IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 37, No. 1, February, 2023, pp. 191-199
Journal homepage: http://iieta.org/journals/ria

Image Counterfeiting Detection and Localization Using Deep Learning Algorithms

Manikyala Rao Tankala[1*], Chanamallu Srinivasa Rao[2]

[1] Department of ECE, JNTUK, Kakinada 533003, Andhra Pradesh, India
[2] Department of ECE, UCEV, JNTUK, Vizianagaram 535003, Andhra Pradesh, India

Corresponding Author's Email: tankalamanik322@gmail.com

https://doi.org/10.18280/ria.370124

Received: 10 October 2022
Accepted: 10 February 2023

Keywords:
accuracy, class activation mappings, epochs, image forgery, localization, Residual Neural Network (ResNet), Graphic Card

ABSTRACT

As social networking services such as Whatsapp, Facebook, Twitter, and Instagram have grown in popularity over the past two decades, the volume of picture data created throughout the globe has exploded. Images that have been altered or doctored using editing software such as Adobe Photoshop, GIMP, and Paint-3D are a major source of concern in the digital age. As a result, it is essential to verify the validity of suspect images before taking action against people who fabricate them. Copy-move forgery and spliced image fraud are two of the most extensively used picture forgery methods in the field. Recent Deep Learning (DL) algorithms have simplified tasks like categorization, localization, segmentation, and other comparable studies. With the use of Residual Neural Networks (ResNet), copy-move forgery and spliced fraud in photographs may be discovered and classified. Experimental results on benchmark datasets such as CASIA-2, MICC-F2000, and CoMoFoD indicate significant gains over state-of-the-art approaches. Gradient Class activation mappings (Grad-CAM) were applied to find forged regions in tampered photographs, and the suggested approach was also proven to be successful in predicting tampered images. On the CoMoFoD dataset, a classification accuracy of 99.9% was attained, while on the MICC-F 2000 dataset, it was 97%.

1. INTRODUCTION

Images are now employed as primary sources of information in various disciplines, including the news media, medicine, scientific research, sports, digital forensics, and education. It is relatively simple to make a forged picture using Android programs, Coral Draw, GIMP, and Photoshop, such as by photo hackers. When an image is used as evidence in a court of law, its legitimacy is critical. Image manipulation, often known as image editing, is any action done on digital images using any program. A way of manipulating the content of an image to make it contradict a historical reality is known as "picture fabrication." Image tampering is a kind of photo counterfeiting in which fresh material replaces some of the original content in a photograph. Duplicate tampering occurs when new material is duplicated from the same image; image enhancement occurs when new information is duplicated from a different image.

Any exploit that may be done on digital material utilising software editing tools is referred to as image manipulation. For example, the copy-move technique duplicates a picture section and then pastes it into another image [1]. The quality of the false pictures increases as editing software advances, and they seem to be natural to the naked eye. Additionally, post-processing alterations such as brightness changes, JPEG compression, or equalisation may diminish the operation evidence and make it harder to detect [2].

Handcrafted and Deep Learning [DL]-based algorithms are popular methods for detecting copy-move forgery [1]. The three types of the techniques are key point-based, block-based, and integration of former two methods. A present day method uses either custom-built models or pre-trained designs like VGG-16 [3] for forgery detection. In block-based algorithms, many techniques of feature extraction are utilized, such as the Discrete Cosine transform (DCT) and Fourier transform [4, 5] or Tetrolet transform [6]. Because a matching technique identifies counterfeiting, one of their concerns is that performance would decrease if the cloned object is rotated or resized. On the other hand, key point-based methods are more robust to rotation and illumination fluctuations, such as Scale Invariant Feature Transform [7, 8] and Speed-Up Robust Features [9]. Identifying forgeries in areas of unvarying intensity, simple identical things being confused for fraudulent, duplicate objects and relying on real, crucial places in the picture are all issues they confront. A hybrid technique produced more consistent consequences in expressions of F1 Score (F1S), Recall (R), and Precision (P), (CN) [10-12]. It recommended a customised network [CN] with a specific data set. Current feature extraction and classification methods employ convolutional neural networks [CNN], fully connected layers (FCL) and convolutional layers (CLs) [13]. The design was trained independently on the CASIA v2 and CASIA v1 datasets with 97.9% and 98.1% accuracy (Acc), respectively. Similar research used a bespoke prototype with six CLs and three FCLs, with batch normalisation in all CLs, failure in the FCLs, and batch normalisation in all CLs. Using the CoMoFoD dataset, this model's interior validation was 95.97% correct [14]. Two CLs and two FCLs are employed [15, 16] for well training of data. The researchers trained and verified the prototypical using three, two, and one layers and achieved Accuracies of 95.4%, 94.2%, and 90.1%, respectively. Even though they report the generalisation is

difficult, their mixed datasets are unstable, with one having a 2:1 ratio of bogus and legitimate photographs and the other a 2:3 ratio. Transfer learning and customised CN Network designs are the second CN Network-based approach types (TL). In this case, pre-trained copies are also used for feature extraction and fine-tuning. A pre-trained Alex Net model has been adopted in training and got F1-Score of 0.93 [17]. In other cases, VGG-16 has also been employed as a feature extractor until the final pooling layer [18] for better results.

2. LITERATURE REVIEW

This section summaries and evaluates a variety of research attempts in Image Splicing Detection (ISD) and Copy Move forgery detection based on their overall performance. The bulk of the research reported here uses a strategy that involves retrieving and learning characteristics from image blocks using a machine learning methodology.

