Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Copy Move Image Tampering : Genuine and Tampered Region Identification and Classification using Various Residual Network Approaches

Smruti Dilip Dabhole
Department of computer science
Karnataka State Akkamahadevi Women University Vijayapura, Karnataka INDIA -586108

G.G Rajput
Department of computer science
Karnataka State Akkamahadevi Women University Vijayapura, Karnataka INDIA -586108

Prashantha
Department of Computer Science,
Rani Channamma University,
Belagavi India.

***Abstract*-Image tampering or forgery involves altering the content of an image with the intent to create false information in images. Developing techniques and methodologies to detect manipulated images is a significant research area in computer vision and forensic science. Copy-move forgery is a well-known kind of forgery, where a portion of an image is copied and pasted within the same image to either conceal or duplicate objects. The research aims to detect copy-move forgery and identify tampered or pristine regions in images. In real-world scenarios, having ground truth images for tampering identification is highly unlikely. Therefore, the goal is to develop a robust copy-move forgery detection model that does not rely on any reference images. In this, paper we propose a ResNet50 neural network architecture taking its advantage of skip connections in residual network for feature extraction and self-correlation approach to find similarity between features in an image using the input image and corresponding mask. A Mask Decoder is employed to up-sample feature maps to the original picture size. Error Level Analysis (ELA) is calculated for ROIs from predicted masks to distinguish as genuine and tampered region in an image. The experiment is performed on MICC-F2000 and CoMoFoD dataset. The proposed model is trained on Tampered images. The performance and efficiency of the proposed model are evaluated using accuracy and loss parameters. The proposed method yields better results in various test cases such as scaling, rotation, blur, noise and other images. The testing accuracy of proposed model is 99% for MICC-F2000 and 98% for CoMoFoD. The results of proposed method are compared to those of previously published methods. Classification of the tampered images identical regions into either pristine or tampered without relying on any kind of reference image**

***Keywords*— deep learning, ELA, Forgery Detection, genuine, ResNet50, Tampered**

I. INTRODUCTION

Digital images are extensively used in scientific publications, invoices, multimedia security, forensics, and document verification. Images pose a significant concern, whether it is photographs of suspects, crime scenes, biometric images, or others, they have long served as crucial tools in forensics and public safety endeavors[1,2]. With the advancement of digital photography, the utilization of digital images in these fields has become increasingly common. While digital image processing has facilitated easier manipulation of images, it has also spurred the emergence of innovative forensic investigation techniques. However, the validity of digital images is now being questioned due to the widespread availability of numerous image alteration programs, which serve as strong evidence in various types of crimes and are essential for documentation purposes. Moreover, the accessibility and simplicity of picture editing and processing software have streamlined the process of capturing and modifying photos. Among the prevalent forms of image fraud copy-move forgery is a specific type of image tampering [3].

The “copy-move” approach generates fresh content within an image by extracting a segment from the same image. Essentially, this involves replicating a specific region within the image. As the characteristics in the image, including illumination, proportion, and focus, remains unaffected, such images are more likely to exhibit no discernible evidence of tampering [4]. Copy-move is typically utilized with the intention to make an object “disappear” from the image by covering it with a segment copied from another part of the image. Patterns found in textured surfaces like grass, foliage, gravel, or fabric offer an ideal camouflage for digital manipulation. When copying elements from these areas, the irregular patterns facilitate seamless blending with the background, making it difficult for the human eye to spot any inconsistencies. Since the copied sections originate from the same image, they maintain uniformity in noise, color, and other essential properties, ensuring compatibility with the overall image. Consequently, methods that detect statistical disparities across different image regions struggle to identify these forgeries. To further obfuscate detection, techniques such as feathered cropping or retouching can be employed

Several methods have been found in the literature including block matching techniques, keypoint-based methods, DCT domain analysis, analyzing gradient of the image, multi resolution techniques and deep learning methods [5, 6, 7, 26]. Combining multiple techniques or developing hybrid methods can enhance the accuracy and robustness of copy-move forgery detection systems. Moreover, ongoing research in this field continually improves the effectiveness of detection methods to keep pace with evolving digital manipulation techniques.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Many of the methods are effective at identifying copied regions within an image; they often face challenges in accurately distinguishing between genuine and tampered areas within the same image [3, 4, 5, 6, 10, 21]. In this paper, we present deep learning approach to identify tampering within an image and classifying the detected region as genuine or tampered without relying on any reference image (figure 1).

