International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I7P124

Volume 72 Issue 7, 224-236, July 2024

Original Article

An Optimized Deep Features for Detecting Tampered Region from the Copy Move Forgery Image

Allu Venkateswara Rao[1], D. Madhavi[2]

[1,2]*Department of Electrical, Electronics and Communication Engineering, GITAM Institute of Technology, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India.*

[1]*Corresponding Author : alluvenkateswararao34@gmail.com*

Received: 29 February 2024 Revised: 17 May 2024 Accepted: 18 June 2024 Published: 26 July 2024

Abstract *- Nowadays, forgery detection systems have rapidly grown in the digital application to find crime events. However, detecting the forgery and identifying the forged tampered portion is more complex because of the noisy data. To overcome this issue, the current research article has aimed to develop a novel Lion-based Optimized Radial Basis Neural Model (LORBNM). Initially, the CoMoFoD dataset has been trained, the training noise has been removed from the pre-processing layer, and then the error-free images are entered into the classification layer. Consequently, the classification parameters were tuned, and the present features were extracted. Furthermore, the image types have been specified in terms of Computer-Generated-Image (CGI), Natural Image (NI), and Forgery Image (FI). Eventually, the tapered region was predicted and segmented from the forgery image, and then the key metrics were calculated and compared with other existing approaches. In that, the presented LORBNM has observed the finest segmentation exactness score.*

Keywords *- Forgery Detection, Neural Networks, Copy-Move-Forgery-Image, Image Type Classification, Tampered Region Prediction.*

1. Introduction

Nowadays, cybercrime is developing rapidly which exceeds the effectiveness of protective measures [1]. Occasionally, digital media information, such as photographs or video, is judged to constitute irrefutable crime evidence or hostile activity [2]. By treating digital information as a technological clue [3], multimedia analytics technologies introduce a fresh approach to assisting in the analysis of indications and assisting in the decision-making process regarding crime events [4]. Multimedia analytics is concerned with the development of technological tools that determine if a property has been manipulated or if acquisition equipment was used in the absence of any extra information contained within the imagery [5]. The detection of tampering, in particular, is related to the difficulty of determining the validity of digital photographs [6]. While data integrity is critical during a trial, it is evident that the introduction of digital images has remained in high authentication score [7]. The critical point retrieved from the original and copied regions has exhibited similar description matrices in the context of a copy-move modification [8].

Besides Deep Learning (DL) and Machine Learning (ML), CMF is a method of image counterfeiting that involves copying specific areas of an image and replacing them with another location within the same idea. It enables the attacker to simply tamper with digital photos by using imaging equipment [9], similar illumination angles, and other properties in the identical image to conceal or accentuate the specific items [10].

Meanwhile, post-processing or geometric techniques are typically performed on the tampered areas throughout the tampering process to render the forgery authentic and undetectable [11]. The high similarity between the modified source and modified regions becomes the primary proof of CMFD [12]. However, current approaches are time-consuming, particularly during the feature extraction step. The placement of tampered zones does not fulfill practical requirements [13] because determining manipulated regions is more critical and essential in actual forensics applications than detecting forgeries [14].

Because splicing alters a picture's natural qualities, numerous image splicing prediction techniques have been created based on the image's statistical characters. The algorithm for detecting spliced images typically employs an approximate classification model and run-length model [15]. CMF detection is crucial in legal investigations, where it verifies the credibility of digital evidence, and in document authentication, where it ensures the validity of official records. Additionally, CMF detection aids media integrity

verification, helping maintain trust in digital content, and supports forensic analysis by uncovering evidence of tampering in images and videos from crime scenes or surveillance footage. Several models, such as pixel-based framework [16], critical point and block-based approaches [17], etc., have been executed in the past years. Still, there is a problem in detecting the tampered and spliced region. So, the present work has aimed to develop a novel optimized DL strategy to predict and segment the tampered region. 90% of criminal prosecutions in the United States now include digital evidence, including photos, according to a report by the American Bar Association. According to a National Association of Criminal Defense Lawyers poll, 68% of defense lawyers had dealt with cases involving CMF and other instances of tampering with digital evidence. Images are becoming more and more important in influencing public opinion and decision-making, especially with the rise of social media and citizen journalism. 63% of journalists have come across modified photos in their reporting, according to research by the International Federation of Journalists. CMF is a widespread practice used to distort facts and mislead audiences. Figure 1 shows the CMF and spliced region prediction system.

The main contribution of this research involves,

- The CoMoFoD dataset is gathered from the net source and trained to the system.
- Consequently, a novel LORBNM has been designed with the appropriate parameters for the tampered and spliced region specification.
- Before the detection process, the present errors were eliminated in the pre-processing function.
- Moreover, the CGI and NI images have become differentiated by analyzing the graphical properties.
- Furthermore, from the original image, the tampered and spliced region has been predicted and segmented.
- Finally, the exactness of the prediction process is determined by evaluating the key metrics like precision, accuracy, recall, F-measure, and error rate.

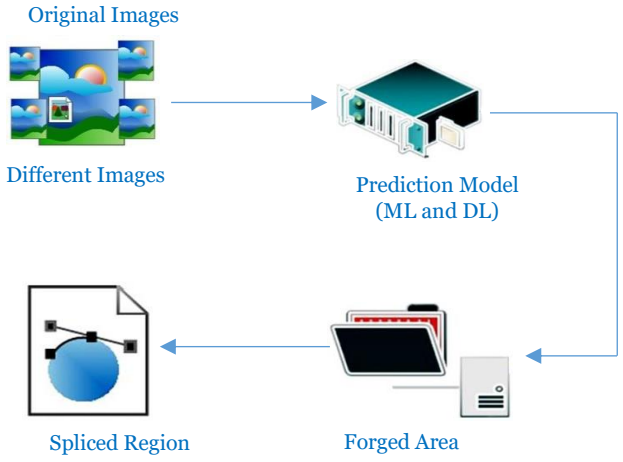


Fig. 1 CMF and spliced region prediction system

The current research chapter is designed as the second section has demonstrated the recent associated literature of CMF detection systems. Consequently, the difficulty score in the FI specification and prediction framework is described in the third section. Moreover, the 4th section has explained the solution to the discussed problem. Also, the 5th section describes the gained outcome of the proposed scheme. Finally, the research discussion has been ended in the 6th section.

