m_{10}) \tag{4}$$

Here's an example to assist in clarifying the process. Once the patch orientation is known, we may compute the descriptor and turn it in a canonical direction to provide rotation invariance, as shown in Figure 4.

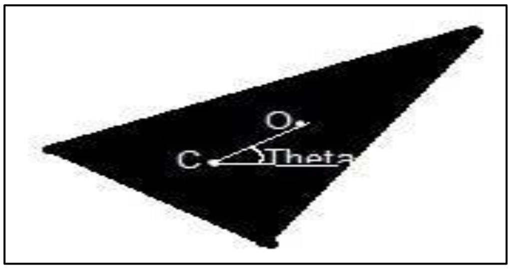


Figure 4.
Theta description.

3.3. BRIEF: Binary Robust Independent Elementary Feature

Brief converts fast algorithm features into binary feature vectors to represent an object. Binary structure vectors, also termed binary structure descriptors, are features with only 1s and 0s. A feature vector, a 128–512-bit string, labels each key point as shown in Figure 5.

Binary feature vector
V1 = [01011100100110……
V2 = [10010100110100……
V3 = [11000100101110……
V4 = [01011111100100……

Figure 5.
Binary Vector.

Using a Gaussian kernel to normalize the image and reduce descriptor sensitivity to high-occurrence noise is a simple start. Next, randomly select two pixels from a preset neighborhood around that critical point. A patch is a square with set pixel widths and heights around a pixel. The first pixel in the arbitrary pair is chosen using a Gaussian distribution centered at the key point and with a maximum deviation or spread of sigma. The second pixel in the random pair is picked from a Gaussian spectrum centered on the initial pixel with a two-sigma deviation. If the first pixel is lighter than the next, it assigns 1 [29].

Choose another pair at random and assign them a value. For a 128-bit vector key point, briefly repeat this technique 128 times. Create a vector like this for each image's main point quickly. Since BRIEF isn't rotation-invariant, ORB uses BRIEF. ORB maintains BRIEF speed to accommodate this functionality [29].

Think of a portion of a smoothed image, p as described in eq. 5. The definition of a binary examination τ is:
where τ (p; x, y) is well-defined as:

$$\tau(p; x, y) = \begin{cases} 1: p(x) < p(y) \\ 0: p(x) \geq p(y) \end{cases} \tag{5}$$

P(x) is the concentration value at pixel x.

BRIEF's matching performance drastically declines at in-plane rotations of a few degrees. ORB provides BRIEF's main point orientation guiding principles. Eq. 6 shows the 2-x n matrix needed for every combination of n binary attribute examinations at location (x_i, y_i).

$$s = \begin{pmatrix} x1, \ldots & x_n \\ y1, \ldots & y_n \end{pmatrix} \tag{6}$$

It uses the matching rotation matrix Rθ and the patch orientation to construct a directed version S of S, as provided by eq. 7:

$$S_\theta = R_\theta S \tag{7}$$

Now, the steered BRIEF operator is as follows, according to equation 8:

$$g_n(p, \theta) = f_n | (x_i, y_i) \in S_\theta \tag{8}$$

After discretizing the angle in 2π/30 (12 degrees) steps, a lookup database with recomputed BRIEF patterns is created. The descriptor will be calculated using the right set of points Sθ, assuming constant key point orientation θ between views. Figure 6 shows the sequence of the suggested picture classification approach. Picture categorization is a crucial machine learning task because of its importance in modern technology. It involves labeling or classifying a full picture using previously defined photographs as training data. The approach may appear straightforward, but it analyzes images pixel-by-pixel to find the appropriate label. We obtain evidence and understanding to make credible decisions and achieve results. The classifier categorizes images to distinguish between original and modified photos in image tampering. Our suggested approach uses CNN classifier fusion and pooling to accurately recognize and categorize faked photos. Figure 6 shows the suggested system's flow, which converts colored images to grayscale. Separating this grayscale image into 8x8 block subarrays allows SSD and ORB fusion to extract precise features. For further dimensionality reduction, CNN model pooling layer will receive extracted features. This layer is regularly added to covnets to reduce volume, speed up computation, reduce memory usage, and prevent overfitting. CNN predicts and classifies picture alterations.