Zhao et al. [19] reasoned that if ISD was difficult in one colour area, it would be accessible in another. As a consequence, they devised a method for detecting passive picture splicing. Four Gray level run lengths and a number of feature vectors in diverse directions are retrieved using a Chroma channel. This system employs a Support Vector Machine (SVM) classifier to detect falsified photographs. According to the approach, the restored attributes also outperform those derived from the blue, green, and red luminance channels. The test was conducted using the COLUMBIA and CASIA v1.0 datasets, with an accuracy of 94.3%, 94.7%, and 82.1%, 85.0%, respectively, on the Cb and Cr channels.

Another method is built on the Discrete Cosine Transform [DCT] and Local Binary Pattern (LBP), in which Alahmadi et al. [20] proposed a unique method for picture splicing forgery detection using a passive technique. After converting the RGB input image to YCbCr colour space, the chrominance channel is divided into overlay blocks, and LBP images are created from each block. Once the LBP images have been translated from the spatial domain to the 2D- DC Transform frequency domain, the DC Transform coefficients are utilised as a feature vector. The SVM classifier is given these feature vectors to classify counterfeit and authorised images. Three datasets, COLUMBIA, CASIA v2.0, and CASIA v1.0, were used in this technique, and performance was measured at 96.6 %, 97.5%, and 97%, respectively.

Using Gray Level Co-occurrence Matrix (GLCoM) structures, Wang et al. [21] proposed a method for identifying splicing in pictures. Following that, the image is transformed into a YCbCr colour scheme. In this procedure, the authors employed the chrominance channel's GLCoM. Because the grey standards along the edges of these channels are unnecessary, the threshold is adequate to reduce the size of GLCoM features. A Brute Force Scheme (BFS) technique was used to reduce the feature vector's size and increase the classifier's performance. The LIB-SUVM classifier is then used to train these feature vectors to recognise the counterfeit image. Only GLCoM characteristics are employed in this method, and no picture orientation information is used. With 50 dimensions, this method attained the most incredible accuracy rate of 90.50%.

He et al. [22] suggested a technique for splicing image forgery using Cosine Transform and Wavelet domain based on Markov characteristics. Firstly, using the input image's cosine coefficients and wavelet coefficients and Markov features are retrieved. Finally, the spliced and legitimate picture is classified using the support vector classifier. The maximum acceptance rate was 94.01% on the COLUMBIA dataset, whereas on the CASIA v2.0 dataset, it was 89.76%.

By combining a Pyramid Transform with Binary Pattern, Muhammad et al. [23] proposed an approach for forgery detection. In this chrominance channels were transformed using steerable pyramid after converting a colour image into YCbCr colour space. A histogram of the LBP transformed sub-bands was created to identify the tamper images. The suggested approach for sorting images into spliced and authentic uses a SUVM classifier. The LBP histogram's feature is employed in this technique, even though the Accuracy results in this methodology were more considerable, with a score of 97.33 % on the CASIA v2.0 dataset. On the other hand, the image's size and orientation information are missing.

To detect spliced images, Agarwal and Chand [24] suggested a multi-scale entropy filter and local phase quantization (LPQ). An entropy filter is used to filter the chrominance channel of a colour image to define its boundaries. After that, the LPQ operator produces internal image statistics based on phase data. To discriminate between non-forged and forged pictures, the histograms of each feature are aggregated and input into a SUVM classifier. This paper demonstrated how their approach might be used to identify copy-move fraud and splicing. The feature vector's chrominance channel width has been increased owing to the approach's use of several entropy filter sizes. When the dataset is balanced and small, the SUVM classifier can handle the two-class issue effectively. The acceptance rates for this technique were 98.33%, 95.41%, and 91.14%, respectively, on CASIA 2.0, CASIA v1.0, and COLUMBIA. It demonstrates that the approach fails without a textured design in the picture.

According to Abrahim et al. [25], the merged image can be recognized by analysing the texture properties of the picture. Several textures and colour aspects of the image are considered in the proposed framework, including higher-order statistical features, histogram-oriented gradients (HoG), and LBP. The features are merged to form a feature vector. These feature vectors are validated using an Artificial Neural Network (ANN) to describe the tamper regions. The majority voting model, in which unique qualities are directed input into an ANN classifier, is likewise defined in this framework. Despite the enhanced Accuracy rate, the effective cost and duration of the technique have risen. Zhang et al. [26] employed a Deep Learning (DL) strategy to identify picture area forgeries. A weighted auto-encoder model for feature extraction was used in the first step to combine contextual information from each patch for successful detection. The CASIA 2.0 and CASIA 1.0 datasets achieve a maximum Accuracy of 87.51% for JPEG pictures. On the CASIA 2.0 dataset, Jaiswal and Srivastava [27] also tested a primary DL strategy employing the deep residual network for forgery detection.

Some of the techniques mentioned above, such as GLCoM, LBP and HoG [22-25] employ colour and texture characteristics, whereas others, such as Discrete Cosine Transform and DWT use frequency-based features. The limitations of the methodologies mentioned above are summarized in the following points. The techniques' global characteristics have the advantages of being simple to calculate, rapid, and compact. None of the studies included

orientation and scale characteristics, except [22-25]. These approaches do not extract information about translation and rotation. Image features for smooth edges are not detected, resulting in data loss. Dong [28] suggested forgery detection and localisation using CASIA image dataset. Further, other latest Deep learning (DL) methods were discussed for forgery detection in images and classification [28-36]. Suresh et al. [37] proposed a method using LBP feature extraction on Low Level (LL) band of Discrete wavelet Transform (DWT) decomposition of images for forgery detection and have achieved good results on multiple attacks like rotation, scaling, translation. But this method failed to classify images for forgery detection. Babu et al. [38] proposed a technique using Polar Complex Exponential Transform (PCET) and directional pattern for image forgery detection, which resulted in better performance.

