[1] Navin Kumar *

Enhanced Copy-Move Forgery Localization Identification: Leveraging Features for Optimized Detection

Journal of Electrical Systems

Abstract: - Image forgery detection has become significantly important in the digital era, as the genuineness of visual output is frequently compromised. This study addresses the growing need for robust techniques to detect image forgeries, particularly copy-move forgeries, which are common and difficult to detect due to the sophisticated methods used by forgers. The study presents an improved ensemble model for detecting and locating copy-move fraud using a powerful combination of machine learning and neural networks. Convolutional Neural Network (CNN) is used for extracting features and capturing complex patterns and details in pictures, while XGBoost is used for classification, taking advantage of its great efficiency and accuracy in processing big datasets. The proposed ensemble model successfully detects and accurately pinpoints forgeries in digital photographs and surpasses the performance of current approaches on the MICC-F600 and MICC-F2000 datasets, attaining F1 scores of 98.59 and 99.03, respectively. Additionally, the ensemble model achieves accuracy, precision, and recall rates of 99%, 98.66%, and 98.62% on the MICC-F600 dataset, and 99%, 98.5%, and 98.03% on the MICC-F2000 dataset. The results clearly indicate the method's exceptional accuracy in detecting copy-move forgeries, establishing it as a dependable tool for digital forensics. The experimental results highlight the method's capacity for practical applications in detecting picture counterfeiting, providing a substantial enhancement compared to conventional approaches.

Keywords: Copy-Move Forgery, Machine learning, Neural Network, Image Forgery Detection, Image Processing; MICC-F600 Dataset; MICC-F2000 Dataset.

I. INTRODUCTION

The widespread availability and growing complexity of digital image-altering tools have led to a fundamental problem, i.e., people no longer trust their eyes [1]. Because some forgers employ highly sophisticated counterfeit photographs to disseminate false information or do other shady operations, image forging is rapidly becoming a worldwide epidemic with far-reaching effects on everyday lives [2]. Copy move forgery (CMF) is a form of image forgery in which important details are hidden or duplicated by copying and pasting selected areas from one picture to another [3]. CMF detection approaches have been discussed extensively in the field of picture forensics and have significant applications in the fields of cybersecurity and multimedia security [4-5]. Objects within an image can be hidden or duplicated with the help of CMF, which is used for evil reasons. Figure 1 compares the original with a replica of the same image.

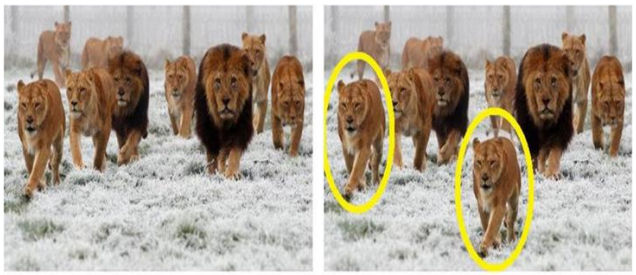

Figure 1. copy–move forgery (a) Original image, (b) Forged image (duplicated object highlighted) [6].

In recent years, a fascinating new discipline known as digital image forensics has evolved. This study seeks to uncover signs of forgery in digital photographs [7]. Investigating digital photographs to determine whether they contain forged content is the fundamental objective of digital image forensics. This can be done using either active or passive (blind) approaches [8]. The information that is placed a priori in the photographs is necessary for active approaches such as watermarking and digital signatures [9]. However, because this information is not readily available, the deployment of active approaches in practice could be restricted [10]. As a result, strategies that do not require any previous information about the photos being authenticated are utilized in the authentication process [11-12].

[1] Independent Scholar, Department of Computer Science
* Corresponding Author Email: navinkumar.25@gmail.com

1.1 The Importance of Identifying Fake Images

Forged photos are common on social networking sites like Facebook and Instagram, but they can also be seen in other areas, including magazines, courtrooms, scientific publications, and political campaigns. For instance, cyber security researchers have shown that hackers can access patients' 3-D medical scans and either remove or change images of cancerous cells. Scans with Al modifications can have misled surgeons, according to recent studies. Therefore, there can be an increased possibility of false diagnoses and insurance fraud. Additionally, politically related modified photos shared on social media might mislead and sway public opinion and action. According to studies, some photos are likely to be repeated and, in some circumstances, exploited in online terrorism communication channels through media sources. Many photos that have been altered have recently received widespread media coverage [13-14]. The cover of The Economist has a false picture, as seen in Figure 2. This issue's cover of The Economist has generated considerable debate. President Obama is shown against a dark and gloomy background, creating the sense that he is worried. However, he bowed his head while speaking with another person [15].

Figure 2. Forged image [Economist] [16]

1.2 Localization methods for copy-move forgeries

Past methods for detecting copy-move forgeries can be classified as either block-based or keypoint-based, and both rely on manually produced features. Meanwhile, key point-based approaches zero down on key point patches, from which they extract local characteristics. A brief overview of the types of copy-move forgery detection techniques is represented in Figure 3.

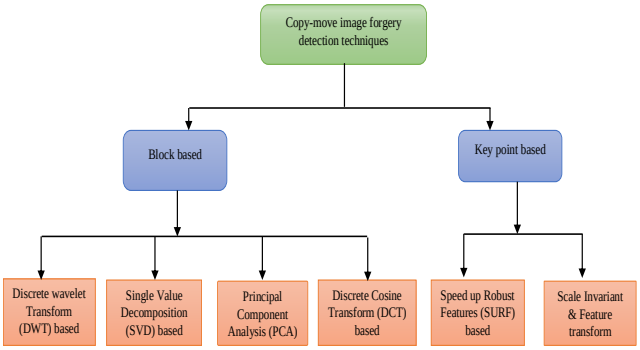

Figure 3. Copy-Move image forgery detection techniques [17].

1.2.1 Block-based approaches

This strategy is a highly frequent technique that has been shown to retain positive values when precision is taken into consideration. The first thing that must be done is to divide the picture up into sub-blocks that overlap each other. In the following stage, called "feature extraction," many methods, including PCA, SVD, DCT, and DWT, are utilized [18]. The result that was created in this way is then compared to the actual image to represent the forged parts of the image. The input image is broken up into blocks, either rectangular or spherical, that can or cannot overlap. Separating overlapping squares requires an M×N pixel picture and b×b square block. Move the block across the image by one pixel in both the horizontal and vertical directions. There are a total of (M - b + 1) × (N - b + 1) overlapping blocks in the image [19-20]. Each section of the image is then subjected to rigorous feature extraction. Following feature extraction, the collected data is sorted using appropriate data structures to identify potential forgeries by comparing the similarities between neighbouring pairs. k-d trees, Euclidean distance,

Lexical sorting, hash values, and radix sorts are only some of the matching algorithms that block-based Copy move forgery detection (CMFD) researchers examine.