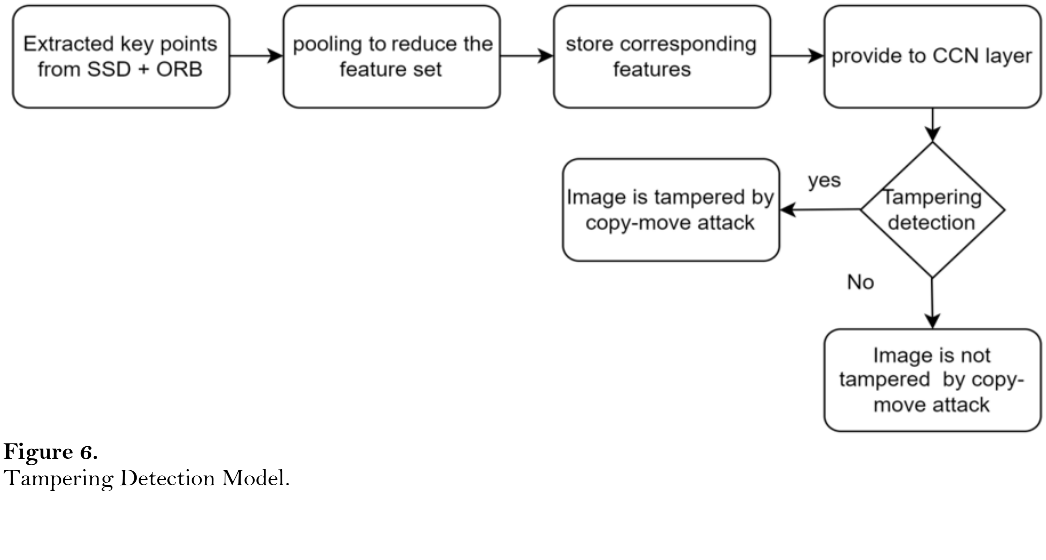

Extracted key points from SSD + ORB
pooling to reduce the feature set
store corresponding features
provide to CCN layer
Tampering detection
yes
Image is tampered by copy-move attack
No
Image is not tampered by copy-move attack

Figure 6.
Tampering Detection Model.

DOI: 10.55214/2576-8484.v9i10.10525

Table 2 compares four machine learning methods for detecting copy-paste fraud in images [30]: k-Nearest Neighbors (kNN), Linear Regression (LR), Naïve Bayes (NB), and Convolutional Neural Network (CNN).

Table 2.
Evaluation Results of Copy-Move Forgery Detection Classifier.

Metric	**KNN (%)**	**LR (%)**	**NB (%)**	**CNN (%)**
Precision	95.11	76.21	82.54	95.46
Recall	88.46	69.72	77.41	90.62
Accuracy	81.81	63.23	72.27	85.79
F1-Score	97.11	75.21	82.54	93.46

4. Results

Evaluation of the advantages and disadvantages of a feature matching algorithm is chiefly reliant on its performance evaluation. Evaluating an algorithm's performance using a singular benchmark is problematic due to the variability in image matching application contexts, goals, and research fields. To comprehensively evaluate the findings and identify the algorithm with optimal overall performance, it is frequently essential to employ a variety of indicators. The precision of forgery detection is evaluated at both the pixel and image levels through three principal performance metrics: Accuracy, Recall, and F1 Score [31-34].

Precision: indicates the likelihood that the regions identified are, in fact, the false regions, as stated in eq. 9.

$$precision = \frac{I_{correct}}{I_{all}} \tag{9}$$

Matching criteria also have an impact on precision. The accuracy and quantity of correct matches increase with the strictness of the matching criteria.