These methods employ SVM-based or ANN-based machine learning techniques to categorize images as forged or non-forged. SVM can handle vast feature spaces, although it is inefficient when dealing with large datasets.

Multimedia tools have been extensively used since the year 2000 and many methods have been used to identify the fake images. Finally, the approaches outlined above do not capture all of the properties of fake pictures from more extensive data sets. The proposed approach is targeted to operate on large datasets and to identify tamper areas with minimum time of computation.

3. METHODOLOGY

Image forgery detection is a binary classification task that defines whether or not an image has been forged. ResNet architecture mainly consists of convolution, batch normalization, and pooling operations, where these operational blocks are repeated during processing of any input image for a classification task. During this process, the width and height of the layer remain constant. Usually 3*3 convolutions were performed on images with dimensions of 64, 128, 256, and 512 pixels. Skip connections are used in the ResNet model during the process of signal and layer reduction is obtained by stride movement. For the ResNet 50 model, there are 50 layers with 48 -convolutional blocks, average pooling, and normalization. Each of the 2-layer blocks in ResNet 34 was replaced with a 3-layer bottleneck block, forming the ResNet 50 architecture. The model mainly consists of residual blocks with skip connections, which play a vital role in the feature extraction of the input. In addition, the ResNet model employs identity connections to avoid the vanishing gradient problem in neural networks.

The proposed method includes Residual Neural Network (ResNet) models of different variants and is allowed to train and test on multiple benchmark datasets of Copy Move forgery and Splicing Image Forgery. Images are well classified on the proposed model, and the best validation accuracy is attained on the three models of Residual Neural Network (ResNet) with Adam optimization. The flow chart below in Figure 1.b and block diagram in Figure 1.a indicates different steps which are present in ResNet algorithm. The proposed method includes ResNet-50, ResNet-101, ResNet-151 models trained and tested for CoMoFoD, MICC-F2000, and CASIA v2 datasets and for localization of tamper areas, Gradient class Activation Mappings (Grad-CAM) have been used. The HD5 model is obtained after training and testing and is used for testing the images for the presence of tamper areas in prediction and localization. Classification Accuracy of higher values is obtained and is compared with state-of-the-art methods. Also, the three models of Residual Neural Network (ResNet) are robust to rotation, shearing, noise presence, and blur in the images of the forgery dataset. Algorithm 1 shows the steps for proposed algorithm using ResNet algorithm.

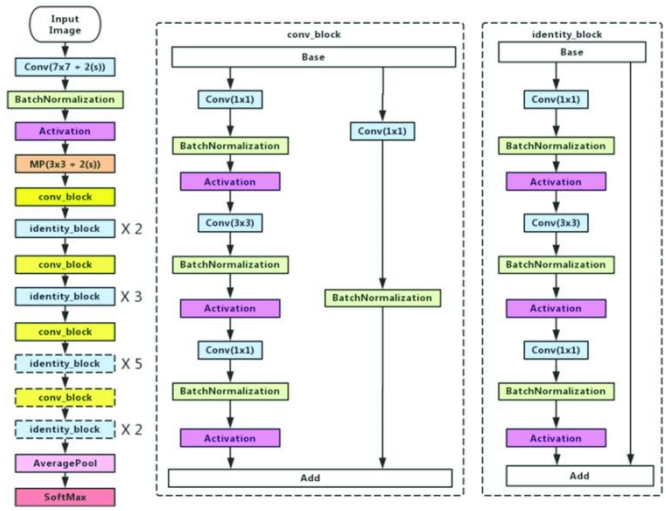

Figure 1a. ResNet-50 architecture comprising convolution block and identity block for learning image features [36]

Algorithm 1 steps - proposed method

Start

1. *Read the Forgery Dataset "Si, Ti" where i = 1 to n*
2. *Pre-process all pictures & use the net weights for training and testing of images*
3. *Choose the batch size as b_s and number of epochs for evaluation.*
4. *Select the Adam optimizer (learning rate)*
   - *Set $n_b = n/ b_s$ as the value for mini-batch size.*
5. *Train the network with tuning parameters for each epoch.*
6. *At each step, from batch 1 to batch n_b*
   - *Train the model for images and reduce the cross-entropy loss.*
   - *For each epoch use Back-propagate for loss calculation.*
   - *Enhance the parameters.*
7. *Re-arrange pictures into real and fake categories.*
8. *Detection of fraud areas in images.*
9. *Apply Gradient class activation mapping (Grad-CAM) for tracing forged areas.*

End

The following is a flowchart for detecting forgeries in images of benchmark dataset. We read the benchmark dataset for Image forgery Classification. Pre-Processing procedures (image scaling, segregation into two folders of actual and altered photographs) are used on the dataset for classification into real and fake images. Dataset undergoes cross-validation during pre-processing process of algorithm. Adam optimizer parameters were tuned to desired values, and download the Residual Neural Network (ResNet) algorithm's 'Image Net' weights, and produce the Model summary. In the training

phase, using the categorical cross-entropy for loss computation minimizes the error function, and graphing the training phase against total epochs of training minimizes the error function.

Metrics evaluation in training Accuracy and testing Precision and Recall matrices are generated for each dataset based on Accuracy. During each dataset, logs are generated for the training and testing phases. The image prediction uses a model created for tamper detection. To identify fabricated regions in pictures, localization employing Gradient class activation mapping (Grad-CAM) is used. Multiple models are compared to each benchmark dataset during evaluation process.