1.2.2 Key-point based approach

Instead of using picture sub-blocking, this method focuses on isolating and labelling certain key points that are of local relevance. Efficient key points are pinpoints inside a digital picture that can be used to identify individual features [21]. This approach must be trustworthy in spotting shifts in lighting, geometric transformations, the presence of noise, and the identification of other distortions. These methods are quite effective at detecting the altered area, and they are developed to drastically cut down on flat matches in expansive spaces like the ocean and the sky. Improve accuracy and detect manipulated data with search methods, including the Nearest Neighbor Distance Ratio (NNDR), Scale Invariant Feature Transform (SURF), and Best Bin First (BBF) [22-25].

Local characteristics like corners, blobs, and edges are retrieved from manipulated images using key point-based approaches. A collection of descriptors represents each characteristic [26]. The descriptor enhances feature dependability. Forged sections in the picture are identified by matching each description with others. Studies have examined many matching algorithms for key-point-based forgery detection, including best bin first, 2-nearest neighbours, clustering, generalized 2NN, and Broad First Search Neighbors (BFSN) [27-30]. The key contribution of this study probably includes the creation and assessment of an upgraded approach or algorithm for identifying copy-move forgeries in digital images. The study can focus on using advanced methods for feature extraction from digital images. The contribution of the study has the potential to have practical implications in the field of image forensics

II. LITERATURE REVIEW

In this section, some related work based on the Enhanced Copy-Move Forgery Localization Identification: Leveraging Features for Optimized Detection is discussed below:

Diwan et al. (2023) [31] present a novel approach for detecting copy-move forgeries in digital images by leveraging the self-supervised image keypoint detector known as SuperPoint. This method employs the cutting-edge features of SuperPoint to reliably detect and localize copy-move fraud by combining keypoint detection with descriptor extraction. The flexibility of this method to process images of varying textures, such as smooth and self-similar structure images, is a key feature. Copy-move forgery can be detected in a wide variety of forged photos, and the findings showed that the suggested technique could generate stable results in images with varied assaults.

Samriya et al. (2023) [32] explore the challenge of high-dimensional, nonlinear data intrusion detection (ID). Data from KDD Cup 99 and NSL-KDD are used for this study. Firstly, the dataset is cleaned using the min-max normalization technique, and then homogeneity is achieved by the 1-N encoding technique. Following dimensionality reduction with the Ant colony optimization (ACO) approach, further processing is performed with deep neural networks (DNNs). Dynamic Voltage and Frequency Scaling (DVFS) approaches are selected for their energy efficiency. As a means of vetting and bettering the proposed model, it is put through its paces and compared against ACO and PCA-based (Naive Bayes) NB models. The experimental results show that the ACO-DNN model outperforms the state-of-the-art methods in accuracy parameters, training time complexity, and overall performance.

Zainal et al. (2022) [33] introduce a cutting-edge strategy for CMFR that relies heavily on deep learning (DL) and hybrid optimization. The suggested model employs a CNN technique based on a hybrid of Grey Wolf Optimization (GWO) and African Buffalo Optimization (ABO). Using convolution and pooling layers, the created model first collects picture characteristics, which are then matched to detect CMF. The results showed that 100 training epochs gave the highest accuracy.

Lee et al. (2022) [34] present a high-frequency wavelet coefficient-based, root-mean-squared-energy feature that is rotation-invariant. Instead of the usual VGG16 network's three-colour picture channels, two scale energy characteristics were employed, and a low-frequency subband image was used. To find duplicated and moved patch pairings, a correlation module uses VGG16 network-generated tiny feature patches. The correlation module calculates the all-to-all similarity. Using two bilinear upsampling stages and two batch-normalized-inception-based mask deconvolution procedures, the final binary localization map is generated via a simpler mask decoder module. The suggested approach is tested on four datasets and compared to leading tampering localization methods. Results show the suggested technique outperforms existing methods.

Das et al. (2022) [35] introduce a new Gated Context Attention Network (GCA-Net) that uses non-local attention and gating to detect finer picture differences and identify forged sections. High-dimensional embeddings

filter and collect important context from coarse feature maps throughout the decoding process in the proposed framework. This enhances the network's global comprehension and decreases false-positive localizations. After evaluating basic picture forensic benchmarks, GCA-Net outperforms state-of-the-art networks by an average of 4.7% Area Under the ROC Curve (AUC).

Tyagi et al. (2022) [36] introduce the evolution of image editing programs that have enabled the production of photorealistic CGI. Forensic systems can have trouble recognizing such images, making verification a tedious process. The author offers Forensic Net, a cutting-edge convolutional neural network (CNN) informed by current developments in computer vision, to solve this problem. The inverted bottleneck, depth-wise convolutions for spatial information mixing, and independent down-sampling layers are the three fundamental breakthroughs in CNNs. The inverted bottlenecks improve accuracy while reducing network parameters/FLOPS. The experimental findings show that Forensic Net performs far better than the state-of-the-art methods currently in use.

Pillai et al. (2022) [37] provide a method for identifying Copy-Move forgeries, in which one picture is partially superimposed over another to conceal an item or create a duplicate to prevent it from being passed off as the original. DBSCAN (Density-based spatial clustering of application with noise) is a real-time superpixel segmentation technique that is used to segment the input picture. Features derived from segmented pictures are matched using an adaptive patch-matching approach, and the overall efficiency of the method is improved by employing the VGGNet 16 architecture, which has a high accuracy rate for feature extraction. The experimental findings show that the proposed deep learning-based architecture can save computing time compared to previous designs and is more accurate at recognizing the tempered region even when the pictures are chaotic.

Tinnathi et al. (2022) [38] used a GWO-based AlexNet model and a superpixel clustering approach to spot fakes. Segment MICC-F600, MICC-F2000, and GRIP images using a superpixel clustering technique. After the images have been segmented, a forgery detection system based on an improved GWO-based AlexNet model extracts deep learning characteristics. AlexNet hyper-parameters are chosen using multi-objective functions in the upgraded GWO method. The adaptive matching algorithm locates forged areas in manipulated photos using characteristics. The model was successful in experiments with salt-and-pepper noise, Gaussian noise, rotation, blurring, and enhancement. Maximum detection accuracy for the improved GWO-based AlexNet model was 99.66%, 99.75%, and 98.48%, respectively.

Kumar et al. (2022) [39] extract visual characteristics using the Haar transform and simplify them using principal component analysis (PCA). Afterwards, incorrect borders were identified, located, and eliminated. Researchers examined the textural properties of the input picture using the grey-level co-occurrence matrix (GLCM). Euclidean distance was used to match features, and mismatched features were identified as forgeries. MATLAB was used to simulate the suggested technique, using accuracy as the performance parameter. Based on simulation findings, this technique exceeded PCA by 13.6% in accuracy.