Recall: denotes the likelihood that the zones of fraud are identified, as stated in Eq. 10.

$$recall = \frac{I_{correct}}{I_{should}} \tag{10}$$

F1 Score: This score generates a signal value by integrating recall and precision. It is computed using Eq. 11.

$$F1 = 2\,X\,\frac{precision\,.\,recall}{precision + recall} \tag{11}$$

As previously mentioned, the recall is the likelihood that a tampered image will be identified, and the precision is the likelihood that a discovered tampering is actually a counterfeit. Better performance is typically indicated by higher recall and precision. The technique is assessed using CoMoFoD's small picture category. The forged photos were created by translating, rotating, resizing, and distorting the source photos. Each image set also includes blurry photos, photos with additional noise, photos with altered brightness, photos with reduced color, and photos with adjusted contrast. Figure 6 contrasts the proposed methodology with contemporary benchmarks. The execution timings for SIFT, ORB, and the proposed approach are presented in Figure 7. Table 3 shows the evaluation of the Copy-Paste Tampering Detection Algorithms.

Table 3.
Outcomes of the Copy-Paste Tampering Detection Algorithms' Evaluation.

Method	Precision (%)	Recall (%)	F1 Score (%)	Time (sec)
GLCM [8]	93.75	7.25	93.75	32.76
Mask-RCNN [13]	98.12	95.85	96.97	45
VGG16 & Buster Net DNN [32]	78.22	73.89	75.98	NA
Proposed Methodology	94	92	95.13	5.66

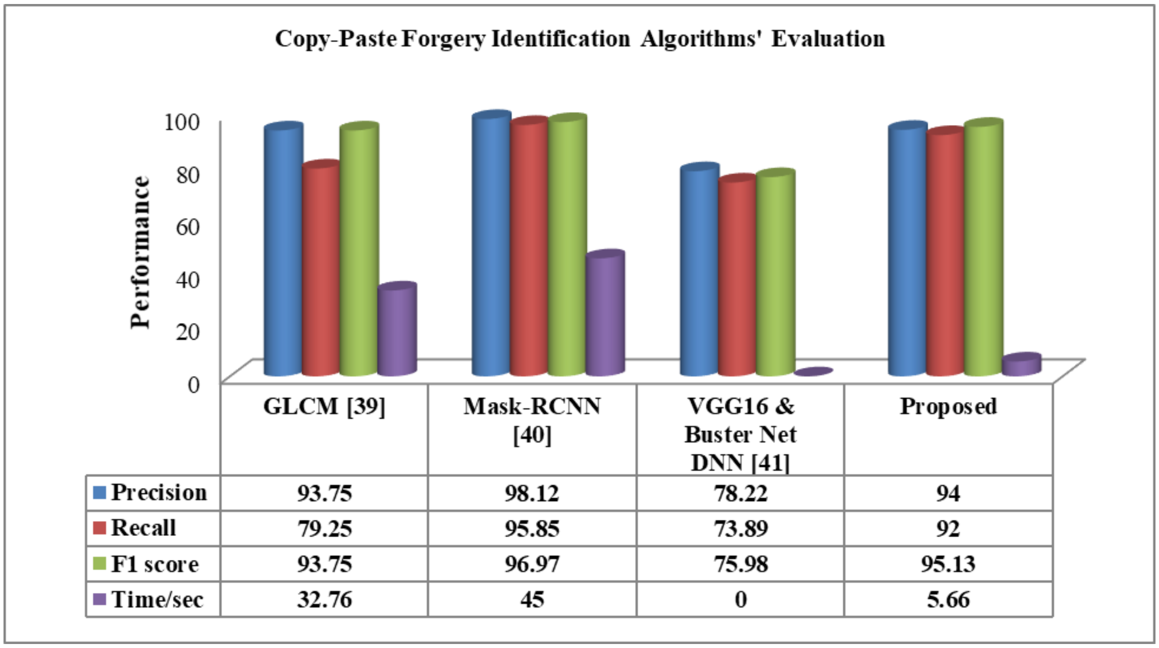


Figure 7.
Comparison of SIFT, ORB With Proposed Method's Performance.

The Table 4 shows the performance of SIFT, ORB, and the proposed method based on key points, dataset, and time consumption. Each method was tested on a specific dataset, with key points extracted to detect forgeries. Time consumption, measured in seconds, was recorded to assess the efficiency of each method. This comparison highlights the strengths and limitations of each approach in terms of accuracy and computational efficiency, providing insight into their practical applicability for forgery detection. The suggested approach shown in Figure 8 can accomplish remarkable precision in a fair amount of time.