2. Related Work

Recent kinds of literature related to CMF and tampered and spliced region detection are described as follows: The pixel-based framework has been implemented for the CMF application by Anuj Rani et al. [15]. Here, the proposed approach can extract the maximum pixel-based features from the trained data from that forged image that has been predicted, and the location of the spliced image has been segmented with a high accuracy rate. Here, the developed region was identified using the matching pixel templates. However, the pixel-based framework has required more resources and time duration to execute the process. CMFD is one of the methods for determining whether the image illustration contains a forged region or not. Moreover, Sreenivasu Tinnathiand and Sudhavani [16] have proposed a novel CMFD approach based on both key point and block-based methods. Hence, to begin with, the forged region extraction and the marker extraction models have been widely utilized with some ML or DL features. In addition, the grey level feature is used to predict the tampered region from the forged image. It has required more resources for the prediction function.The deep convolution neural network has been utilized efficiently in CMFD applications to predict the tampered region. In addition, to improve the prediction features of the convolutional model, Mohassin Ahmad and Farida Khursheed [17] have implemented the optimization features in the Convolutional dense layer then the prediction and segmentation function has been noted. Finally, a comparison assessment has been made to measure the improvement rate. The CMF has been made to tamper with the image region by replacing other graphical illustrations. In many cases, the forged images were the same as the original image, so an efficient prediction system has been required to predict the forged area. Yang et al. [18] have introduced the benefits of the key point strategy in predicting the tampered region from the image data. In addition, to filter the present noise in the trained data, the grid filter has been used. But, in this model, the spliced region is not predicted. The double-matching process has been implemented by Qiyue Lyu et al. [19] for the CFI detection system. Here, the tampered regions were identified by enabling the matching process of the original images. Moreover, the matching process functioned in the form of a triangle shape. Hence, it has provided the finest prediction outcome but takes more time when the image contains too much noise. Also, this method is highly dependent on human interpretation.

Table 1. Research gap

Sl.no	Author name and year	Technique name	Merits	Demerits	Attained outcomes
1	Anuj Rani et al. [15]	pixel-based framework	Better pre-processed and post-processed images	Difficult to predict the small region	Accuracy:97.5 Recall:93.75
2	Sreenivasu Tinnathi and Sudhavani [16]	CMFD approach based on both key point and block-based methods	Efficiently identifies the multiple tampered regions of the processed images	Videos are not applicable for detection performance	Error rate:2% Classification accuracy:87 Recognition accuracy:91
3	Mohassin Ahmad and Farida Khursheed [17]	Optimized Convolution Neural network	Simultaneously detect the copy move as well as sliced images	Decrease the precision for extending the no of images	Accuracy:93.41 Computation time:45s
4	Yang et al. [18]	key point strategy	Attained highest Recall score with suitable robustness	Failed to detect the higher JPEG compression	Recall:93.72 F-measure:82 Processing time:126s
5	Qiyue Lyu et al. [19]	double matching process	Classification and segmentation is well done	It needs more training time and cannot address the localization issues	F-measure:81.42 Computation time:3s
6	Chaitra et al. [24]	Transfer Learning based CNN	Classification dome in two levels, such as original images and forgery images	Large sets of datasets are affected by the noise	Exactness:91.9 Recall:92
7	Wang et al. [25]	Key-point-based copy move forgery identification strategy	Accurately detect the small-size manipulated images as well as large-scale images	During the detection time, the information is lost	Accuracy:92 Precision:92 Recall:94 Computation time:2s
8	Kaur et al [26]	contrast limited adaptive-based histogram equalization algorithm was integrated with CNN	Attained better validation and raining accuracy	Difficult to predict the high-resolution images	Error rate:0.02% RMSE:78% Accuracy:97.23 Precision:98

Chaitra et al. [24] have developed the Transfer Learning based CNN to address the generalization problems. Because the existing approaches are effective, widespread forgery detection is not supported. Moreover, a pre-trained Google Net was employed for predicting multiple forgeries. Also, Harris Hawks Optimization is adapted to change the weightage function of the CNN model. This model has achieved a 93% true negative rate and 93.8% true positive rates over the traditional methods. Image editing software is developed for some important applications but that also caused serious problems. Therefore, Wang et al. [25] have introduced a keypoint-based copy-move forgery identification strategy to predict the forged parts from the local visual features. Moreover, the linear clustering model and K multiple means algorithm were combined to perform the detection process. The proposed algorithm has outperformed the effective and extracted the robust hybrid features. In modern life digital images are easily modified and offer editable images using various software tools. Therefore, the detection and classification of the digital images are very important for decreasing the image forgery. Here, Kaur et al. [26] have developed the contrast-limited adaptive-based histogram equalization algorithm that was integrated with the CNN model to provide optimal results. Moreover, the experimental work has been done with numerous datasets such as IMD, F2000, and GRIP. Consequently, the effectiveness of the proposed strategy is shown against the different attacks such as noise addition, scaling, etc. Moreover, the research gap is enclosed in Table 1.The efficacy of current CMF detection techniques in precisely identifying modified regions inside images is frequently hampered by a number of issues. The problems such as computational complexity, vulnerability to post-processing, dependency on feature extraction, hard in

managing the large-scale dataset, and finally, limited recognition accuracy. These drawbacks are intended to be addressed by the Lion-based Optimized Radial Basis Neural Model, which makes use of an advanced neural network model designed especially for forgery detection applications.

Limitations of the mentioned CMF detection approaches include their resource-intensive nature, requiring significant computational resources and time. Some methods heavily rely on human interpretation, leading to subjective results and potential inconsistencies. While some approaches achieve high prediction accuracy, others may struggle with accurately detecting tampered regions, especially in cases closely resembling original images.

Challenges in handling image noise and generalization issues also persist, highlighting the need for further research to enhance the model aims to improve robustness against different manipulation approaches, decrease computing complexity, and increase detection accuracy by utilizing techniques like optimized radial basis function networks and the Lion optimization algorithm.

This technology is expected to improve copy-move forgery detection state-of-the-art and lead to more dependable and effective techniques for maintaining the integrity of digital images. The efficacy of CMF forgery detection techniques in precisely identifying modified regions inside images is frequently hampered by several issues.

3. System Description with Problem Statement

Detecting the forgery from the imaginary data is difficult because the forged image is visualized only as the original image. Hence, to identify the forged location, the pixel range has been analyzed throughout the entire region of the image data. However, that process has needed more resources and time to identify the forged areas. Several neural approaches were implemented to predict the tampered and spliced region. However, those models failed in the prediction process because of image complexity and the present noisy contents.

Usually, the digital fields are well-supported forgery, and modifications matter. Hence, detecting the edited portion or forgery is a complex task in the digital visualization application. To find the forgery region or the modified part from the original image, the CMF prediction framework has been implemented. In addition, the prediction system for the tampering region has been implemented to find the forgery region in the original image. The system description of the problem is described in Figure 2. So, the present work has motivated this research toward the specification of natural, forgery, and Computer Generation Images (CGI). In addition, the tampered region has been predicted and segmented from the forgery image to identify the forgery region.