Singh et al. (2022) [40] offer a method of hiding sensitive information in a digital image without leaving obvious signs of alteration. In the eyes of forensic experts, such actions cast doubt on the integrity of a picture. To identify instances of cloning and copy-move forgeries, the author suggests a technique that employs a hybrid of DWT-based block extraction and Scale Invariant and feature transform (SIFT)-based feature point extraction. To extract features from each of the blocks, the proposed approach relies on tentacle matching of features of the same features, which can be done by computing the dot products between the unit vectors. The suggested method achieves a recall factor of 100%, a precision factor of 97%, and an efficiency of 98.12%.

Tahaoglu et al. (2022) [41] offer a real-time implementation of a system for detecting the counterfeit of digital images. The suggested technique begins by determining the input image's underlying textural shape. Because the SIFT features and descriptors are extracted from textual pictures, they are more robust. By comparing specific features, people can see if an image has been tampered with and can pinpoint potentially fraudulent areas. The forgery detection based on Ciratef is implemented. The labelling pixels are improved in the post-processing stage by employing Connected Component Labeling and morphological operation. Both the state-of-the-art and the suggested techniques are shown on the GRIP and CMH datasets. The approach is resistant to distortion of geometric shapes and picture deterioration. The findings show that the suggested technique performs well, especially when attacked with geometric distortions like rotation and scaling.

Khan et al. (2021) [42] mentioned that UAVs have many developing uses in diverse fields. Without establishing human life safety, UAVs are hard to obtain public acceptability. Regular UAVs use centralized servers to process data using complicated machine-learning techniques. All typical cyber threats apply to UAV data transmission and storage. Because UAVs rely on smart algorithms that employ machine learning to make judgments in human absence, their impact is severe. The author suggests a distributed machine learning system built on the blockchain

to enhance UAV functionality. Data integrity and storage for intelligent decision-making among several UAVs can be enhanced by this design.

Alipour et al. (2020) [43] suggested a novel method for identifying and localizing forgeries in non-aligned JPEGs. This approach utilizes a deep neural network to perform semantic pixel-wise segmentation of JPEG blocks. Regarding JPEG compressions, the trained deep CNN can reliably identify block boundaries. As a result, abnormalities in the segmented block borders can be used to quickly identify and locate non-aligned JPEG forgeries. JPEG forgeries with the same and different quantization matrices, as well as picture forgeries with multiple compression stages, are all detectable and localizable using the suggested method. Researchers put the suggested algorithm through its paces using a wide range of fake and real photos and compared the results to those of state-of-the-art methods. The suggested CNN-based method shows promising results in detecting and localizing non-aligned JPEG forgeries, as evidenced by experiments.

Zhang et al. (2018) [44] used Stack Autoencoder to retrieve the tampered picture block characteristics so that the forgery could be discovered in a semi-automatic way. To further enhance localization precision, contextual information on picture blocks is included. The method is evaluated on a reference dataset, where it achieves a localization accuracy of 92.84% and an Area Under Curve (AUC) score of 0.9375. Our method improves AUC by over 40% and F1 by 5.7 times compared to the current gold standard for multi-format pictures. The results also boast an F1 score that is 4–8 times higher than those of various methods that are tailored to JPEG pictures.

Chen et al. (2017) [45] show noticeable form variations between actual and fabricated blurs near images following a splicing procedure. And then use this information to present a deep-learning architecture that can identify and locate fake images. More specifically, the Author demonstrates how a convolutional neural network can be used to tackle the issue by recasting it as one of handwriting recognition. Using splicing and retouching to create a huge dataset, this study indicates that the suggested method is more accurate and resilient than state-of-the-art methods.

III. Research Objectives

- To develop a diverse and meticulously curated dataset containing instances of copy-move forgery (CMF) and image splices.
- Analyzing the forgery type classification results to gain insights into the specific types of forgery detected within the images.
- To explore and implement a block-wise segmentation approach to enable a detailed analysis of distinct segments within pre-processed images, facilitating focused examination and feature extraction.

IV. Research Methodology

The concept of designed architecture is examined in the context of research methodology.

4.1 Technique Used

The "Enhanced Copy-Move Forgery Localization and Identification" method incorporates several crucial contributions to improve the detection of image forgeries. Initially, it employs the Discrete Cosine Transform (DCT) algorithm to extract important features from pre-processed image blocks [46-47]. The DCT transforms spatial information into a frequency-domain representation, which greatly improves the dataset's informativeness and allows for more accurate detection and categorization of forgery and non-forgery regions. Following is a mathematical formula that can be used to determine the DCT:

$$X_k = \frac{2}{N \times C_k \times sum\left(x_n \times \left(\frac{cos\ (\pi \times k \times (2n+1))}{2N}\right)\right)} \quad (1)$$

where,

N = number of samples in the signal

x_n = value of the signal at time n

X_k = kth coefficient of the DCT

C_k = normalization constant

Second, the Watershed Algorithm is an essential component in the process of segmenting images, which involves separating them into discrete sections that have comparable qualities [48]. This segmentation allows for finer-grained examination of certain regions inside a picture, which improves analysis. Finally, Histogram

Equalization enhances the readability of pre-processed images by making targeted regions of interest (ROIs) more distinct. Increasing the contrast and brightness in these ROIs contributes to a more precise forgery-type categorization and the detection of possible instances of copy-move forgery or picture splicing. The early classification of ROIs is also made possible with the incorporation CNNs [49]. To better detect ROI fraud, CNNs can learn complex visual cues and patterns [50]. As a result of this preliminary categorization step, areas for additional examination are identified, which ultimately enhances fraud detection and localization. Finally, XGBoost works together with CNN during the first phase of categorization. The unique feature of XGBoost is that it can be used in tandem with CNN to classify refined ROIs that have been acquired through picture segmentation and augmentation. By combining the benefits of both methods, this ensemble strategy can accurately evaluate the extent to which the dataset can have been subject to copy-move forgeries or image splicing.