Table 4.
Time Spent on Feature Matching Using Various Techniques.

Method	Dataset	Key Points	Time consumption /s
SIFT	CoMoFoD	500	8.79417 sec
ORB	CoMoFoD	500	6.27471 sec
Proposed	CoMoFoD	423	5.66734 sec

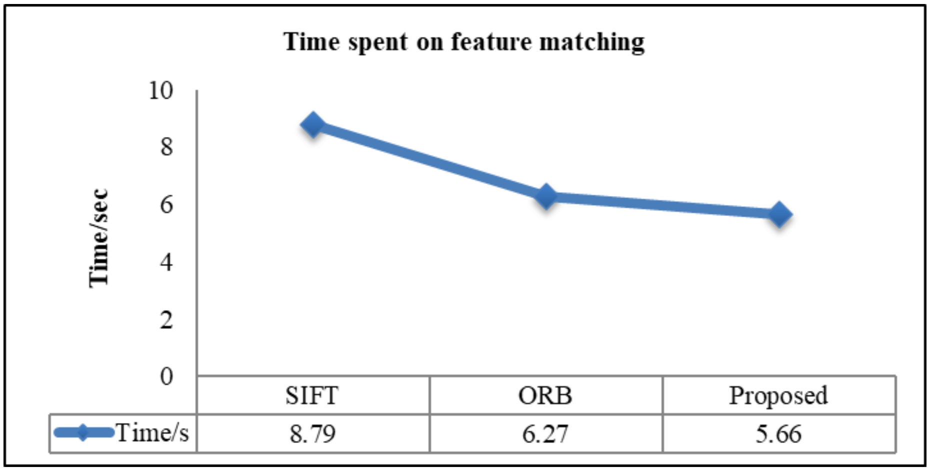
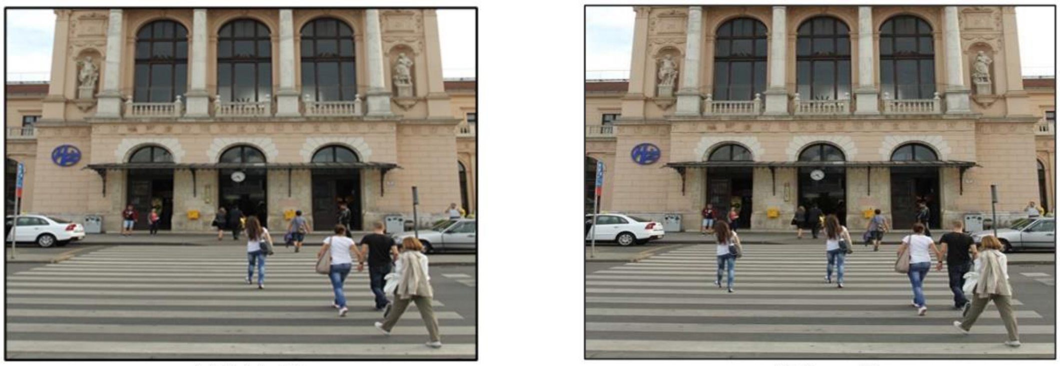


Figure 8.
Time consumption by different algorithm for feature matching.

The results section illustrates the efficacy of the suggested forgery detection system, which amalgamates ORB (Oriented FAST and Rotated BRIEF) and SSD (Single Shot Detector) methodologies. This method proficiently detects and locates altered areas inside photographs, including instances of geometric alterations. By utilizing the advantages of ORB for key point detection and SSD for accurate matching, the method guarantees precise identification of modified regions while preserving computational performance. The graphic outputs demonstrate the sequential process and illustrate the algorithm's capacity to recognize and localize forged areas with high accuracy and dependability.