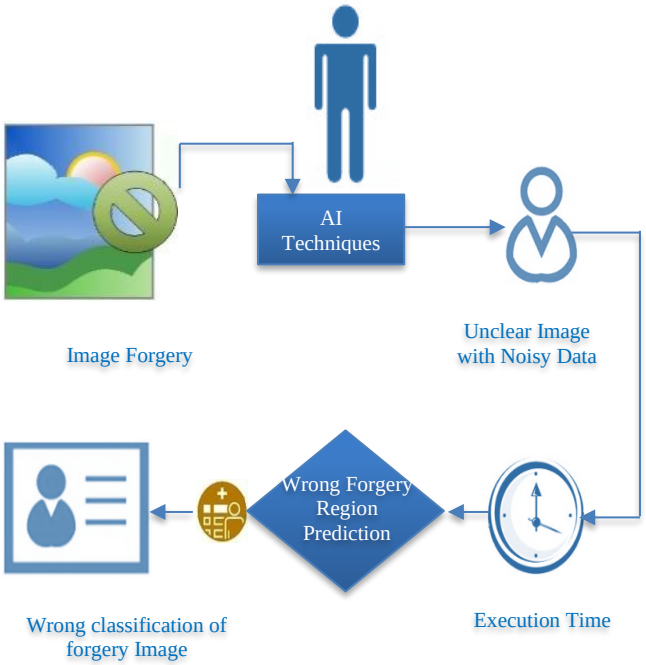


Fig. 2 System model with problem

In complex images, distinguishing between genuine and forged regions becomes difficult as forgeries blend seamlessly with surrounding content, leading to inaccuracies. Image noise, such as variations in pixel values, also complicates CMF detection by obscuring features and interfering with detection algorithms. Additionally, the limited availability of labeled datasets, computational complexity, execution time, and susceptibility to adversarial attacks further hinder CMF detection. Overcoming these challenges requires ongoing research to improve algorithm robustness, efficiency, and scalability, ultimately enhancing the integrity of digital imagery.

4. Proposed LORBNM for Tampered Region Prediction and Segmentation

The current research work has implemented a novel Lion-based Optimized Radial Basis Neural Model (LORBNM) for detecting tampering and splicing regions in the CMF images. RBNs are a type of artificial neural network that uses radial basis functions as activation functions. They are particularly useful for function approximation and pattern recognition tasks. RBNs are capable of learning complex relationships between input data and output labels. Optimization Inspired by Lion Behavior involves mimicking the behavior of lion prides in nature to optimize the performance of the neural model. Lion prides exhibit cooperative hunting strategies and territorial behaviors, which can be metaphorically translated into optimization algorithms. Lion Optimization further boosts model performance by optimizing RBN parameters based on cooperative hunting behavior observed in a lion pride.

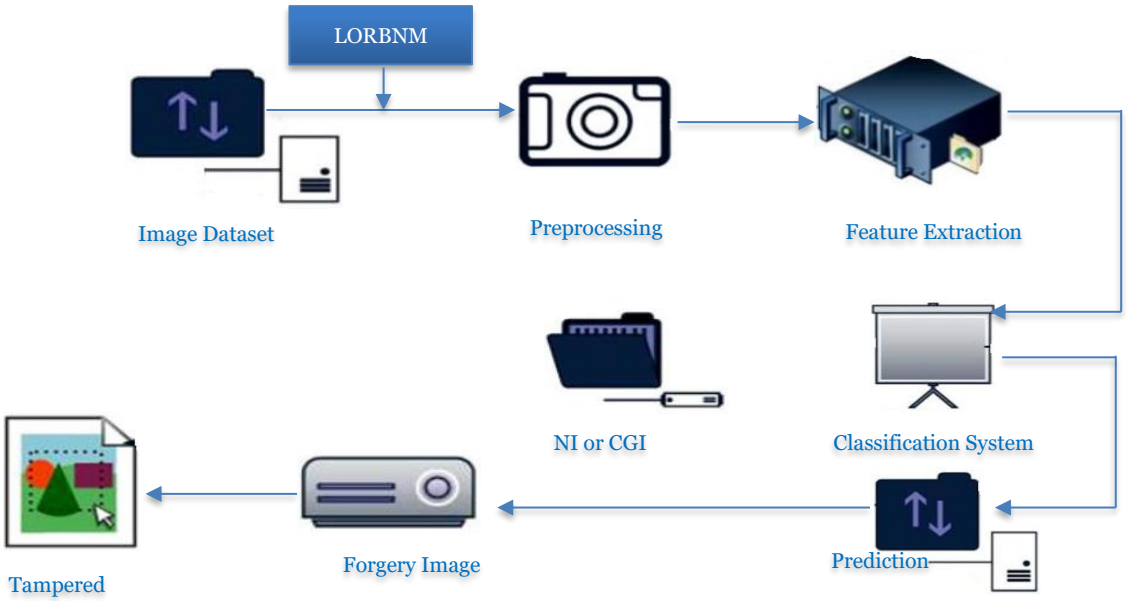


Fig. 3 Proposed LORBNM architecture

These optimization algorithms are designed to improve the training process of the neural network, enhancing its ability to detect tampering and splicing regions. Hence, to find the tampered region, the forgery image has to be detected and then predicted based on the tampering region. Moreover, the proposed technique's efficiency differentiates the CGI and natural image. Finally, the chief metrics are calculated and compared with other models to find the performance improvement rate. The proposed architecture is detailed in Figure 3. Detecting the FI and identifying the forgery location is essential for crime applications. Hence, after classifying the image types, the FI images are considered for forecasting the tampered region.

4.1. Design of LORBNM layers

The input layer, hidden layer, and output layer make up the three layers of an RBNN neural network type. The input data, which is usually represented as feature vectors, is received by the input layer. The hidden layer uses Radial Basis Functions (RBFs), which are situated at particular locations in the input space, to calculate the activation of neurons. The final output is created by combining the activations from the hidden layer in the output layer. The RBNN model in the LORBNM architecture is trained using Lion Optimization to identify and learn patterns from input data efficiently. To optimize the RBNN's parameters, such as the centers and widths of the RBFs in the hidden layer, Lion Optimization is incorporated into the training process. By using gradient descent or other optimization techniques, the optimization process seeks to minimize the error between the goal values and the network's predictions. By utilizing its capacity to explore and exploit the search area, Lion Optimization effectively improves the training process, which may result in higher convergence and improved generalization performance. Usually, in the optimization process, the difference between the goal values and the network's predictions is represented by an objective function that has to be minimized. Lion Optimization simulates a lion's hunting behavior and iteratively updates the RBNN's settings in an attempt to obtain the ideal parameter values that minimize the objective function. The designed LORBNM layers description is diagrammatically described in Figure 4.

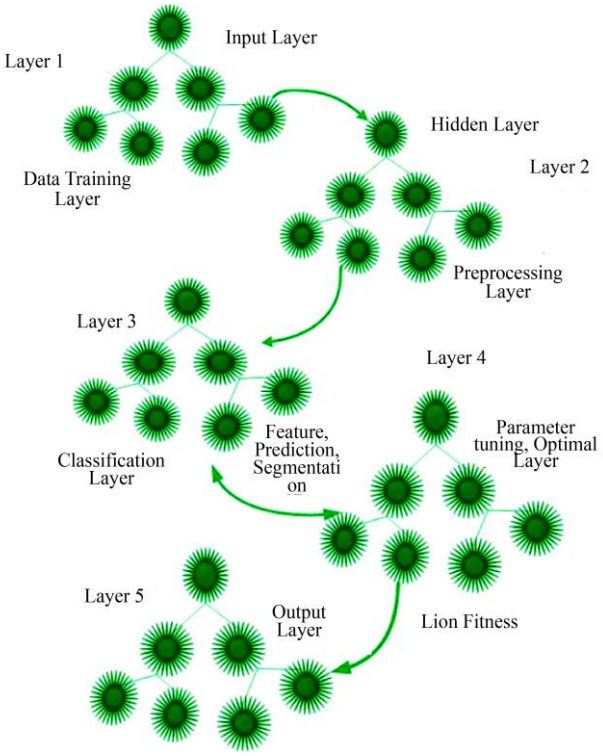


Fig. 4 Illustrations of LORBNM layers

4.2. Process of LORBNM Methodology

The proposed novel LORBNM design has five layers: input, hidden, prediction or classification, fitness updating, and output. Moreover, the proposed LORBNM has been developed in the principle of Lion Optimization [23] and the Radial Basis (RB) model [22]. Also, each function that was performed in the specific layer has been discussed.

$$f(S) = S\{1,2,3,4,5,\ldots\ldots n\} \quad (1)$$

Here $S$are the CoMoFoD datasets and$\{1,2,3,4,5,\ldots\ldots n\}$ have denoted the $n$number of images. Hence, the initialization of the dataset is processed using Equation (1).