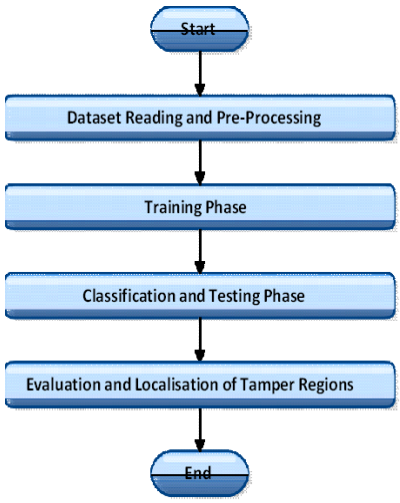

Figure 1b. Flow chart of proposed method

4. EVALUATION OF PROPOSED METHOD

Several tests are used to test the proposed method for detecting altered images. The approach is tested on various picture datasets [28-30], including the scene, natural, texture, and animal categories. The suggested method is also compared to previously published ISD methods and Copy-Move forgery. In comparison to previously discovered methodologies, the proposed technique yields superior outcomes. The datasets and assessment measures are described in the sections below.

4.1 Datasets

Three benchmark datasets [28-30] are used to test the proposed technique These three datasets are explained in Table 1. CASIA v2.0 [28], the initial dataset, is similar to CASIA v1.0 and comprises fake images for testing. The photographs have been processed in numerous ways, including scaling, rotation, and distortion. After the areas were cropped, several post-processing techniques such as blurring were applied. Images in various formats are included in the collection (.jpg and .tiff). The dataset has 12,614 images with dissimilar sizes from 240 × 160 to 900 × 600 pixels, with 7491 realistic and 5123 fake images. Images in the second dataset CoMoFoD [29], have been subjected to various processing techniques, including translation, rotation, scaling, distortion, and combination. The dataset contains 260 images with sizes 512 × 512 and 3000 × 2000 pixels, with 60 large images. MICC-F2000 [30], the third dataset, has 2000 photos, 700 of which have been tampered images and 1300 original images. The photographs have been processed in various ways, including rotation and distortion. The dataset has 2000 images with the size of 2048 × 1536 pixels.

Table 1. Datasets used for the proposed algorithm

Dataset	Size	Total Images	Image Format
CASIA v2.0 [28]	240 × 160 & 900 × 600	12,614	JPG, TIFF, BMP
CoMoFoD [29]	512 × 512	10,000	BMP
MICC -F2000 [30]	2048 × 1536	2000	JPG

4.2 Evaluation metrics

Every classifier model requires evaluation metrics to measure classifier performance. The first model assessment phase, a 10-fold cross-authentication test, is used to assess the categorization technique utilized in this study. In this technique, datasets are separated into nine parts for training and one part for testing, with nine parts being used to train the classifier model and one part being used to test the learned model. The dataset's average value influences the outcome. The classifier model's confusion matrix is then utilized to calculate classifier assessment metrics, including accuracy, recall and precision. A confusion matrix is a 2 × 2 square matrix that clarifies the performance of a model having two retort classes (negative and positive). As a result, there are four values: True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). TP: The positive class was correctly anticipated. TN: The negative class was correctly anticipated. FP: The positive class was incorrectly anticipated. FN: Anticipated the negative class incorrectly. The formulas 1,2,3,4 can be used to calculate the Accuracy (Acc), Recall (R), Precision (P) and F1-Score of the above-mentioned confusion matrix, where accuracy provides an overall result about how often the model is correct. F1-Score represents the likelihood that an image is correctly classified based on analysis, while Precision (P) represents the likelihood that an image is correctly classified based on true value. The formula for computing these metrics is shown below.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

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

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

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

4.3 Implementation details

The Jupyter Notebook IDE was used to develop algorithms using Python programming. The algorithm was put into practise using the Tensor flow and Keras Deep learning libraries. With an i3 processor, 8GB RAM and Nvidia Graphics Card 1050 serves as a hardware resource for neural net training and testing platforms. Adam optimizer is used for optimization with learning rate :0.01, weights; 'imagenet', 'softmax' as activation function, categorical cross-entropy as

loss function. During training process the number of epochs used were 05 with 75 incremental steps. Adam optimizer is used in our proposed method for updating the network weights more efficiently than traditional stochastic gradient descent. In earlier deep learning methods, gradient descent is used, whereas the proposed method uses Adam for deep learning model training. Adam merges the finest features of the Ada-Grad and RMS-Propagation methods to have an optimization algorithm capable of dealing with sparse gradients on noise issues. Batch size of 16 is considered with learning rate of 0.01.

5. RESULTS AND DISCUSSION

Experiments with the proposed approach were carried out on a Windows OS with an i5-processor, 8 GB RAM and a NVidia Graphic Card with GPU-1050.In the suggested method, the characteristics of images are separated into two folders (real and tamper) before pre-processing and are trained and tested accordingly. This study presents a novel result that shows how the proposed method outperforms other state-of-the-art approaches. These section summaries the results of experiments conducted on three distinct datasets and their analyses

The proposed methodology was studied as a image forgery classification algorithm for two classes that is original and forgery. Original patches had been chosen from original image sections, whereas deformed patches were chosen from the embedded area's boundaries. The patch has been chosen to be 28x28 pixels in size. A Half-patch overlap of 20 pixels was used to choose patches again from the image. The pixels in the patches had normalized prior to training. For each epoch the algorithm has been trained for 75 incremental steps and the proposed network was trained and tested accordingly. In Table 2 three proposed models are compared with respect to training and testing Accuracies. As depicted in Table 2, the proposed method with the CoMoFoD dataset gives superior accuracy than the proposed methods with CASIA v2.0 & MICC-F2000.