Figure 9(a) depicts the original, unaltered version of the manipulated image. It functions as a benchmark for assessing the algorithm's proficiency in reliably identifying forgeries and localizing altered areas. The image in 9(b) below depicts the manipulated input, which includes modifications deliberately implemented to evaluate the resilience of the proposed method. This serves as the benchmark for comparing the identified parts with the original forgeries and evaluating the efficacy of the detection algorithm in recognizing altered areas.


(a) Original Image

(b) Forged Image

Figure 9.
Original unaltered image vs. manipulated image.

Figure 10 depicts the recognized significant points in the altered image. Essential points, irrespective of size or position, display all identified features, perhaps encompassing extraneous information. Conversely, essential points for size and orientation encompass solely the salient elements linked with geometric changes. This contrast highlights the suggested method's capability to adeptly manage

DOI: 10.55214/2576-8484.v9i10.10525

variations in scale, rotation, and orientation.

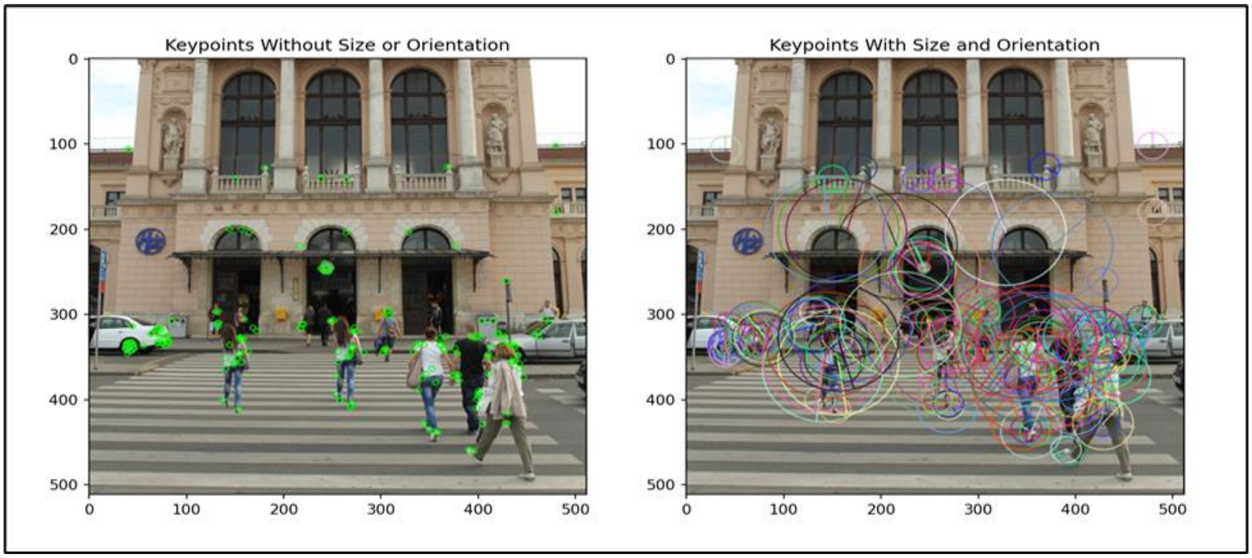

Keypoints Without Size or Orientation
Keypoints With Size and Orientation
0
100
200
300
400
500
0
100
200
300
400
500

Figure 10.
Key point identification without size or orientation and with size and orientation.

Figure 11 illustrates the relevant important points between the forged areas and their respective positions in the altered image. These matches represent regions recognized as potentially altered due to feature similarity. The visualization of matches demonstrates the efficacy of the ORB-SSD combination in identifying tampered areas, even under difficult circumstances.