All optimum ranges and functions were fixed in the lion fitness module then the optimal fitness function was upgraded in the classification phase of the RB neural model. During the testing process, the classification parameters were tuned until a suitable solution was obtained. By Enhancing feature extraction, it capture specific characteristics of different forgery types and facilitates detection. Integration of domain knowledge and transfer learning techniques further improves model generalization. Through iterative refinement, the approach ensures robust detection across a wide range of image manipulation scenarios.

4.1.1. Pre-Processing

In visualization concepts like image or video processing, filtering the noise is the key factor to gain the finest detection and specification accuracy. Also, noisy content in the trained datasets has taken more time for the execution process. Although image processing pipelines frequently include noise filtering as a pre-processing step, a CMF detection system may also include additional image enhancements in its pre-processing phase. With these improvements, the input photos should be of higher quality and be better suited for further analysis and forgery detection. Hence, the error filtering has been functioned by Equation (2).

$$f_e = \sum_{n=1}^{n} S - T(E(S) = S^* \quad (2)$$

The pre-processing variable is denoted asf_e, data counts are determined as$n = 1$, $T$is the noise analyzing and tracking variable, and $E$is the present noise in the trained data. Furthermore, the filtered data is represented asS^*.

4.1.2. Feature Extraction and Image Type Classification

To meet the prediction target, extracting the features before the classification process is the most required task. Hence, the function features extraction is processed using Equation (3). Where, $x$are the present meaningful features like object features, also $y$defined the entire features like grass, wall, etc. Moreover, the maximum possible meaningful features are extracted from the entire image feature, and the meaningless features are removed, λwhich is the monitoring parameter attained from the lion fitness.

$$F_a = \lambda\left(\frac{\sum_{n=1}^{n} x(S^*)}{\sum_{n=0}^{n} y(S^*)} - z\right) = mf \quad (3)$$

Hence, the extracted meaningful features were denoted as mfandF_a, the feature extraction function is described in Equation (3). The present types of images were classified that are CGI, NI, and forgery. From the CoMoFoD dataset, the image types have been organized based on labels form that is '0' and '1'. If the test data is under the 0th label category during the testing process, then it is specified as CGI. Moreover, if the tested image is followed under the 1st label, it is classified as a forgery image. Lastly, if the image is not under both the 0 and 1st labels, it is specified as a natural image.

4.1.3. Tampered Region Prediction

After the image classification process, the specified forgery images were taken for the following process that is: tampered region identification and segmentation. By analyzing texture, color, and spatial information, the segmentation algorithm precisely separates tampered regions from authentic content, achieving fine-grained boundary delineation. Additionally, it enhances segmentation accuracy by learning complex patterns associated with tampering, further refining boundary detection.

In order to efficiently learn and discern between authentic and tampered regions in photos, the Lion Optimization Algorithm (LOA) optimizes the parameters of the predictive model, such as the Radial Basis Neural Network (RBNN). The centers and widths of the Radial Basis Functions (RBFs) in the RBNN are two examples of the predictive model parameters that LOA optimizes. LOA steers the model toward settings that reduce prediction errors and maximize the detection of tampered regions by iteratively modifying these parameters in response to performance feedback received during training. Through optimization, the model becomes more sensitive to minute discrepancies created by manipulation.

$$(CMF)_{tp} = \begin{cases} 1 & selected\_pixel(mf) < (pixel)_{ar} \\ 0 & selected\_pixel(mf) = (pixel)_{ar} \end{cases} \quad (4)$$

During the testing process, one of the images was taken to identify the forgery in that specific image. Hence, the forgery prediction is measured by Equation (4), where arrepresents all-region, $tp$is the tampered portion prediction variable. In addition, to find the forgery region, the pixel range has been analyzed for all-region. If any specific portion is mismatched from the other region pixel, the forgery has been detected.

$$t_s = max\left(\frac{pixel(mf) < (pixel)_{ar}}{Total_{ip}}\right) \quad (5)$$

Here, the image pixel is determined asip; from the entire image pixel range, the pixel range of the forgery image has been analyzed and segmented. Moreover, the tampered region segmentation function is represented ast_s. The best solution of the lion algorithm is utilized here to segment the predicted tampered region, which is equated in Equation (5).