4.2 Proposed Methodology

The Proposed layout in Figure 4 shows the operation depicted in diagrammatic form. The provided steps outline a comprehensive process for identifying and classifying copy-move forgery within images. Here's a detailed description of each step:

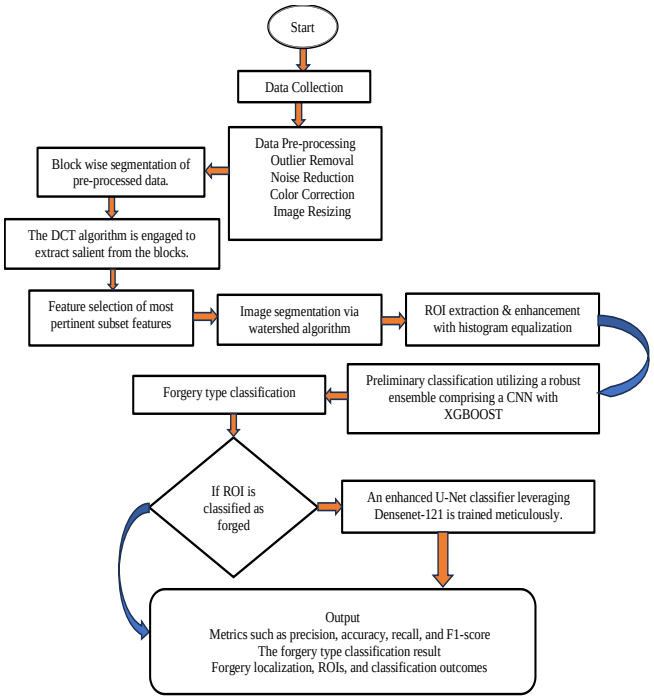

Figure 4: Proposed methodology

Step 1: Data Collection

In this initial stage, a diverse and carefully curated dataset is accumulated. This dataset includes images with copy-move forgery (CMF) and image splicing. It provides the foundation for subsequent analysis and classification duties.

Step 2: Data **Pre-processing**

In this stage, a set of procedures is applied to each image in the dataset. The goal of these procedures is to improve the data's quality and usefulness for subsequent analysis.

- Outlier Removal: There is an improvement in data quality because of the systematic removal of any outliers or inconsistencies.
- Noise Reduction: Any visual artefacts or disturbances are removed using various image processing techniques.
- Colour Correction: This procedure normalizes colour differences, providing a reliable baseline for further study.
- Image Resizing: The image is scaled to a constant size for homogeneous processing.

Step 3: Block-wise **Segmentation of Pre-processed Images**

Images that have been pre-processed are meticulously divided into smaller blocks. This segmentation enables a comprehensive examination of distinct image segments, allowing for a more focused examination.

Step 4: Application **of Discrete Cosine Transform (DCT) Algorithm**

In this step, the Discrete Cosine Transform (DCT) algorithm is applied to extract significant features from the blocks. This mathematical technique serves to convert spatial information into a frequency-domain representation, enabling a different perspective for analysis.

Step 5: Feature **Selection**

A subset of the most important features from the converted data is chosen for closer inspection. The data is cleaned up in this way, with the most informative variables being saved for later.

Step 6: Image Segmentation via Watershed Algorithm

The watershed segmentation technique is used to separate the image into clear areas. This method locates regions with common features, which aids in the separation of various image components.

Step 7: Region **of Interest (ROI) Extraction and Enhancement with Histogram Equalization**

Histogram equalization is used to zero in on target areas and boost them specifically. Using this method, the details in the image become much more pronounced and distinct. Following ROI refinement, the data is saved for subsequent analysis.

Step 8: Preliminary **Classification utilizing Ensemble Classifiers**

At this stage, an ensemble of classifiers is utilized, specifically a Convolutional Neural Network (CNN) coupled with XGBoost. This ensemble collaborates to provide a preliminary classification of the refined ROIs.

Step 9: Forgery **Type Classification**

This step involves two possible scenarios:

- If an ROI is classified as a forgery, an Enhanced U-Net Classifier, leveraging DenseNet-121, is trained using the training data along with the selected features. This classifier is subsequently tested on the testing data, ultimately yielding the forgery-type classification result.
- If an ROI is not classified as a forgery, the training of the Enhanced U-Net Classifier is bypassed, and the process continues directly to the subsequent phase.

Step 10: Outcome

In this final phase, a comprehensive analysis and reporting are conducted for each ROI:

- A quantitative evaluation of the model's efficacy is provided by computing metrics like precision, accuracy, recall, and F1-score based on the classification results.
- If applicable, the forgery type classification result is retrieved, providing insight into the type of forgery detected.
- The input image is displayed with forgery localization, ROIs, and classification results highlighted, providing a visual representation of the analysis and results.

4.3 Proposed Algorithm

The major steps of the proposed algorithm on enhanced copy-move forgery localization identification framework are as follows:

4.3.1 Data Collection

Let D be the diverse dataset containing N images, where each image is labelled as d_i With i ranging from 1 to N.

4.3.2 Data Pre-processing

- For each image d_i:
  - Perform Outlier Removal:
    $d_i = RemoveOutliers(d_i)$
  - Apply Noise Reduction:
    $d_i = ReduceNois(d_i)$ *Explain*
  - Implement Color Correction:
    $d_i = CorrectColor(d_i)$ *Explain*
  - Resize the image:
    $d_i = Resize\ (d_i)$ *Explain*

4.3.3 Block-wise Segmentation of Pre-processed Images

- For each pre-processed image d_i, partition it into M smaller blocks:
  $B_{ij} = Segment(d_i)\ for\ j = 1\ to\ M$

4.3.4 Application of Discrete Cosine Transform (DCT) Algorithm

- For each block B_{ij}, apply DCT:
  $F_{ij} = DCT\ (B_{ij})$

4.3.5 Feature Selection

- Select a subset of the most relevant feature from F_{ij}
  $F'_{ij} = SelectFeatures(F_{ij})$

4.3.6 Image Segmentation via Watershed Algorithm

- Apply Watershed Segmentation to identify regions:
  $R_{ij} = WatershedSegmentation(F'_{ij})$

4.3.7 Region of Interest (ROI) Extraction and Enhancement with Histogram Equalization

- For each region R_{ij}
- Pinpoint and enhance the ROI using histogram equalization:
  $E_{ij} = EnhanceROI(R_{ij})$

4.3.8 Preliminary Classification utilizing Ensemble Classifiers

- Initialize an example set C
- For each enhanced ROI E_{ij}
- Utilize an ensemble of classifiers:
  $C_{ij} = EnsembleClassify(E_{ij})$
- Add C_{ij} to C

4.3.9 Forgery Type Classification

- For each enhanced ROI E_{ij} and corresponding classification result C_{ij}
- If C_{ij} Indicates forgery:
- Train an Enhanced U-Net Classifier:
  $U_{ij} = TrainUNet(E_{ij}, SelectedFeatures)$
- Test U_{ij} On the testing data to get the forgery-type classification result:
  $F_{typeij} = TestUNet(U_{ij}, TestingData)$

4.3.10 Outcome

The experiment is conducted based on accuracy, precision, recall, and F1-score metrics.