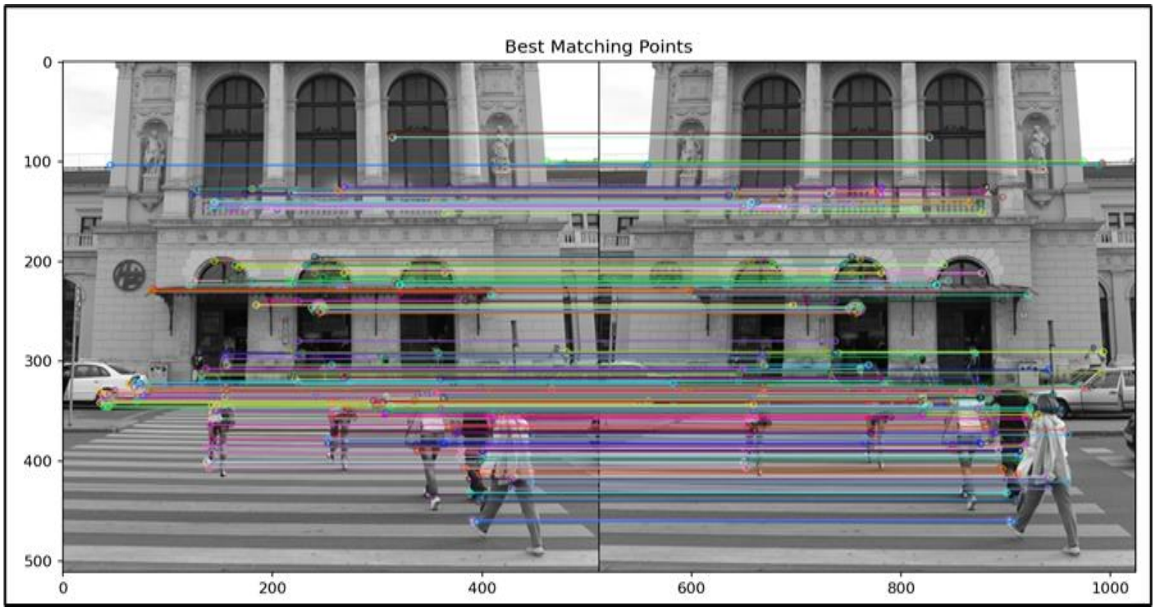


Figure 11.
Best matches.

Figure 12 functions as the benchmark for verifying the detection outcomes. It delineates the precise areas of forgeries in the image, against which the algorithm's efficacy is evaluated. Metrics such as

DOI: 10.55214/2576-8484.v9i10.10525

accuracy, precision, recall, and F1 score are computed by contrasting the identified tampered regions with the ground truth to assess the dependability and efficacy of the suggested technique.

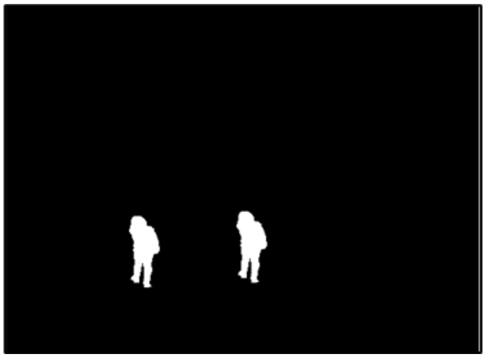


Figure 12.
Ground Truth.

5. Conclusion

The primary approach for picture manipulation is copy-paste forgery, which involves replicating specific segments of an image within the same composition. This study focused on utilizing key point-based methods to efficiently identify copy-move frauds. Using image key points enables the detection of corresponding sections within the same image. The proposed method integrates SSD (Single Shot Detector) and ORB (Oriented FAST and Rotated BRIEF) techniques to detect objects and extract their attributes. The descriptor's low-dimensional, binary characteristics reduce the computational cost of feature matching, thereby enhancing efficiency. Additionally, CNN was employed for image verification. The experimental results indicate that the proposed algorithm achieves a balanced trade-off between speed and performance, as detailed in Table 1. The key point-based features effectively handled both basic and advanced forgery scenarios, without external attacks. A comparative analysis with other advanced copy-paste forgery detection algorithms demonstrated that the proposed strategy achieved superior precision, recall, and F1-score in identifying tampered images, as shown in Table 2. These findings underscore the method's effectiveness in accurately detecting modified regions.