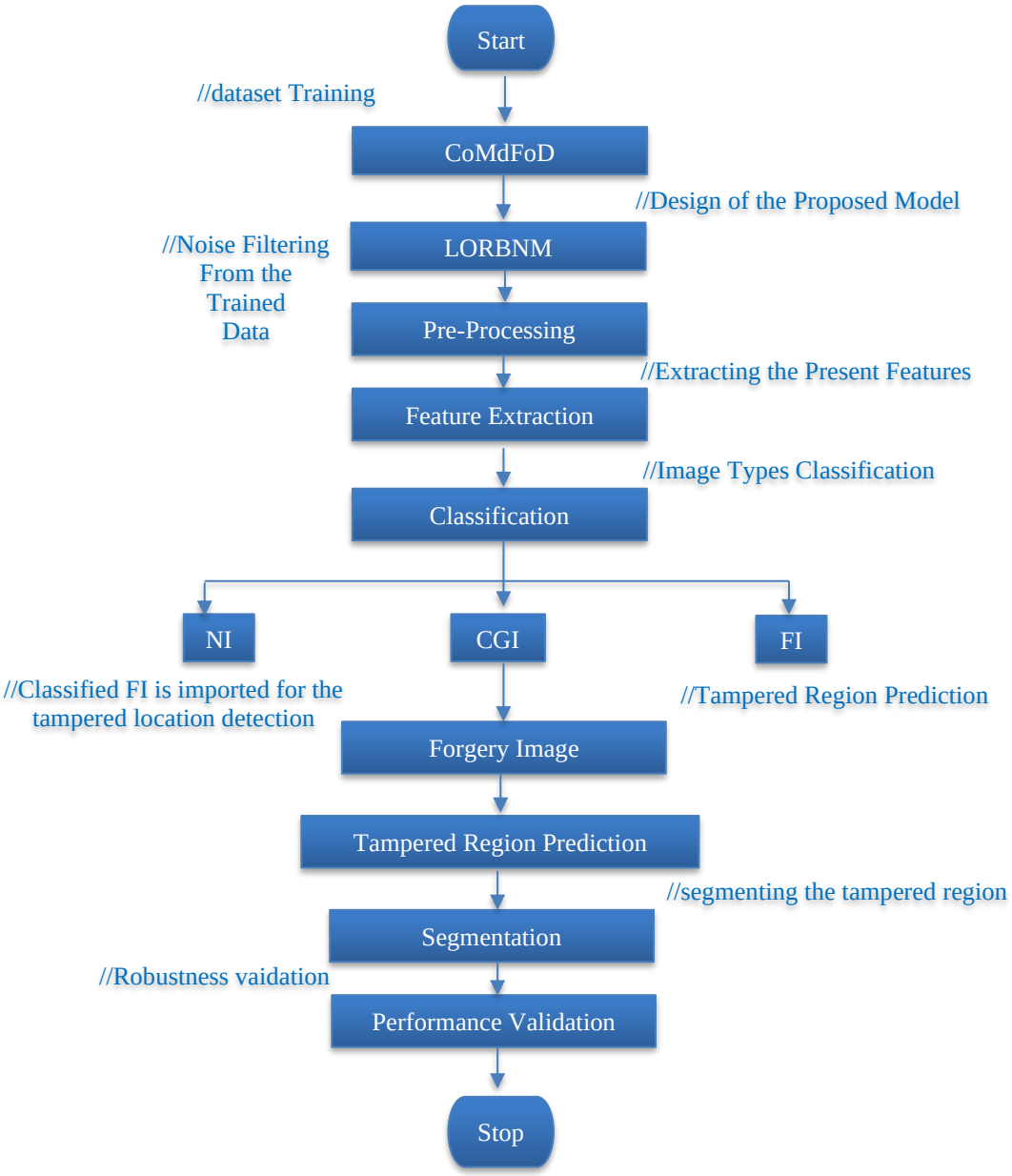


Fig. 5 Proposed LORBNM flow model

Here, convergence is assessed by tracking changes in the objective function value, parameter updates, iteration count, and convergence rate. Convergence is declared when the objective function value stabilizes, parameter updates become minimal, the maximum iteration limit is reached, or the rate of improvement slows down. These criteria help determine when an optimal or sufficiently close-to-optimal solution has been found. The working procedure of the designed system is illustrated in Figure 5 and Algorithm 1.

The working process of the developed scheme is diagrammatically explained in the way of the flowchart in Figure 5. Also, the utilized mathematical equations are written in pseudo-code format in Algorithm 1, which is employed to design the Python codes. The fitness function is essential in directing the optimization process toward the best answer when employing Lion Optimization (LO) to identify tampered regions in photos. The fitness function assesses candidate solutions' quality, such as possible tampered regions, according to certain task-specific criteria. Color moments or color histograms can be used to evaluate the color consistency within an area. The distribution of colors in tampered regions is frequently inconsistent with that of the surrounding areas. Significant variations in color features can result in regions being penalized by the fitness function. While penalizing areas with abrupt or discontinuous edges, the fitness function may benefit regions with smooth and continuous edges.

Algorithm 1 LORBNM

```
Start
{
   int S
   // dataset initialization
   Pre-processing ()
   {
   int T , E;
   //initializing the pre-processing variable
   f_e → S − noise = S*
   // removing noise from the trained data
   }
   Feature extraction()
   {
   int x , y,
   //feature extraction variable initialization
   F_a = x(S*) ← y(S*)
   // meaningful features were predicted
   }
   Classification()
   {
   if(test_data=0)
   {
   CGI
   }else if(test_data=1)
   {
   Forgery image
   }else (NI)
   // By executing the if condition, image types were
   classified
   }
   Tampered region prediction ()
   {
   if(test_ image p ≠0)
   {
   Tampered region
   }else (normal)
   }
   Segmentation()
   {
   segment → tampered_region
   //Segmenting the predicted tampered region
   }
}
Stop
```

5. Results and Discussion

The planned novel LORBNM framework is executed in the Python platform and running in the Windows 10 platform. The implementation process has been carried out within the splitting ratio of 20% testing and 80% training. The available dataset is split into two subsets: the training set, which contains 80% of the data, and the testing set, which contains the remaining 20%. This is indicated by the training-testing split ratio of 80%–20%. When training predictive models for the identification of picture forgeries, among other machine learning and data mining tasks, this split ratio is frequently selected. The model may learn from a wider variety of instances in a larger training set, which improves its ability to identify underlying patterns and relationships in the data. When applied to untested data, this may result in enhanced generalization performance and model accuracy. The testing set acts as a separate sample that the model did not encounter during training, making it possible to evaluate the model's predicted ability objectively on untested data. Moreover, the CoMoFoD database has included a total of 170 images, including 33 CGI, 80 FI, and 57 NI. After designing the novel LORBNM, the performance of the prediction and segmentation has been analyzed in the testing scenario. Forensic investigators can utilize the CMF detection system to verify digital photos that are provided as evidence in criminal cases, civil lawsuits, or other court cases. Before publishing or disseminating photos to the public, journalists, news agencies, and media organizations can utilize the CMF detection system to confirm the authenticity of the images. The CMF detection system can be integrated into social media platforms, online marketplaces, and digital content-sharing websites to stop the spread of false information and misleading content.

5.1. Dataset Description

CoMoFoD datasets are mainly designed to apply the research and development fields for the application of digital image forgeries. It can provide standardized images that consist of specific ground truth images. Moreover, this is to allow the various copy-move image forgery detection strategies for training and validation purposes. Consequently, the CoMoFoD database includes 260 sets of images, from which 60 images are grouped in large categories (3000×2000) and 200 images are grouped in small categories (512×512). Every image set contains the original image (image without transformation), binary mask, forged image, and colored image. A common option for assessing techniques for identifying image tampering is the Copy-Move Forgery Detection dataset. This sort of forgery involves copying and pasting a portion of an image onto another portion of the same picture in order to hide or alter information. A range of images with varying content, resolutions, and complexity are usually included in the dataset. Because of this diversity, the assessed approach is guaranteed to be reliable across a large range of image kinds, which increases its applicability in real-world circumstances where image attributes might vary greatly.

5.2. Experimental Result

The accuracy validation has been attained to validate the proficiency score of the tampered region forecasting accuracy. The training accuracy is to measure the proposed algorithm performance in training the datasets. The accuracy for validation and training is detailed in Figure 7.