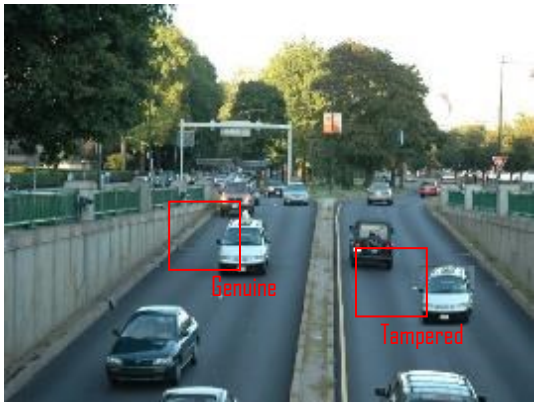


Figure 1. The genuine region and tampered region of the image (Source MICC-F2000)

The rest of the paper is organized as follows, section 2 focuses on literature review, section 3 deals with the proposed methodology, and Section 4 presents results and discussion. Section 5 presents comparative analysis of the proposed methods with the methods in the literature and conclusion is presented in section 6.

II. RELATED WORK

In the literature, various methods for copy-move forgery detection have been proposed 10, 16, 26], each leveraging different techniques and approaches to identify duplicated regions within an image. Here, we provide brief overview of some of these methods.

A. Block Based Forgery Detection

These methods partition the image into fixed-size blocks and compare them to detect identical or similar regions. Techniques like block matching or block hashing are commonly used. Block matching involves sliding a window across the image and comparing the blocks within the window to find duplicates, while block hashing computes hash values for each block and compares them for similarity.

Azra Parveen et.al. [10] introduced a block-based approach for detecting copy-move forgery utilizing Discrete Cosine Transformation (DCT). In this method, a gray image is partitioned into overlapping 8x8 blocks, and features are extracted using DCT across different feature sets. Subsequently, the K-means clustering algorithm is applied to group these blocks. While radix sort is employed to match features, the use of the clustering method enhances the speed of matching in block matching, albeit at the cost of increased time for detecting forged parts in an image. However, the model encounters limitations when faced with images containing multiple forged regions. Next, the forgery detection method proposed by Badal Soni et.al.[37] studies various block-based techniques such as Singular Value Decomposition (SVD), PCA, FFT, and experiments carried out on various datasets with scaling and rotational attacks. Even Osamah M. Al-Qershi et.al. [21] presented an approach that involves the use of overlapping blocks, and features are clustered through the K-Means algorithm. The RANSAC method is applied to eliminate outliers, and subsequently, the results are identified using a binary detection map. Ankit Kumar Jaiswal et.al. [19] introduced a technique employing Shift Invariant Stationary Wavelet Transform (SWT) and Block Division Mean feature vector in the YCbCr color space. This approach utilizes overlapping blocks for feature extraction, with the blocks further subdivided into 4 rectangular and 2 triangular blocks. While the method successfully identifies forgery, it is associated with high computational time.

B. Keypoint Based Forgery detection

Keypoints are distinctive points in the image, such as corners or junctions, characterized by their local features. Keypoint-based methods extract keypoints from the image and match them to identify duplicated regions. Algorithms like Scale-Invariant Feature Transform (SIFT) or Speeded-Up Robust Features (SURF) are employed for keypoint extraction and matching.