Future endeavors will be focused on enhancing the selection of image features by including additional forensic methodologies to tackle image forgeries on a broader scale, especially in instances requiring rotation, smoothing, and intricately textured areas. Furthermore, the existing methodology fails to address splicing a type of image manipulation that involves amalgamating components from many sources to produce a counterfeit image. Future improvements will focus on creating a robust approach for detecting splicing attacks while also addressing smooth sections in photos, thereby establishing a more comprehensive framework for tampering detection.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] A. Raja, "Active and passive detection of image forgery: A review analysis," *International Journal of Engineering Research & Technology*, vol. 9, no. 5, pp. 418-424, 2021.

[2] H.-Y. Huang and A.-J. Ciou, "Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation," *EURASIP Journal on Image and Video Processing*, vol. 2019, p. 68, 2019. https://doi.org/10.1186/s13640-019-0469-9

[3] M. F. Abdulqader, A. Y. Dawod, and A. Z. Ablahd, "Detection of tamper forgery image in security digital mage," *Measurement: Sensors*, vol. 27, p. 100746, 2023. https://doi.org/10.1016/j.measen.2023.100746

[4] T. B. Taha, R. Ngadiran, and D. B. Taha, "Perceptual mapping-based image tamper detection and recovery algorithm," *Advances in Multimedia*, vol. 2022, no. 1, p. 5771954, 2022. https://doi.org/10.1155/2022/5771954

[5] Y. Hu, Y. Wang, and X. Ai, "Image-based copy-paste tamper detection technology based on improved SURF," *IOP Conference Series: Materials Science and Engineering*, vol. 612, no. 5, p. 052017, 2019. https://doi.org/10.1088/1757-899X/612/5/052017

[6] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq, and K. Kumar, "An efficient approach for copy-move image forgery detection using convolution neural network," *Multimedia Tools and Applications*, vol. 81, pp. 11259-11277, 2022. https://doi.org/10.1007/s11042-022-11974-5

[7] P. Bhole and D. Wajgi, "An image forgery detection using SIFT-PCA," *International Journal of Engineering Research & Technology*, vol. 9, no. 6, p. Article ID IJERTV9IS060127, 2020. https://doi.org/10.17577/IJERTV9IS060127

[8] G. Tahaoglu, G. Ulutas, B. Ustubioglu, M. Ulutas, and V. V. Nabiyev, "Ciratefi based copy move forgery detection on digital images," *Multimedia Tools and Applications*, vol. 81, pp. 22867-22902, 2022. https://doi.org/10.1007/s11042-021-11503-w

[9] A. Kuznetsov, "Digital image forgery detection using deep learning approach," *Journal of Physics: Conference Series*, vol. 1368, no. 3, p. 032028, 2019. https://doi.org/10.1088/1742-6596/1368/3/032028

[10] V. Mall, A. K. Roy, and S. K. Mitra, "Digital image tampering detection and localization using singular value decomposition technique," in *2013 Fourth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG) (pp. 1-4). IEEE*, 2013.

[11] B. Patil and S. Wade, "Digital image forgery detection using SIFT feature," *International Journal of Engineering Research & Technology*, vol. 5, no. 1, pp. 1–4, 2018.

[12] X. Tian, G. Zhou, and M. Xu, "Image copy-move forgery detection algorithm based on ORB and novel similarity metric," *IET Image Processing*, vol. 14, no. 10, pp. 2092-2100, 2020. https://doi.org/10.1049/iet-ipr.2019.1145

[13] K. Wattanachote, T. K. Shih, W.-L. Chang, and H.-H. Chang, "Tamper detection of JPEG image due to seam modifications," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2477-2491, 2015.

[14] V. Srivastava and S. K. Yadav, "Digital image tampering detection using multilevel local binary pattern texture descriptor," *Journal of Applied Security Research*, vol. 17, no. 1, pp. 62-79, 2022. https://doi.org/10.1080/19361610.2021.1883397

[15] N. Krishnaraj, B. Sivakumar, R. Kuppusamy, Y. Teekaraman, and A. R. Thelkar, "[Retracted] design of automated deep learning-based fusion model for copy-move image forgery detection," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 8501738, 2022. https://doi.org/10.1155/2022/8501738

[16] A. Singh and J. Singh, "Image forgery detection using deep neural network," in *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 504-509). IEEE*, 2021.