Table 2. Illustration of three proposed ResNet models in terms of validation and training accuracy (Acc) using Adam optimizer

S.No	Proposed model using ADAM Optimizer	MICC-MF2000	COMOFOD	CASIA-v2
1	RESNET-50	Training Acc: 97% Validation Acc: 97%	Training Acc: 98% Validation Acc: 99%	Training Acc: 86% Validation Acc: 73%
2	RESNET-101	Training Acc: 98 % Validation Acc: 97%	Training Acc: 98% Validation Acc:96%	Training Acc: 86% Validation Acc: 77%
3	RESNET-151	Training Acc: 96 % Validation Acc: 96%	Training Acc: 96% Validation Acc: 97%	Training Acc: 86% Validation Acc: 74%
4	Localisation using GRAD-CAM technique	**Achieved-√** ***Acc = Accuracy**	**Achieved-√**	**Achieved-√**

The test is run on the first dataset, CASIA v2.0, in the first instance. Table 2 illustrates the test and training accuracies on the CASIA v2.0 dataset Compared to previous methodologies, the proposed model has a 142-dimension vector with Training Accuracy of 86% and 80% as Validation Accuracy. Using the CASIA v2.0 dataset (shown in Figure 2), the proposed method detects the location of faked regions. The dataset was separated into training and test images and have been trained on ResNet-50, ResNet-101, and ResNet-151 neural networks. Plots obtained using CASIA v2.0 dataset indicate red-for Validation and blue- for Training curves. Figures 3 and 4 indicate Accuracy and Loss curves. Evaluation of testing Accuracy and Loss curves is shown for 300 steps and epochs. From Figures 3 and 4, it is observed that ResNet -50 classifier using CASIA v2.0 dataset has improved Accuracy and low Loss compared to ResNet -101, and ResNet -151. ResNet -50, ResNet-101, and ResNet-151 neural networks performed well using CASIA v2.0 dataset and obtained higher Accuracy and decreased Loss compared to other methods.

The second case experiment demonstrated a model on the CoMoFoD dataset. The Accuracy and F1-Score are shown in Table 3 using benchmark datasets. Table 3 compares experimental results on the CoMoFoD dataset with results from different models on the same dataset, as mentioned before. Compared to existing approaches, the proposed methodology has higher Accuracy of 99.3 % and F1-Score of 0.96. The proposed process is displayed in Figure 5, utilizing the CoMoFoD dataset to identify the location of forged regions in benchmark datasets. Table 3 demonstrates that the proposed strategy outperforms existing methods using Deep learning algorithms.

The image collection (dataset) was separated into training and test samples and has been tested on ResNet-50, ResNet-101, and ResNet-151 neural network using CoMoFoD dataset. During Evaluation red and blue colour indicates in Validation Accuracy and Training Accuracy. Evaluation of metrics with Accuracy and Loss curves is shown in Figures 6 and 7. From Figures 6 and 7, it is observed that ResNet-50 classifier using the CoMoFoD dataset has shown improvement in Accuracy and decrement in Loss compared to ResNet-101, and ResNet-151 models. ResNet variants using CoMoFoD dataset has shown increased Validation Accuracy and minimum Loss during evaluation using Adam optimizer.

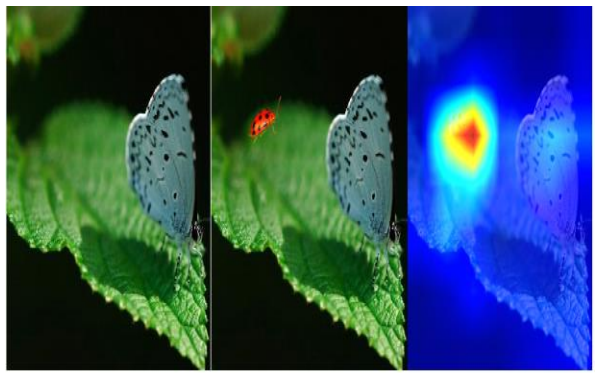

Figure 2. Original image (leftmost), fake image (middle image), and localization of forged areas (rightmost) image, image courtesy CASIA v2.0 dataset

The proposed model is also tested on MICC-MF2000 dataset. Its Accuracy is compared to the preceding approaches against state of art methods and found to be out casting those techniques. Table 3 compares the experimental outcomes to different models on the MICC-MF2000 dataset. Compared to

existing approaches, the proposed model has an Accuracy of 99.8%. The proposed model is displayed in Figure 8, utilizing the MICC-MF2000 dataset to identify the location of forged regions using GRAD-CAM technique.