The hybrid optimization method presented in [18] uses a cutting-edge deep learning method called stacked sparse denoising autoencoder (SSDAE) to determine if the photos are real or false. Furthermore, the Spotted Hyena optimizer (SHO) and the Grasshopper Optimization Algorithm (GOA) are utilized to optimize the SSDAE model's weight and bias parameters for classification. Method proposed by Aditya Pandey et.al. [17] determine which part of the image has been altered and forecasts the matching mask. In light of the findings, methods, and recommendations are offered to create a stronger foundation for spotting and identifying tampering using deep learningThe UNET-based model is used in identifying output masks and the locations of the tamper in addition to identifying regions of the image that have been altered. Analyzing the raw image in some way (DCT or ELA) is still a useful step in strengthening the model. Hesham A. Alberry, et al [9] presented manipulation detection method using Fast SIFT techniques for forensic images from the MICC-220 dataset. Fuzzy C Means clustering is used to detect the forgery portion. Kunj Bihari Meena et.al [8] introduced a hybrid approach that combines Fourier Mellin technique with SIFT for a keypoint-based approach. This hybrid method is preferred over using solely SIFT, as the latter struggles to extract keypoints from smooth regions. The image is partitioned into smooth and textured parts, with SIFT applied in the textured region and FMT utilized in the smooth region. The matching of keypoints and blocks is achieved through G2NN and PatchMatch algorithms, respectively. Chengyou Wang et.al [11] introduced a novel approach that combines Accelerated-KAZE (A-KAZE) and Speeded-Up Robust Features (SURF) for forgery detection. Many keypoint-based forgery detection methods face challenges in acquiring sufficient points in smoother regions. To overcome this limitation, the proposed method establishes low response

thresholds for both the A-KAZE and SURF feature detection steps. The innovation extends to the introduction of a correlation coefficient map, which delineates duplicated regions through a fusion of filtering and mathematical

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

morphology operations. Rigorous experiments validate the effectiveness of this method in identifying duplicated areas and its resilience against various distortions and post-processing techniques such as noise injection, rotation, scaling, image blurring, JPEG compression, and hybrid image manipulation. Significantly, the experimental results highlight the superiority of the proposed approach compared to other tested copy-move forgery detection methods.

The above explained methods works on single image. Therefore, in the area of tampering detection continuous growth is taking place using deep learning approach to work on large datasets.

C. Deep Learning Based Forgery Detection

Deep learning approaches, particularly convolutional neural networks (CNNs), have shown promising results in copy-move forgery detection. CNNs can learn hierarchical representations of features directly from image data, making them effective at capturing complex patterns and variations associated with copy-move forgeries.