V. Results and Discussion

This section provides the system configuration and evaluation metrics used and presents a comparative analysis that evaluates the performance of the system in relation to existing methods

5.1 Dataset description

5.1.1 MICC-F600

The MICC-F600 dataset has 440 genuine photos and 160 manipulated ones. This dataset comprises photos in the JPEG and BMP file types. The images vary in size, with measurements ranging from 800 × 533 to 3888 × 2592 pixels. The cloned portions in the manipulated photos exhibit arbitrary shapes and sizes. Manipulated photographs can be classified into four distinct groups. Every category consists of 40 photos and is associated with a distinct altering attack. The initial category comprises manipulated photographs featuring singular instances of plain cloning, whereas the subsequent category encompasses examples of multiple cloning. The third group consists of photographs that have cloned regions that are rotated, while the fourth category includes images where the cloned portions have been both scaled and rotated [51, 52].

5.1.2 MICC-F2000 Dataset

The MICC-F2000 dataset comprises 2000 photographs, with 700 being modified and 1300 being original. The digital photos contained in the MICC-F2000 dataset can undergo copy-move forgery, a technique where a small section of an image is duplicated and placed in another location to create the illusion of authenticity. This dataset

can serve as a benchmark for evaluating the efficacy of deep learning approaches in detecting manipulated photos [53].

5.2 Evaluation Metrics

This section discusses the evaluation metrics used in the study to assess the performance of the proposed model.

5.2.1 Accuracy

Accuracy is a metric that quantifies the ratio of correct predictions, including both true positives (TP) and true negatives (TN), to the total number of predictions made. It is calculated using the formula:

$$Accuracy = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ predictions} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

A higher accuracy value signifies that the model correctly predicts a large proportion of instances. However, accuracy might not be the most suitable metric for evaluating model performance with imbalanced datasets, as it does not account for the distribution of different classes.

5.2.2 Precision

It quantifies the ratio of accurate positive forecasts to all positive predictions, including both TP and false positives (FP).

$$Precision(P) = \frac{TP}{TP+FP} \quad (2)$$

It calculated the amount of appropriately identified positive instances among all the projected positive outcomes. High accuracy refers to the ability to minimize the occurrence of FP.

5.2.3 Recall

It, sometimes referred to as sensitivity, quantifies the ratio of appropriately predicted TP to the total number of real positive outcomes, including TP and False Negative (FN).

$$Recall\ = \frac{TP}{TP+FN} \quad (3)$$

Recall indicates how well the model identifies true positive cases. Higher recall indicates a lower number of FN.

5.2.4 F1-Score

It is a statistical measure that calculates the harmonic average of recall and precision. It serves as a unified metric that considers both recall and precision, striking a balance between the two factors.

$$F1 - Score\ = \ 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

The F1 score is a valuable metric when there is a requirement for maintaining an equilibrium between precision and recall. It is especially beneficial when the available data indicates an imbalance.

5.3 Dataset Pre-processing

5.3.1 MICC-F600 dataset

The various phases of data pre-processing for the MICC-F2000 dataset utilized in the Enhanced Copy-Move Forgery Localization Identification framework are shown in Figure 5. The initial image (Figure 5a) depicts an automobile in motion with a person in the background. The pre-processed picture (Figure 5b) undergoes modifications such as blurring, noise reduction, and contrast enhancement. The pre-processing methods enhance the identification and location of forgeries by emphasizing crucial characteristics and minimizing noise. This technique guarantees that the image is adjusted to ensure precise analysis by the detecting algorithms.

Figure 5. (a) Original image and figure 5 (b) Pre-processed image

5.3.2 MICC-F2000 dataset

Figure 6 depicts the various phases of data pre-processing for the MICC-F2000 dataset employed in the Enhanced Copy-Move Forgery Localization Identification framework. Figure 6a depicts a distinct view of a parked scooter. The pre-processed image (Figure 6b) undergoes adjustments such as blurring, noise reduction, and contrast alteration. The pre-processing processes optimize crucial characteristics, reduce interference, and enhance the clarity of regions of significance, hence facilitating the precise identification and positioning of counterfeit elements. This method ensures consistency and enhances the efficiency of detection algorithms.

Figure 6. (a) Original image and figure 6 (b) Pre-processed image

5.4 Result Analysis

5.4.1 Confusion matrix based on MICC-F600

The performance of the classification model in identifying different types of forgeries using the MICC-F600 dataset is depicted in Figure 7. The matrix displays actual labels against predicted labels for three classes: 'gt' (ground truth), 'scale', and 'tamp' (tampered). The model correctly classified 23 instances as 'gt' with no misclassifications in this category. For the 'scale' class, the model accurately identified 40 instances but mistakenly classified 4 instances as 'tamp'. In the 'tamp' category, 9 instances were correctly identified, while 4 were misclassified as 'scale'. The confusion matrix indicates high accuracy in detecting 'gt' and 'scale' forgeries but shows some confusion between 'scale' and 'tamp' forgeries. This performance analysis highlights the effectiveness of the feature extraction and optimization techniques used in the pre-processing stage to enhance the model's ability to accurately localize and identify copy-move forgeries.

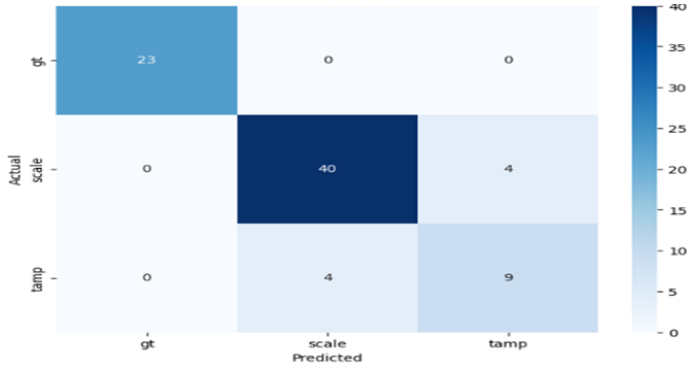

Figure 7. Confusion matrix for forgery-type classification

Figure 8 evaluates the classification model's performance on the MICC-F600 dataset for forgery detection. The matrix shows three classes: '0', '1', and '2'. The model correctly classified all 30 instances of class '0' with no errors. For class '1', 79 instances were correctly identified, but 8 were misclassified as '2'. In class '2', 22 instances were correctly identified, while 14 were misclassified as '1'. The model's high accuracy in identifying classes '0' and '1' indicates some confusion o and '2'. This demonstrates the effectiveness of pre-processing techniques in improving forgery detection, though further refinement is needed to reduce misclassification between similar forgery types.