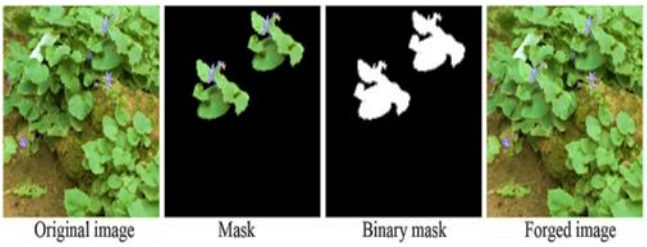


Fig. 6 CoMoFoD dataset samples

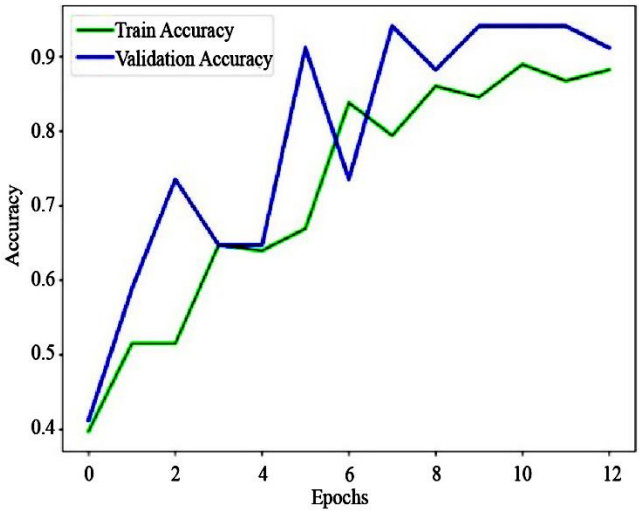


Fig. 7 Training and validation accuracy

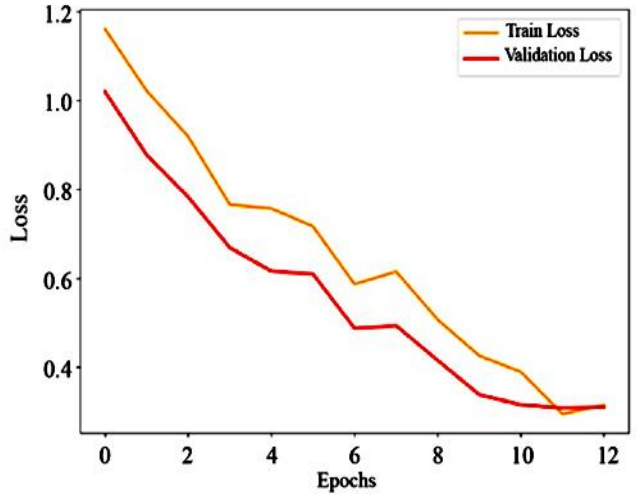


Fig. 8 Training and validation loss

The misleading statistics in the training process have been measured in terms of training loss. Moreover, to find the possible rate in the tampered region, misclassification or prediction is calculated as validation loss. The loss validation has been detailed in Figure 8.The dataset worn in this present work is CoMoFoD; it has included three different classes: Forgery Image (FI), CGI, and NI images. So, the image classification has been performed before the tampered region detection.

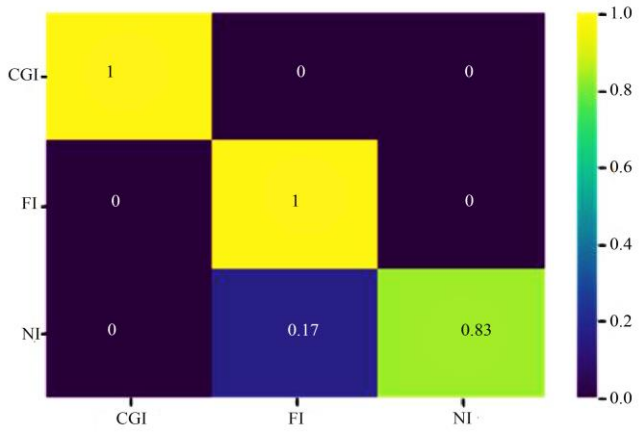


Fig. 9 Confusion matrix

Hence, the image type classification results have been obtained in the form of the confusion matrix that is described in Figure 9.

5.3. Case Study

A few examples were taken to verify the functioning rate of the proposed model, and the designed methods have been applied to the trained samples. The tampered region predicted outcome is described in Table 2. Three samples were taken, including a library, trees with light, and a hill area. Primarily, the trained images were filtered for noise removal then the noise-reduced image data was taken for the image type classification and tampered region detection process. Table 2 shows four original images, which indicate the images used for testing.

5.3.1. Forged Image

Some strange objects or functions have been performed, and that forgery part is taken from the image itself. It is described as some portion of the image being copied and pasted in other regions. So, it is called a CMF image.

5.3.2. Tampered Region Detection

After the forged image's specification, the forgery's tampered region has been predicted by analyzing the pixel range. Finally, the detected tampered portion has been segmented, and the parameters were validated.

5.4. Performance Analysis

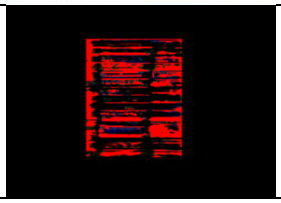
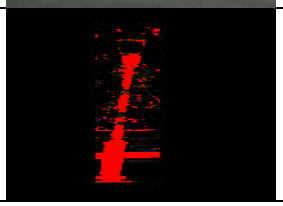
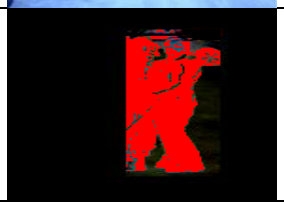
To value the improvement score of the developed approach, some existing models have been adopted: that are Convolutional Neural Model (CNM) [21], VGGNet [22], and Polar-Complex-Exponential (PCE) [20].

5.4.1. Accuracy

To measure the exactness range in forecasting and to segment the tampered region is termed accuracy. In addition, the accuracy score depends upon the image clarity.

$$Accuracy = \frac{ip+in}{ip+in+jp+jn} \quad (6)$$

Table 2. Tampered region prediction results

	Sample 1	Sample 2	Sample 3
Original image			
Forged image			
Tampered region			
Tampered region segmentation			

Here, $ip$is the true-positive, true-negative is determined asin jnhas represented false-negative and jpdetermines false-positive. The accuracy has been valued by Equation (6). The proposed LORBNM approach has gained the highest exactness score of 99.9%.

Moreover, the model VGGNet has observed the tampered region forecasting exactness score as 95%. The CNM scheme has earned the most acceptable detection accuracy of 98.39%. The comparison statistics are described in Figure 10. Hence, the designed framework has achieved a better exactness score in predicting the tampered region compared to other existing schemes.

5.4.2. Precision Assessment

In addition, to estimate the number of correct segmentation and prediction, the metrics precision has been validated by analyzing the positive predicted values. Moreover, the formula of the precision is detailed in Equation (7).

$$Pr = \frac{ip}{ip+jp} \tag{7}$$

The VGGNet model has observed the precision as 98% for identifying the tampered region. The approach CNM has earned the precision score of 98.63%, and the model PCE has recorded the precision range as 96.83%. Also, the proposed LORBNM has measured the precision measure as 99.4%, which is higher than the compared existing schemes.