Yaqi Liu et.al.[16] presented CMFDFormer, a Transformer-style copy-move forgery detection network to support CMFDFormer in handling new tasks. The authors defined a novel PCSD (Pooled Cube and Strip Distillation) continual learning architecture, to enhance the detectability of forgeries and prevent disastrous forgetting while tackling new tasks. The components of CMFDFormer are a mask prediction network using PHD (Pluggable Hybrid Decoder) and a MiT (Mix Transformer) including CNN-style and MLP-style backbones, the Transformer-style MiT backbone network was implemented after thorough analysis. The PHD network is built using a multi-scale cycle fully connected block, mask reconstruction, hierarchical feature integration, and self-correlation computation. The proposed continuous learning framework uses cube pooling and strip pooling to limit intermediate features from the PHD network. Experiments performed on openly accessible datasets shows how well CMFDFormer performs and how useful the PCSD continuous learning architecture is for tampering detection. Nagaveni K et.al.[15] proposed a method utilizing pre-trained models in transfer learning to categorize fake photos. To identify the tampered pixels in terms of error level, first preprocessed the photos using the ELA. The findings show that merely deepening the network does not improve performance; rather, performance declines. The model's overfitting is the cause of the decline in performance. Therefore, using DenseNet and ResNet50, which include feature maps from earlier layers in the subsequent layer, overfitting is prevented. Compared to models that employed picture patches, the network's complexity and processing time are lower because it was trained using the entire set of images without the need for patches. Out of the six models that were used, the ResNet50 model performed better. Sumaira Bibi et.al. [30] introduced AlexNet and VGG16 for image feature extraction, and multiple structures stacked autoencoders (SAE) for tampering detection in various image compression schemes [30]. The classification of pristine and fake images is done using the Ensemble Subspace Discriminant classifier. And conducted a thorough ablation research on two CASIA datasets, and the outcomes with two autoencoders and AlexNet features outperform any other approach. Junlin Ouyang et. al [33] presented a new approach for detecting copy-move forgery using convolutional neural networks. The method utilizes a pre-trained model from a large database, such as ImageNet, and fine-tunes the network structure with small training samples of copy-move instances. The method results well in detecting copy-move forgery. However, it exhibits less robustness when faced with copy-move forgery scenarios in real-world situations. The author analyzed this limitation, visualizing the feature map of the convolutional neural network (CNN). Despite its imperfections, this method marks the first application of CNN in copy-move forgery detection. Kaur, N. et al [34] proposed a CMF detection framework based on deep learning, employing a combination of contrast-limited adaptive histogram equalization (CLAHE) and convolutional neural network (CNN) to classify images as pristine or tampered. The CLAHE algorithm enhances the visibility of hidden features in the image, making it easier to detect certain elements in CMF. The proposed framework's efficacy is evaluated using benchmark datasets, including GRIP, MICC-F2000, IMD, and MICC-F220 datasets which highlights the effectiveness of the proposed approach. Prabakar [35] proposed a hybrid method to detect tampering from noisy images. Initially, sample images from MICCF2000 were extracted. Subsequently, resized the images and applied a filtering technique to eliminate any noise that might have been present in the tampered image and finally, integrated Convolutional Neural Networks (CNN) and Support Vector Machine (SVM) to construct a hybrid DL model.

The methods mentioned above perform effectively in restricted constraints such as duplication of the object limited to one or two, dynamic range of intensity values in the image is limited, presence of outliers leads to wrong results and in certain cases computational time is high. Also, it doesn't highlight which region from the detection regions in an image is genuine or tampered.

III. METHODOLOGY

The proposed methodology detects and classifies the tampered region from the images. This section will outline the precise methods for implementing the procedure in depth, with the stages being separated into different categories: feature extraction, self-correlation, mask decoding, and classification (Figure 2).

A. Dataset Generated

The input dataset provided to the network is MICC-F2000. The dataset comprises of 1300 genuine images and 700 tampered images, all with a resolution of 739 × 492 [7,13]. This dataset is employed to assess the resilience of the proposed method against geometric attacks, encompassing translation, rotation, and stretching, as well as various combinations of these operations. Tampered images are used for training the structure. The algorithm's robustness is evaluated based on the degrees of rotation, stretch, and translation, each imposing distinct requirements on its performance. The dataset doesn't include any binary mask. Therefore, to train the proposed model binary mask for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

tampered images are created using genuine form of the image and the corresponding tampered image with the help of VGG Image Annotator (VIA). Here, the genuine and tampered portion is highlighted as shown in figure 3. The dataset is split into training and validation with 70% and 30% respectively. The image data is fed to the proposed model.

The experiment primarily focuses on the MICC-F2000 dataset and then extends its scope to include the CoMoFoD dataset. The CoMoFoD dataset comprises 10,000 images, each of size 512x512 pixels. Within this dataset, 200 images are genuine. Subsequently, additional images are generated in 25 categorize by applying post-processing attacks such as additive noise, JPEG compression, image blurring, color reduction, and contrast adjustment. Ground truth comparisons are facilitated by providing color masks and binary masks [38]. For the CoMoFoD dataset, 600 contrast-adjusted images are considered and fed into the model alongside their corresponding ground truth images.