[17] S. Manjunatha and M. M. Patil, "Deep learning-based technique for image tamper detection," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1278-1285). IEEE*, 2021.

[18] E. González Fernández, A. L. Sandoval Orozco, L. J. García Villalba, and J. Hernandez-Castro, "Digital image tamper detection technique based on spectrum analysis of CFA artifacts," *Sensors*, vol. 18, no. 9, p. 2804, 2018. https://doi.org/10.3390/s18092804

[19] M. Ahmad and F. Khursheed, "A novel image tamper detection approach by blending forensic tools and optimized CNN: Sealion customized firefly algorithm," *Multimedia Tools and Applications*, vol. 81, pp. 2577-2601, 2022. https://doi.org/10.1007/s11042-021-11529-0

[20] M. S. Kaushik and A. B. Kandali, "Hybrid feature selection for effective copy-move forgery detection," *International Journal of Intelligent Engineering & Systems*, vol. 17, no. 2, pp. 71–82, 2024.

[21] G. Fu, Y. Zhang, and Y. Wang, "Image copy-move forgery detection based on fused features and density clustering," *Applied Sciences*, vol. 13, no. 13, p. 7528, 2023. https://doi.org/10.3390/app13137528

[22] K. Asghar, M. Saddique, M. Hussain, G. Bebis, and Z. Habib, "Image forgery detection using noise and edge weighted local texture features," *Advances in Electrical and Computer Engineering*, vol. 22, no. 1, pp. 57-68, 2022.

[23] U. Diaa, "A deep learning model to inspect image forgery on SURF keypoints of SLIC segmented regions," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12549-12555, 2024. https://doi.org/10.48084/etasr.6622

[24] B. Chaitra and P. B. Reddy, "An approach for copy-move image multiple forgery detection based on an optimized pre-trained deep learning model," *Knowledge-Based Systems*, vol. 269, p. 110508, 2023. https://doi.org/10.1016/j.knosys.2023.110508

[25] Y. Aydın, "Automated identification of copy-move forgery using Hessian and patch feature extraction techniques," *Journal of Forensic Sciences*, vol. 69, no. 1, pp. 131-138, 2024. https://doi.org/10.1111/1556-4029.15415

[26] W. Liu *et al*., "SSD: Single shot multiBox detector," *[arXiv preprint arXiv:1512.02325]*, 2015.

[27] E. Rosten and T. Drummond, "Machine learning for high-speed corner detection," in *European Conference on Computer Vision (pp. 430-443). Berlin, Heidelberg: Springer Berlin Heidelberg*, 2006.

[28] R. I. Borman, A. Harjoko, and Wahyono, "Improved ORB algorithm through feature point optimization and Gaussian pyramid," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 2, pp. 268-275, 2024.

[29] P. Aglave and V. S. Kolkure, "Implementation of high performance feature extraction method using oriented fast and rotated brief algorithm," *International Journal of Research in Engineering and Technology*, vol. 4, no. 2, pp. 394-397, 2015.

[30] V. B. Punia and R. Goel, "Evaluation of machine learning algorithms for copy-move forgery detection," EasyChair Preprint No. 11523. EasyChair, 2023.

[31] C. Luo, W. Yang, P. Huang, and J. Zhou, "Overview of image matching based on ORB algorithm," *Journal of Physics: Conference Series*, vol. 1237, no. 3, p. 032020, 2019. https://doi.org/10.1088/1742-6596/1237/3/032020

[32] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Busternet: Detecting copy-move image forgery with source/target localization," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018.

[33] S. Shinde *et al*., "Identification of fake currency using soft computing," *Multidisciplinary Science Journal*, vol. 6, no. 2, pp. 2024018-2024018, 2024. https://doi.org/10.31893/multiscience.2024018

[34] N. Shelke, D. Sale, S. Shinde, A. Kathole, and R. Somkunwar, "A comprehensive framework for facial emotion detection using deep learning," *International Journal of Performability Engineering*, vol. 20, no. 8, pp. 487-497, 2024. https://doi.org/10.23940/ijpe.24.08.p3.487497

DOI: 10.55214/2576-8484.v9i10.10525