5.4.3. Recall Validation

The recall parameter was calculated to evaluate the sensitive range in the case of positive and negative means. Hence, the recall has been validated in Equation (8). If the method has earned the finest segmentation accuracy, it has earned a good recall rate.

$$Re\,c = \frac{ip}{ip+in} \tag{8}$$

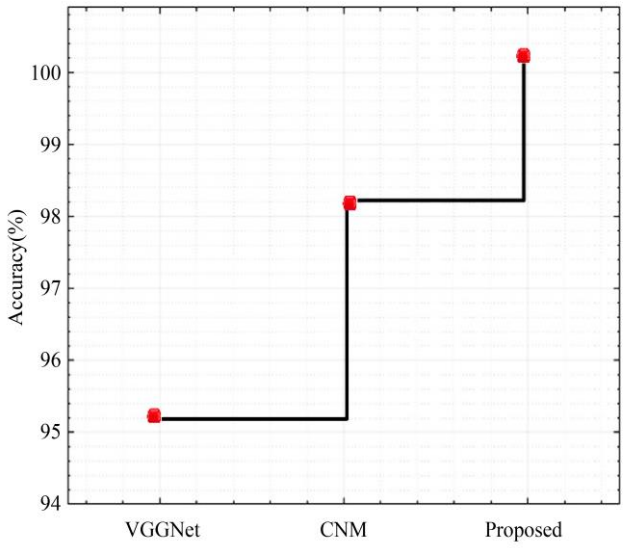


Fig. 10 Accuracy measurement

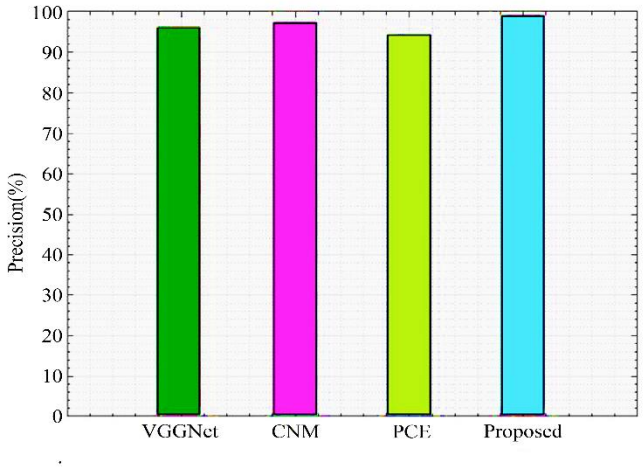


Fig. 11 Precision validation

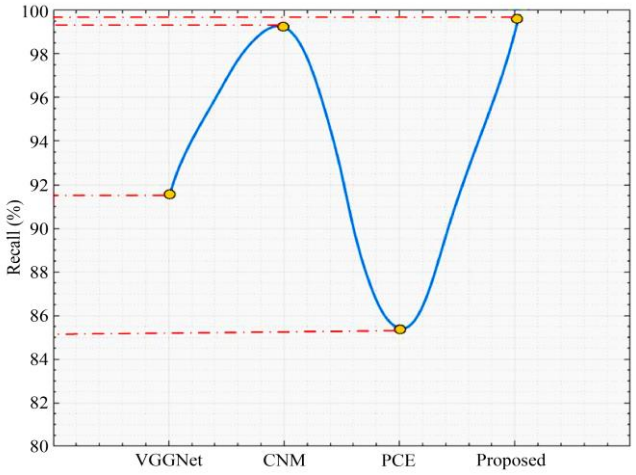


Fig. 12 Recall validation

In the visualization framework, recall is the crucial parameter for finding the correctness score in forecasting the tampered portion. The PCE approach has observed the recall score as 85.19%, CNM has gained a recall score of 99.6%, and VGGNet has yielded a recall value of 89.6%. When compared to these existing approaches, the proposed scheme has obtained a recall score of 99.99%, which is higher than other models.

5.4.4. F-Measure

The metrics F-measure has been validated to find the mean of the measurement precision and recall score. Moreover, the f-measure is formulated in Equation (9).

$$F - measure = 2 * \frac{pr \times rec}{pr + rec} \quad (9)$$

The attained F-measure for the designed LORBNM is 99.7%; it has proved the stability range of the tampered region prediction and segmentation exactness score. Moreover, the model VGGNet has employed the F-score of 92%, CNM has achieved the F-value of 99%, and the approach PCE has recorded the F-value as 90.2%.The overall assessment of comparison statistics is described in Table 3.

Table 3. Overall Comparison statistics

Overall comparison assessment				
Methods	F-measure	Recall	Precision	Accuracy
VGGNet	92	89.6	98	95
CNM	99	99.6	98.63	98.39
PCE	90.2	85.19	98.83	-
Proposed	99.7	99.9	99.4	99.9

Table 4. Overall performance of the proposed LORBNM

Statistics of LORBNM	
Accuracy	99.9%
F-measure	99.7%
Recall	99.9%
Precision	99.4%
Error rate	0.058%
Classification time	3.8s

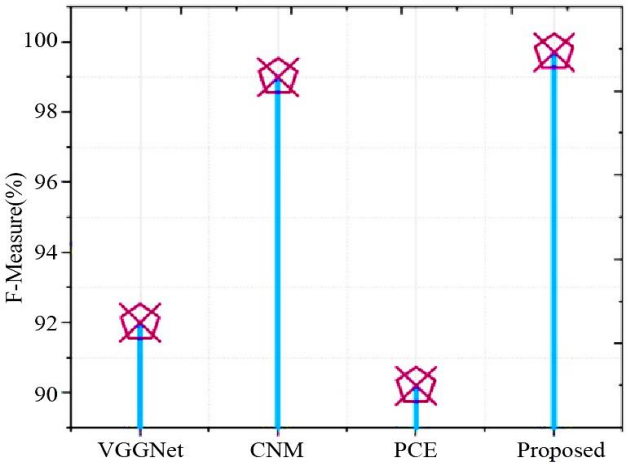


Fig. 13 Comparison of F-score

5.5. Discussion

The proposed novel LORBNM has earned the finest tampered region identification and segmentation range from all the validated parameters. In addition, the method is suitable for all digital image applications to find the forgery or the manual modification by the third user. In addition, the proposed LORBNM has been executed in a short duration that is 0.49s; when compared to other existing schemes, it has earned a reduced execution time. Moreover, the CNM has recorded the processing time as 3.8s, and the PCE has observed the execution duration as 168.81s. Also, the miss prediction score is measured in the form of an error. Hence, the presented framework has obtained the lowest error score of 0.058%. The overall performance statistics of the designed LORBNM are described in Table 4. Hence, the designed framework is suitable for the forgery forecasting system.The technique probably makes use of strong detection algorithms that may pick up on minute irregularities and discrepancies that point to image modification. These algorithms might use sophisticated machine learning strategies, including ensemble methods or neural networks that have been trained on a variety of datasets to handle different kinds of forgeries.

Multi-resolution analysis techniques may be employed by the method to address forgeries that involve several source regions or intricate modifications. These methods enable the detection of complex forging patterns by capturing global and local information from picture analysis at various scales or resolutions. All things considered, the suggested approach most likely overcomes the difficulties caused by intricate image alterations or forgeries involving numerous source locations by utilizing strong detection algorithms and sophisticated feature representations.

However, Lion Optimization is iterative; it may take a long time and a lot of computing power to reach the best answer, which makes it less useful in situations when resources are few or for real-time applications. The settings selected for both Lion Optimization and the RBNN may have an impact on the LORBNM method's performance. If the forgeries are intricate or nuanced and drastically different from the patterns the system was trained on, it might not be able to identify them. Moreover proposed LORBNM uses RBFs for efficient capture of complex data relationships and Lion Optimization to fine-tune model parameters effectively.