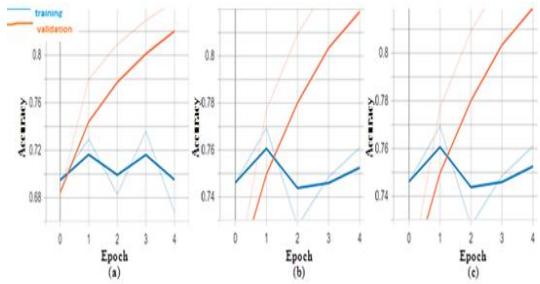

Figure 3. Accuracy vs Epochs curves of (a) ResNet-50, (b) ResNet -101, and (c) ResNet -151 using CASIA v2.0 dataset **(----training curve, ----testing curve)**

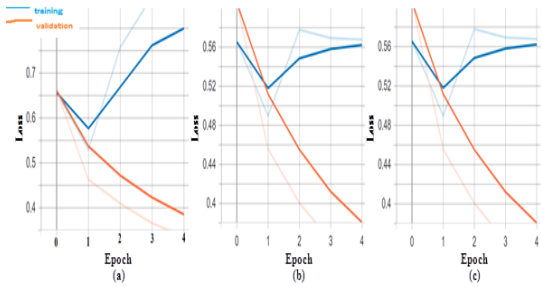

Figure 4. Loss vs Epochs curves of (a) ResNet -50, (b) ResNet -101, and (c) ResNet -151 using CASIA v2.0 dataset (----training curve, ----testing curve)

Figure 5. Original image (leftmost), fake image (middle image), and localization of forged areas (rightmost) from CoMoFoD dataset

The dataset was separated into training and test samples of images for ResNet -50, ResNet -101, and ResNet -151 neural network for forgery classification. Figures of red (Validation) and blue (Training) curves indicate Accuracy and Loss plots. Evaluation on dataset is shown in Figures 9 and 10. From Figures 9 and 10, it is observed that ResNet -50 using the MICC-MF2000 dataset has shown improved Accuracy and low Loss compared to ResNet -101, and ResNet -151 networks. ResNet -50, ResNet-101, and ResNet -151 neural networks using MICC-MF2000 dataset performed well in terms of Validation Accuracy and Training Accuracy with minimum loss during evaluation phase.

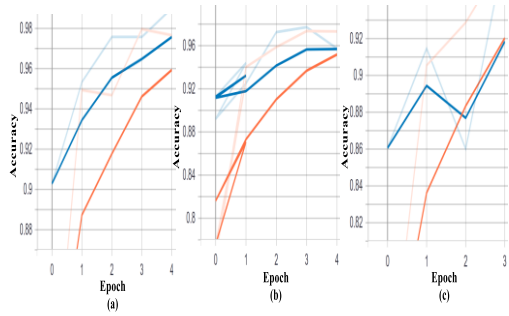

Figure 6. Accuracy curves of (a) ResNet -50, (b) ResNet -101, and (c) ResNet -151 using CoMoFoD dataset (----training curve, ----testing curve)

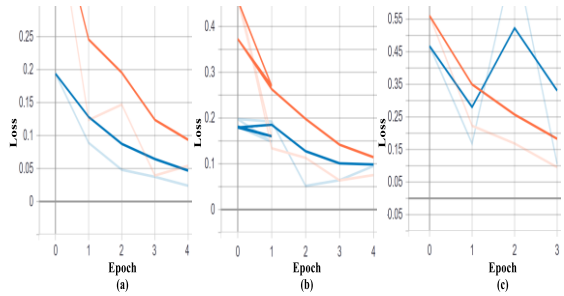

Figure 7. Loss curves of (a) ResNet -50, (b) ResNet -101, and (c) ResNet -151 using CoMoFoD dataset (----training curve, ----testing curve)

Figure 8. Original image (leftmost), fake image (middle image), and localization of forged areas (rightmost) using MICC-MF2000 dataset.

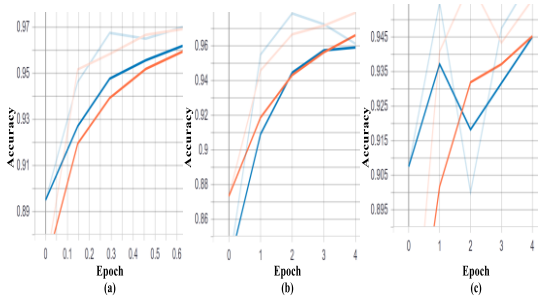

Figure 9. Accuracy curves of (a) ResNet -50, (b) ResNet-101, and (c) ResNet-151 with MICC-MF2000 dataset. **(----training curve, ----testing curve)**

Table 3. Performance of the proposed method against the state-of-the-art methods

S.no	Method/year	CASIA v2 dataset	COMOFOD dataset	MICC-MF2000 dataset	Accuracy	F1-Score
1	CNN/ 9 -Convolution layers/2016	√	√	√	98.0 %	
	Proposed network	√			99.0 %	0.98
					Localisation achieved	
2	Mantra-Net/2019	√			56.14%	
	Buster-Net/2020	√			49.06%	
	CAT-Net/2021	√			87.29%	
	Proposed Network	√			77%	0.80
					Localisation achieved	
3	KEY-POINT CLUSTERING/2020		√		94%	
	VGG-16 MODEL/2020		√		94%	
	Proposed network		√		99%	0.93
					Localisation achieved	0.98
4	CNN/3 conv layers/2021				96%	
	Hand-crafted feature point /2016			√	95%	0.74
	VGG-16 based (block 5-pool)/2019			√	97%	0.96
	Proposed network				Localisation achieved	
5	MASK RCNN/2020			√	97%	
	Proposed network				97%	0.97
					Localisation achieved	0.97
6	VGG-16 MODEL/2020			√	97%	0.97
	Proposed network				97%	0.97
					Localisation achieved	

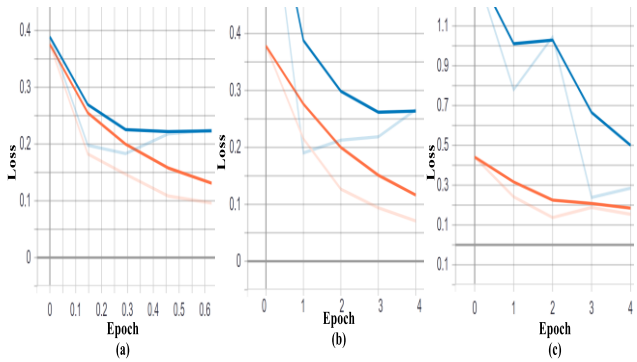

Figure 10. Loss curves of (a) ResNet -50, (b) ResNet- 101, and (c) ResNet -151 with MICC-F2000 dataset (----training curve, ----testing curve)