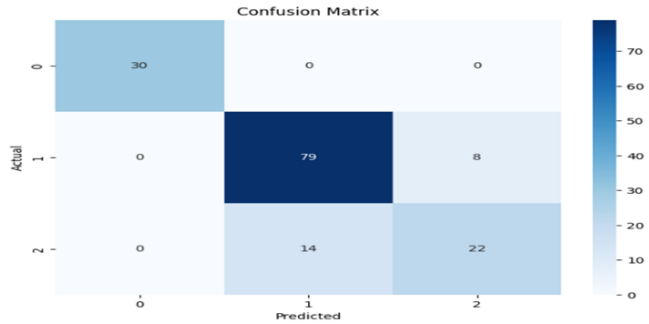

Figure 8. Confusion matrix for CNN

Figure 9 illustrates the classification model's performance in distinguishing between different types of forgeries using the MICC-F2000 dataset. The matrix compares actual versus predicted labels for 'scale' and 'tamp' forgeries. The model accurately classified 48 instances of 'scale' forgeries but misclassified 5 instances as 'tamp'. For 'tamp' forgeries, the model correctly identified 22 instances, with 5 instances misclassified as 'scale'. This matrix highlights the model's effectiveness in identifying both forgery types, demonstrating robust performance with some misclassification. The pre-processing and feature extraction techniques employed have significantly contributed to optimizing detection accuracy, although minor confusion between similar forgery types persists.

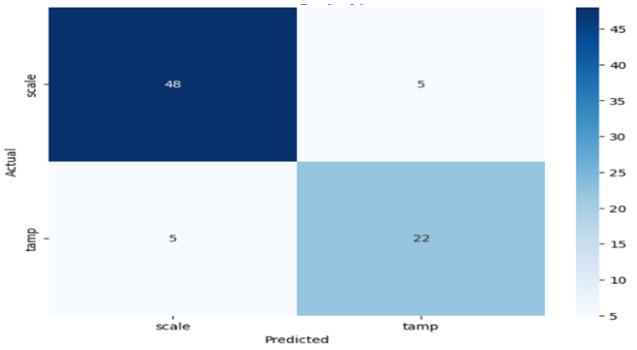

Figure 9. Confusion matrix for forgery-type classification

Figure 10 shows the model's performance in detecting forgeries in the MICC-F2000 dataset. It accurately classified 242 instances of class '0' with 7 misclassifications and correctly identified 150 instances of class '1' with only 1 misclassification. This demonstrates the model's high accuracy and effective pre-processing techniques for enhanced forgery detection.

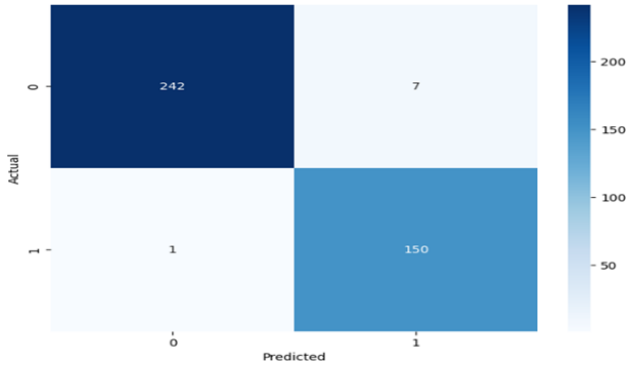

Figure 10. Confusion matrix for CNN

5.5 Performance evaluation

5.5.1 Based on the MICC-F600 dataset

The analysis of various techniques employed for copy-move forgery localization using the MICC-Fssss600 dataset, as depicted in Figure 11. The Convolutional Neural Network (CNN) achieved an accuracy of 94%, precision of 93.33%, recall of 96%, and an F1-score of 94.66%, demonstrating strong performance in detecting and identifying forgeries. XGBoost exhibited an accuracy of 90.20%, precision of 90.28%, recall of 90.20%, and an F1-score of 90.23%, indicating slightly lower robustness compared to CNN. The Ensemble method surpassed both individual techniques, with an accuracy of 99%, precision of 98.66%, recall of 98.62%, and an F1-score of

98.59%, highlighting that combining multiple techniques enhances the overall detection capability. Thus, the Ensemble method proves to be the most effective approach for optimized detection of copy-move forgeries in the MICC-F600 dataset.

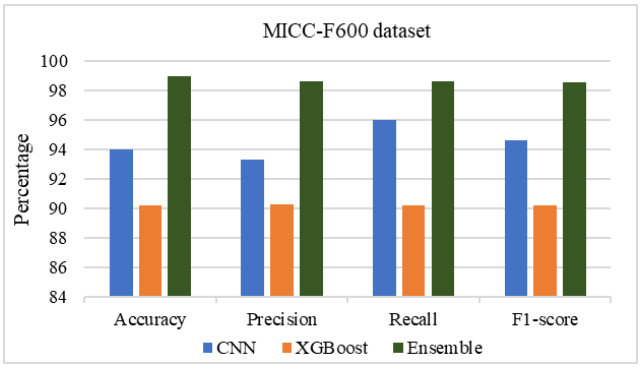

Figure 11. Performance on the MICC-F600 dataset

5.5.2 Based on the MICC-F2000

The analysis of various machine learning techniques was conducted using the MICC-F2000 dataset to determine their effectiveness in detecting forgeries, as shown in Figure 12. The evaluated techniques include CNN, XGBoost, and an Ensemble method. CNN achieved a high accuracy of 98.8%, with precision, recall, and F1-score of 98.02%, 97.82%, and 97.5%, respectively, indicating its robust performance in forgery detection. XGBoost demonstrated a lower accuracy of 90%, with precision, recall, and F1-score close to 90%, showing moderate effectiveness. The Ensemble method outperformed both, with an accuracy of 99% and precision, recall, and F1-score of 98.5%, 98.03%, and 99.03%, respectively, suggesting that combining multiple techniques leads to more optimized detection results.

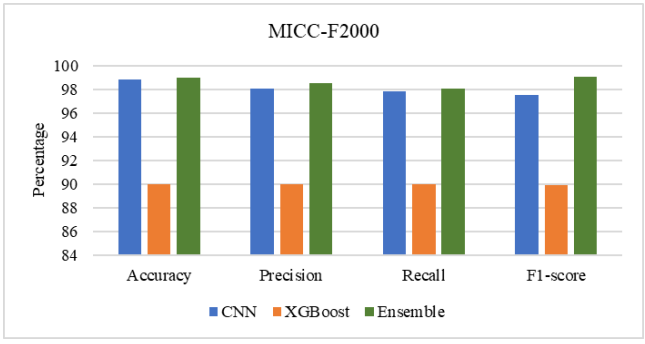

Figure 12. Performance on the MICC-F2000 dataset

5.6 Comparative Analysis

The comparative study demonstrates that the proposed approach has superior performance compared to existing strategies in both the MICC-F600 and MICC-F2000 datasets, as measured by the F1-Score, which assesses precision and recall. The proposed approach achieved an F1 score of 98.59 on the MICC-F600 dataset, compared to SuperPoint's 97.26 and GWO-ABO-CNN's 93.98. In the MICC-F2000 dataset, the suggested technique achieved a remarkable F1-Score of 99.03, outperforming the rotation-invariant module's score of 90.2 and the improved GWO's score of 98.50. This superior performance underscores the effectiveness of the proposed method in accurately detecting copy-move forgeries, making it a highly reliable solution for digital forensics applications.