Unlike some existing methods, LORBNM offers improved scalability by optimizing computational resources and processing time. Additionally, it enhances generalization capabilities, mitigates vulnerability to adversarial attacks, and reduces dependency on manual parameter tuning. By combining RBFs with Lion Optimization, LORBNM achieves higher accuracy and efficiency in detecting tampering and splicing regions within images, surpassing the limitations of traditional CMF detection approaches.

6. Conclusion

CMF detection is the hottest topic for many cybersecurity applications in the digital industry. Finding the forgery in the digital images is a complicated task with simple ML models. So, the present research work intended to design a novel intelligent tampered region prediction system from the CMF image. Hence, the novel scheme is LORBNM, developed based on deep features and optimization best solution. The dataset that has been considered in this research work is CoMoFoD.Moreover, the observed exactness score for the designed LORBNM is 99.9% compared to other approaches; the proposed solution has maximized the exactness range up to 3%. In addition, the observed recall score by the designed approach is 99.9%, which has shown an improvement rate up to an average of 10%. Hence, the outstanding results verified the successive score of the designed model. Also, the designed tampered region prediction framework is suitable for all CMF image applications to identify the forgery region.

References

[1] Muhammad Bilal et al., "A Robust Technique for Copy-Move Forgery Detection from Small and Extremely Smooth Tampered Regions Based on the DHE-SURF Features and mDBSCAN Clustering," *Australian Journal of Forensic Sciences*, vol. 53, no. 4, pp. 459-482, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] X.H. Zhou, and Q.J. Shi, "Multiple Copy-Move Forgery Detection Based on Density Clustering," *Pattern Recognition and Image Analysis*, vol. 31, pp. 109-116, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] P. Niu et al., "Fast and Effective Keypoint-Based Image Copy-Move Forgery Detection Using Complex-Valued Moment Invariants," *Journal of Visual Communication and Image Representation*, vol. 77, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ankit Kumar Jaiswal, and Rajeev Srivastava, "Detection of Copy-Move Forgery in Digital Image Using Multi-Scale, Multi-Stage Deep Learning Model," *Neural Processing Letters*, vol. 54, no. 1, pp. 75-100, 2022.[CrossRef] [Google Scholar] [Publisher Link]

[5] Ritu Agarwal, and Om Prakash Verma, "Robust Copy-Move Forgery Detection Using Modified Superpixel Based FCM Clustering with Emperor Penguin Optimization and Block Feature Matching," *Evolving Systems*, vol. 13, no. 1, pp. 27-41, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Gul Tahaoglu et al., "Improved Copy Move Forgery Detection Method via L*a*b* Color Space and Enhanced Localization Technique," *Multimedia Tools and Applications*, vol. 80, pp. 23419-23456, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Anuja Dixit, and Soumen Bag, "A Fast Technique to Detect Copy-Move Image Forgery with Reflection and Non-Affine Transformation Attacks," *Expert Systems with Applications*, vol.182, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Esteban Alejandro Armas Vega et al., "Copy-Move Forgery Detection Technique Based on Discrete Cosine Transform Blocks Features," *Neural Computing and Applications*, vol. 33, pp. 4713-4727, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Kavita Rathi, and Parvinder Singh, "Copy–Move Forgery Detection by Using Key-Point-Based Harris Features and CLA Clustering," *New Approaches for Multidimensional Signal Processing: Proceedings of International Workshop*, pp. 113-124, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Preeti Kale, Vijashree. A. More, and Ulhas Shinde, "Copy Move Forgery Detection-A Robust Technique," *2021 Sixth International Conference on Image Information Processing*, Shimla, India, pp. 121-125, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Kha-Tu Huynh, Tu-Nga Ly, and Phuong-Thanh Nguyen, "Improving the Accuracy in Copy-Move Image Detection: A Model of Sharpness and Blurriness," *SN Computer Science*, vol. 2, no. 4, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] D. Suganya, K. Thirunadana Sikamani, and J. Sasikala, "Copy-Move Forgery Detection of Medical Images Using Most Valuable Player Based Optimization," *Sensing and Imaging*, vol. 22, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Gaël Mahfoudi et al., "CMID: A New Dataset for Copy-Move Forgeries on ID Documents," *2021 IEEE International Conference on Image Processing*, Anchorage, AK, USA, pp. 3028-3032, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nidhi Goel, Samarjeet Kaur, and Ruchika Bala, "Dual Branch Convolutional Neural Network for Copy Move Forgery Detection," *IET Image Processing*, vol. 15, no. 3, pp. 656-665, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Anuj Rani, Ajit Jain, and Manoj Kumar, "Identification of Copy-Move and Splicing Based Forgeries Using Advanced SURF and Revised Template Matching," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 23877-23898, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Sreenivasu Tinnathi, 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*, vol. 74, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mohassin Ahmad, and Farida Khursheed, "A Novel Image Tamper Detection Approach by Blending Forensic Tools and Optimized CNN: Sealion Customized Firefly Algorithm," *Multimedia Tools and Applications*, vol. 81, no. 2, pp. 2577-2601, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jixiang Yang et al., "A Novel Copy-Move Forgery Detection Algorithm via Two-Stage Filtering," *Digital Signal Processing*, vol. 113, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Qiyue Lyu et al., "Copy Move Forgery Detection Based on Double Matching," *Journal of Visual Communication and Image Representation*, vol. 76, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Yilan Wang, Xiaobing Kang, and Yajun Chen, "Robust and Accurate Detection of Image Copy-Move Forgery Using PCET-SVD and Histogram of Block Similarity Measures," *Journal of Information Security and Applications*, vol. 54, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ritu Agarwal, and Om Prakash Verma, "An Efficient Copy Move Forgery Detection Using Deep Learning Feature Extraction and Matching Algorithm," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7355-7376, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Parag C. Pendharkar, "Hybrid Radial Basis Function DEA and its Applications to Regression, Segmentation and Cluster Analysis Problems," *Machine Learning with Applications*, vol. 6, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] G. Saranraj, K. Selvamani, and P. Malathi, "A Novel Data Aggregation Using Multi Objective Based Male Lion Optimization Algorithm (DA-MOMLOA) in Wireless Sensor Network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 5645-5653, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] B. Chaitra, and P.V. Bhaskar Reddy, "An Approach for Copy-Move Image Multiple Forgery Detection Based on an Optimized Pre-Trained Deep Learning Model," *Knowledge-Based Systems*, vol. 269, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Xiang-yang Wang et al., "Accurate and Robust Image Copy-Move Forgery Detection Using Adaptive Keypoints and FQGPCET-GLCM Feature," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 2203-2235, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Navneet Kaur, Neeru Jindal, and Kulbir Singh, "A Deep Learning Framework for Copy-Move Forgery Detection in Digital Images," *Multimedia Tools and Applications*, vol. 82, no. 12, pp. 17741-17768, 2023. [CrossRef] [Google Scholar] [Publisher Link]