6. CONCLUSION

This paper uses the Deep Learning (DL) approach using Residual Neural Network (ResNet) variants to provide an automated tool to decide forgery in spliced and non-spliced images and Copy-Move forgery images. The paper's key contributions are the most basic feature set that it may be utilised to appropriately categorise the composite images and Copy-Move forgery and a full evaluation of the proposed model outcasts the existing approaches and traditional approaches. CASIA v2.0, MICC-MF2000, and CoMoFoD are three datasets used to test the proposed model's evaluation metrics. The texture, nature, and scenes of the images in these datasets are all highly distinct. Detecting spliced forged images in such a diverse set of images is a difficult challenge. On the CASIA v2.0 dataset, an accuracy of 77% is achieved and 99% accuracy on MICC-MF2000. And 98.6% accuracy on the CoMoFoD dataset was achieved using the ResNet architecture. The proposed work's results demonstrate that the modeled classifier recognizes counterfeit photos more effectively than the previous techniques. By utilizing a similar feature set and deep learning approaches, localizing spliced items in a picture is possible. Furthermore, as shown in the Figures 2, 5, 8, localisation is accomplished by employing the Gradient-Class Activation Mapping (Grad-CAM) approach on three different benchmark datasets. Further, the ResNet model is robust to rotation, shearing, and noise presence in images of tampered images. In the future, these methods may be extended to be implemented on cloud computing and hardware for optimization of metrics.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING

This research received funding from RUSA Grants from JNTU-Kakinada University, Kakinada, Andhra Pradesh, India.

REFERENCES

[1] Thakur, R., Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief Review. Forensic Science International, 312: 110311. https://doi.org/10.1016/j.forsciint.2020.110311

[2] Warif, N.B.A, Wahab, A.W.A., Idris, M.Y.I., Ramli, R., Salleh, R., Shamshirband, S., Choo, K.K.R. (2016). Copy-move forgery detection: Survey, challenges and future directions. Journal of Network and Computer Applications,75(2016):259-278. http://dx.doi.org/10.1016%2Fj.jnca.2016.09.008

[3] Ferreira, W. D., Ferreira, C.B.R., Júnior, G.C., Soares, F. (2020). A review of digital image forensics. Computers & Electrical Engineering, 85: 106685. https://doi.org/10.1016/j.compeleceng.2020.106685

[4] Dua, S., Singh, J., Parthasarathy, H. (2020). Detection and localization of forgery using statistics of DCT and Fourier components. Image Communication, 82: 115778. https://doi.org/10.1016/j.image.2020.115778

[5] Gani, G., Qadir, F. (2020). A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata. Journal of Information Security and Applications. https://doi.org/54. 10.1016/j.jisa.2020.102510

[6] Meena, K.B., Tyagi, V. (2020). A copy-move image forgery detection technique based on tetrolet transform. Journal of Information Security and Applications. 52(2020): 102481. https://doi.org/10.1016/j.jisa.2020.102481

[7] Sharma, S., Ghanekar, U. (2018). A hybrid technique to discriminate Natural Images, Computer Generated Graphics Images, Spliced, Copy Move tampered images and Authentic images by using features and ELM classifier. Optik, 172: 470-483. https://doi.org/10.1016/j.ijleo.2018.07.021

[8] Alberry, H.A., Hegazy, A.A., Salama, G.I. (2018). A fast SIFT based method for copy move forgery detection. Future Computing and Informatics Journal, 3(2): 159-165. https://digitalcommons.aaru.edu.jo/fcij/vol3/iss2/3

[9] Badr, A., Youssif, A., Wafi, M. (2020). A Robust copy-move forgery detection in digital image forensics using SURF. 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (2020), Beirut, Lebanon, pp. 1-6. https://doi.org/10.1109/ISDFS49300.2020.9116433

[10] Tinnathi, S., Sudhavani, G. (2021). An efficient copy move forgery detection using adaptive watershed segmentation with AGSO and hybrid feature extraction. Journal of Visual Communication and Image Represent, 74(2021): 102966. https://doi.org/10.1016/j.jvcir.2020.102966

[11] Ulloa, C., Ballesteros, D.M., Renza, D. (2021). Video Forensics: Identifying Colorized Images Using Deep Learning. Applied Sciences, 11(2): 476. https://doi.org/10.3390/app11020476

[12] Pachón, C.G., Ballesteros, D.M., Renza, D. (2021). Fake Banknote Recognition Using Deep Learning. Applied-Science, 11(3): 1281. https://doi.org/10.3390/app11031281

[13] Rao, Y., Ni, J.Q. (2016). A deep learning approach to detection of splicing and copy-move forgeries in images. 2016 IEEE International Workshop on Information Forensics and Security (WIFS), United Arab Emirates, pp. 1-6. https://doi.org/10.1109/WIFS.2016.7823911

[14] Rodriguez-Ortega, Y., Ballesteros, D.M., Renza., D. (2021). Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. Journal-of-Imaging, 7(3): 59. https://doi.org/10.3390/jimaging7030059

[15] Kumar, S., Gupta, S.K. (2020). A Robust Copy Move Forgery Classification Using End to End Convolution Neural Network. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 253-258. https://doi.org/10.1109/ICRITO48877.2020.9197955

[16] Liu, Y., Guan, Q., Zhao, X. (2018). Copy-move forgery detection based on convolutional kernel network. Multimedia Tools and Applications, 77: 18269-18293. https://doi.org/10.48550/arXiv.1707.01221

[17] Muzaffer, G., Ulutas, G.A (2019). A new deep learning-based method to detection of copy-move forgery in digital images. In Proceedings of the 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), Istanbul, Turkey, pp. 1-4. https://doi.org/10.1109/EBBT.2019.8741657

[18] Agarwal, R., Verma, O.P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimedia Tools and Applications, 79: 1-22. https://link.springer.com/article/10.1007/s11042-019-08495-z, accessed on Nov. 12, 2022.