Table 1: Comparison of F1-score across MICC-F600 and MICC-F2000 Datasets

Dataset	**Technique**	**F1-Score**
MICC-F600	SuperPoint [31]	97.26
	GWO-ABO-CNN [33]	93.98
	Proposed	98.59
MICC-F2000	Rotation-invariant module [34]	90.2
	enhanced GWO [38]	98.50
	Proposed	99.03

VI. Conclusion and Future Scope

The study highlights the effectiveness of the proposed method in identifying and detecting instances of copy-move fraud in digital images. The ensemble model achieves impressive accuracy, precision, and recall rates of 99%, 98.66%, and 98.62% on the MICC-F600 dataset, and 99%, 98.5%, and 98.03% on the MICC-F2000 dataset. As compared to previously developed models, the proposed ensemble approach shows a superior performance. The results highlight the strength and effectiveness of the suggested technique in precisely identifying copy-move forgeries, stressing its potential for practical use in digital forensics and picture authentication. The elevated F1 scores demonstrate the method's capacity to successfully manage accuracy and memory, guaranteeing a minimal occurrence of false positives and negatives, which is essential for dependable forgery detection.

The future scope of this research includes the exploration of deep learning models for feature extraction, the application of this method to video forgery detection, and the development of real-time forgery detection systems for digital forensic applications.

Author contributions

Navin Kumar: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Liu, Yaqi, Qingxiao Guan, Xianfeng Zhao, and Yun Cao. "Image forgery localization based on multi-scale convolutional neural networks." In Proceedings of the 6th ACM workshop on information hiding and multimedia security, pp. 85-90. 2018.

[2] Wu, Yue, Wael Abd-Almageed, and Prem Natarajan. "Busternet: Detecting copy-move image forgery with source/target localization." In Proceedings of the European Conference on computer vision (ECCV), pp. 168-184. 2018.

[3] BR, Sampangirama Reddy, Mohan Vishal Gupta, Pawan Bhambu, and Alka Singh. "Detection of Copy-Move Forgery (CMF) in Videos through the Application of a Machine Learning Algorithm." International Journal of Intelligent Systems and Applications in Engineering 11, no. 8s (2023): 18-26.

[4] Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based image copy-move forgery detection scheme." IEEE transactions on information forensics and security 10, no. 3 (2014): 507-518.

[5] Cozzolino, Davide, Giovanni Poggi, and Luisa Verdoliva. "Efficient dense-field copy–move forgery detection." IEEE Transactions on Information Forensics and Security 10, no. 11 (2015): 2284-2297.

[6] https://www.researchgate.net/figure/Example-of-copy-move-forgery-a-Original-image-b-Forged-image-duplicated-object_fig1_317495890

[7] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," Forensic Science International, vol. 224, no. 1–3, pp. 59–67, 2013.

[8] Aslam, Alvina, Ankita Saxena, Sonali Saxena, Vaishnavi Raman Dwivedi, Manish Gupta, and Priyanka Goel. "Image Forgery Detection Using Convolutional Neural Network." (2020).

[9] Qureshi, Muhammad Ali, and Mohamed Deriche. "A bibliography of pixel-based blind image forgery detection techniques." Signal Processing: Image Communication 39 (2015): 46-74.

[10] Qazi, Tanzeela, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, and Cheng‐Zhong Xu. "Survey on blind image forgery detection." IET Image Processing 7, no. 7 (2013): 660-670.

[11] Mahmood, Toqeer, Tabassam Nawaz, Rehan Ashraf, Mohsin Shah, Zakir Khan, Aun Irtaza, and Zahid Mehmood. "A survey on block based copy move image forgery detection techniques." In 2015 International Conference on Emerging Technologies (ICET), pp. 1-6. IEEE, 2015.

[12] Mahmood, Toqeer, Tabassam Nawaz, Aun Irtaza, Rehan Ashraf, Mohsin Shah, and Muhammad Tariq Mahmood. "Copy-move forgery detection technique for forensic analysis in digital images." Mathematical Problems in Engineering 2016 (2016).

[13] O'Halloran, Kay L., Sabine Tan, Peter Wignell, and Rebecca Lange. "12 Multimodal Recontextualisations of Images in Violent Extremist Discourse." Advancing multimodal and critical discourse studies: Interdisciplinary research inspired by Theo van Leeuwen's social semiotics (2017).

[14] Tan, Sabine, Kay L. O'Halloran, Peter Wignell, Kevin Chai, and Rebecca Lange. "A multimodal mixed methods approach for examining recontextualisation patterns of violent extremist images in online media." Discourse, Context & Media 21 (2018): 18-35.

[15] Wignell, Peter, Sabine Tan, Kay L. O'Halloran, Rebecca Lange, Kevin Chai, and Michael Wiebrands. "11 Images as Ideology in Terrorist-Related Communications." Shifts towards Image-centricity in Contemporary Multimodal Practices (2020): 253.

[16] https://www.theguardian.com/media/greenslade/2010/jul/06/the-economist-news-photography

[17] https://www.semanticscholar.org/paper/AN-ENHANCEMENT-OF-COPY-MOVE-FORGERY-DETECTION-IN-Naincy-Bathla/afccb96f63cccc125a4cec643ad39efb2c7699e9
[18] Kujur, Priyanka. "DIMENSION REDUCTION OF HIGH DIMENSIONAL IMAGE DATA USING HYBRID COMPRESSION TECHNIQUE." DIMENSION 8, no. 02 (2021).
[19] Yang, B., Sun, X., Chen, X., et al.: 'An efficient forensic method for copymove forgery detection based on DWT-FWHT', Radioengineering, 2013, 22, (4), pp. 1098–1105
[20] Li, L., Li, S., Zhu, H., et al.: 'An efficient scheme for detecting copy-move forged images by local binary patterns', IEEE Trans. Image Process., 2016, 4, (1), pp. 46–56
[21] Tinnathi, Sreenivasu, and G. Sudhavani. "An efficient copy move forgery detection using adaptive watershed segmentation with AGSO and hybrid feature extraction." Journal of Visual Communication and Image Representation 74 (2021): 102966.
[22] Gupta, Surbhi, Kutub Thakur, and Munish Kumar. "2D-human face recognition using SIFT and SURF descriptors of face's feature regions." The Visual Computer 37 (2021): 447-456.
[23] Mishra, P., Mishra, N., Sharma, S., et al.: 'Region duplication forgery detection technique based on SURF and HAC', Int. J. Adv. Comput. Technol., 2013, 6, (17), pp. 1–8
[24] Chen, L., Lu, W., Ni, J., et al.: 'Region duplication detection based on Harris corner points and step sector statistics', J. Vis. Commun. Image Represent., 2013, 24, (3), pp. 244–254
[25] Kunlun, L., Hexin, L., Bo, Y., et al.: 'Detection of image forgery based on improved PCA-SIFT'. Int. Conf. on Computer Engineering and Network, 2014, pp. 679–686
[26] Jaberi, M., Bebis, G., Hussain, M., et al.: 'Improving the detection and localization of duplicated regions in copy-move image forgery'. Int. Conf. on Digital Signal Processing (DSP), 2013, pp. 1–6
[27] Liu, L., Ni, R., Zhao, Y., et al.: 'Improved SIFT-based copy-move detection using BFSN clustering and CFA features'. Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, 2014, pp. 626–629
[28] Hashmi, M.F., Anand, V., Keskar, A.G.: 'Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform', AASRI Procedia, 2014, 9, pp. 84–91
[29] Mohamadian, Z., Pouyan, A.A.: 'Detection of duplication forgery in digital images in uniform and non-uniform regions'. Int. Conf. on Computer Modelling and Simulation, 2013, pp. 455–460
[30] Amerini, I., Ballan, L., Caldelli, R., et al.: 'Copy-move forgery detection and localization by means of robust clustering with J-Linkage', Signal Process., Image Commun., 2013, 28, (6), pp. 659–669
[31] Diwan, Anjali, Dinesh Kumar, Rajesh Mahadeva, H. C. S. Perera, and Janaka Alawatugoda. "Unveiling Copy-Move Forgeries: Enhancing Detection with SuperPoint Keypoint Architecture." IEEE Access (2023).
[32] Samriya, Jitendra Kumar, Mohit Kumar, and Rajeev Tiwari. "Energy-aware aco-dnn optimization model for intrusion detection of unmanned aerial vehicle (uavs)." Journal of Ambient Intelligence and Humanized Computing 14, no. 8 (2023): 10947-10962.
[33] Zainal, Anna Gustina. "Recognition of Copy Move Forgeries in Digital Images using Hybrid Optimization and Convolutional Neural Network Algorithm." (IJACSA) International Journal of Advanced Computer Science and Applications 13, no. 12 (2022).
[34] Lee, Sang In, Jun Young Park, and Il Kyu Eom. "CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature." IEEE Access 10 (2022): 106217-106229.
[35] Das, Sowmen, Md Saiful Islam, and Md Ruhul Amin. "GCA-Net: utilizing gated context attention for improving image forgery localization and detection." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 81-90. 2022.
[36] Tyagi, Shobhit, and Divakar Yadav. "ForensicNet: Modern CNN-based Image Forgery Detection Network." (2022).
[37] Pillai, Anuradha, and Deepika Punj. "A Novel Approach to Detect Copy Move Forgery using Deep Learning." (2022).
[38] Tinnathi, Sreenivasu, and G. Sudhavani. "Copy-Move Forgery Detection Using Superpixel Clustering Algorithm and Enhanced GWO Based AlexNet Model." Cybernetics and Information Technologies 22, no. 4 (2022): 91-110.
[39] Kumar, Ankit, Kamred Udham Singh, Chetan Swarup, Teekam Singh, Linesh Raja, and Abhishek Kumar. "Detection of Copy-Move Forgery Using Euclidean Distance and Texture Features." Traitement du Signal 39, no. 3 (2022).
[40] Singh, Richa, Sandeep Verma, Suman Avdhesh Yadav, and S. Vikram Singh. "Copy-move Forgery Detection using SIFT and DWT detection Techniques." In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), pp. 338-343. IEEE, 2022.
[41] Tahaoglu, Gul, Guzin Ulutas, Beste Ustubioglu, Mustafa Ulutas, and Vasif V. Nabiyev. "Ciratefi based copy move forgery detection on digital images." Multimedia Tools and Applications 81, no. 16 (2022): 22867-22902.
[42] Khan, Ammar Ahmed, Muhammad Mubashir Khan, Kashif Mehboob Khan, Junaid Arshad, and Farhan Ahmad. "A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs." Computer Networks 196 (2021): 108217.
[43] Alipour, Neda, and Alireza Behrad. "Semantic segmentation of JPEG blocks using a deep CNN for non-aligned JPEG forgery detection and localization." Multimedia Tools and Applications 79, no. 11-12 (2020): 8249-8265.
[44] Zhang, Ying, and Vrizlynn LL Thing. "A semi-feature learning approach for tampered region localization across multi-format images." Multimedia Tools and Applications 77 (2018): 25027-25052.

[45] Chen, Can, Scott McCloskey, and Jingyi Yu. "Image splicing detection via camera response function analysis." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5087-5096. 2017.

[46] Zhao, Zixiang, Jiangshe Zhang, Shuang Xu, Zudi Lin, and Hanspeter Pfister. "Discrete cosines transform network for guided depth map super-resolution." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 5697-5707. 2022

[47] Gani, Gulnawaz, and Fasel Qadir. "A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata." Journal of Information Security and Applications 54 (2020): 102510.

[48] Guo, Qinpeng, Yuchen Wang, Shijiao Yang, and Zhibin Xiang. "A method of blasted rock image segmentation based on improved watershed algorithm." Scientific Reports 12, no. 1 (2022): 7143.

[49] Uliyan, Diaa M., Somayeh Sadeghi, and Hamid A. Jalab. "Anti-spoofing method for fingerprint recognition using patch-based deep learning machine." Engineering Science and Technology, an International Journal 23, no. 2 (2020): 264-273.

[50] Ghosh, A., Sufian, A., Sultana, F., Chakrabarti, A., & De, D. (2020). Fundamental concepts of convolutional neural network. In Recent Trends and Advances in Artificial Intelligence and Internet of Things (pp. 519-567). Springer, Cham.

[51] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy–move attack detection and transformation recovery." IEEE transactions on information forensics and security 6, no. 3 (2011): 1099-1110.

[52] Zedan, Ibrahim A., Mona M. Soliman, Khaled M. Elsayed, and Hoda M. Onsi. "A New Matching Strategy for SIFT Based Copy-Move Forgery Detection." International Journal of Intelligent Engineering & Systems 16, no. 4 (2023).

[53] Gupta, Ruchi, Pushpa Singh, Tanweer Alam, and Shivani Agarwal. "A deep neural network with hybrid spotted hyena optimizer and grasshopper optimization algorithm for copy move forgery detection." Multimedia Tools and Applications 82, no. 16 (2023): 24547-24572.