[19] Zhao, X., Li, J., Li, S, Wang. S. (2010). Detecting digital image splicing in chroma spaces. International Workshop on Digital Watermarking, pp. 12-22. https://link.springer.com/chapter/10.1007/978-3-642-18405-5_2, accessed on Dec. 10, 2022.

[20] Alahmadi, A.A., Hussain, M., Aboalsamh, H., Muhammad, G. (2013). Splicing image forgery detection based on DCT and local binary pattern. 2013 IEEE Global Conference on Signal and Information Processing, TX, USA, pp. 253-256. https://ieeexplore.ieee.org/document/6736863, accessed on Dec. 10, 2022.

[21] Wang, W., Dong, J., Tan, T. (2009) Effective image splicing detection based on image Chroma. IEEE International Conference on Image Processing, Cairo, Egypt, pp 1257-1260. https://doi.org/10.1109/ICIP.2009.5413549

[22] He, Z.W., Lu, W., Sun, W., Huang, J.W. (2012). Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognition, 45(12): 4292-4299. https://doi.org/10.1016/j.patcog.2012.05.014

[23] Muhammad, G., Al-Hammadi, M.H., Hussain, M., Bebis, G. (2014). Image forgery detection using steerable pyramid transform and local binary pattern. Machine Vision Applications, 25: 985-995. https://doi.org/10.1007/s00138-013-0547-4

[24] Agarwal, S., Chand, S. (2015). Image forgery detection using multi scale entropy filter and local phase quantization. International Journal of Image, Graphics and Signal Processing, 8: 64-74. https://doi.org/10.5815/ijigsp.2015.10.08

[25] Abrahim, A.R., Rahim, M.S.M., Bin, S.G. (2018). Splicing image forgery identification based on artificial neural network approach and texture features. Cluster Computing, pp. 1-14. https://doi.org/10.1007/s10586-017-1668-8

[26] Zhang, Y., Goh, J., Win, L.L., Thing. V. (2016). Image region forgery detection: a deep learning approach. Singapore Cyber-Security Conference, 14: 1-11. https://doi.org/10.3233/978-1-61499-617-0-1

[27] Jaiswal, A.K., Srivastava, R. (2019) Image splicing detection using deep residual network. SSRN Electronic Journal. https://doi.org/0.2139/ssrn.3351072

[28] Dong, J., Wang, W., Tan, T. (2013). CASIA image tampering detection evaluation database. In Proceedings of the 2013 IEEE China Summit and International Conference on Signal and Information Processing, Beijing, China, pp. 422-426.

[29] Tralic, D., Zupancic, I., Grgic, S., Grgic, M. (2013). CoMoFoD — New database for copy-move forgery detection. Proceedings ELMAR-2013, Zadar, Croatia, pp. 49-54. https://www.researchgate.net/publication/266927943, accessed on Dec. 20, 2022.

[30] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE, 6(3): 1099-1110. https://doi.org/10.1109/TIFS.2011.2129512

[31] Wu, Y., Abd Almageed, W., Natarajan, P. (2019). ManTra-Net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, pp. 9535-9544. https://doi.org/10.1109/TIFS.2011.2129512

[32] Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). BusterNet: Detecting copy-move image forgery with source/target localization. In Proceedings of the European Conference on Computer Vision (ECCV), Glasgow, UK, pp. 23-28. https://doi.org/10.1007/978-3-030-01231-1_11

[33] Kwon, M.J., Yu, I.J., Nam, S.H., Lee, H.K. (2021). CAT-Net: Compression artifact tracing network for detection and localization of image splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, pp. 375-384. https://doi.org/10.1109/WACV48630.2021.00042

[34] Ali, S.S., Ganapathi, I.I., Vu, N.S., Ali, S.D., Saxena, N., Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. Electronics, 11(3): 403. https://doi.org/10.3390/electronics11030403

[35] Jaiswal, A.K., Srivastava, R. (2020). A technique for image splicing detection using hybrid feature set. Multimedia Tools and Applications, 79: 11837-11860. https://doi.org/10.1007/s11042-019-08480-6

[36] Ali, L., Alnajjar, F., Jassmi, H., Gochoo, M., Khan, W., Serhani, M. (2021). Performance evaluation of deep CNN-based crack detection and localization techniques for concrete structures. Sensors, 21(5): 1688. https://doi.org/10.3390/s21051688

[37] Suresh, G., Srinivasa Rao, C. (2016). RST invariant image forgery detection. Indian Journal of Science and Technology, 9(22): 1-8. https://doi.org/10.17485/ijst/2016/v9i22/89227

[38] Babu, S.B.G., Rao, C.S. (2022). Efficient detection of copy-move forgery using polar complex exponential transform and gradient direction pattern. Multimedia Tools and Applications, 82: 10061-10075. https://doi.org/10.1007/s11042-022-12311-6