B. FEATURE EXTRACTION USING RESNET50

Feature extraction using ResNet50 involves training the model with input images and their corresponding masks. The masks are binary images of size (256, 256, 1), while the images are in RGB format with dimensions (256,256,3). Utilizing the ResNet50 pre-trained model leverages its properties as a residual network with skip connections, enhancing the training performance of the model[22]. The initial layers of the ResNet50 architecture are employed to extract features from the images. Following this, the model is tasked with a self-correlation task to identify similarities within these features, with the goal of detecting cloned regions. This similarity detection task involves predicting a binary copy-move mask.

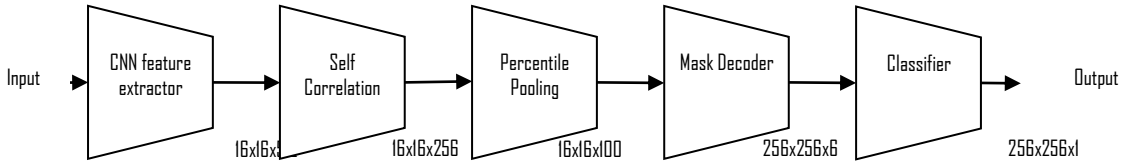


Figure 2: Proposed System Architecture for tampered image detection

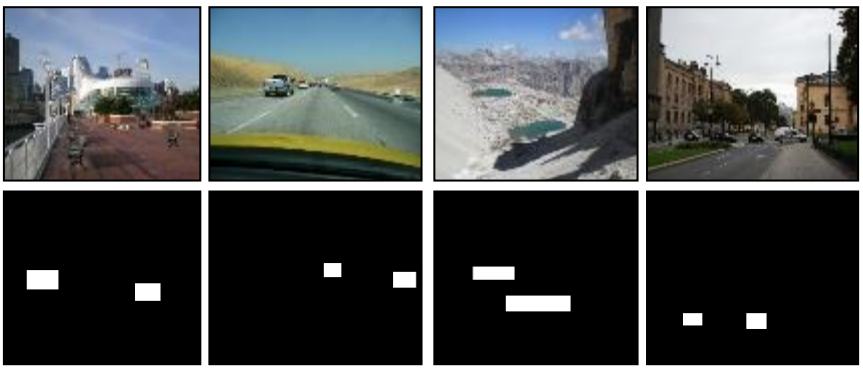


Figure 3: row 1: Tampered images row 2 : Mask images created using VGG image annotator

The process begins with feature extraction via the ResNet50 CNN Feature Extractor, which generates a feature tensor of size 16×16×512, resembling patch-like features of 16×16, each containing 512 dimensions. To identify matched patch-like features and recover potential copy-move regions, all-to-all feature similarity scores are computed using a Self-Correlation module. Subsequently, meaningful statistics are collected through percentile pooling, utilizing the Pearson correlation coefficient (ρ) to quantify feature similarity. This process results in a tensor of shape 16×16×100. To ensure the resulting network's capability to handle inputs of various sizes, percentile pooling selects scores at percentile ranks of interest, standardizing the sorted score vector. This step eliminates the network's reliance on input size variations. Once percentile pooling is completed, the feature maps are upsampled gradually to the original image size using a Mask Decoder. A binary classifier is then employed to produce a copy-move mask at the same resolution as the input image, fulfilling the auxiliary task of identifying copy-move regions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

C. Mask decoder and classification

The resultant CNN feature measures 16×16×512, exhibiting a resolution notably lower than that necessary for the manipulation mask. Hence, a decoding process is essential to restore the feature to its original resolution. Deconvolution techniques [31] are employed via the Mask Decoder. This decoding process alternates between BN-Inception and BilinearUpPool2D methods, resulting in a tensor sized 256×256×6. The dimensionality of 6 in the output filter is due to the final BN-Inception layer, denoted as 2@[5,7,11], which amalgamates three Conv2D responses. Each response comprises 2 output filters, with kernel sizes of (5,5), (7,7), and (11,11) respectively, totaling 6 output channels. Ultimately, the pixel-level manipulation mask is predicted using a Binary Classifier. This classifier entails a single Conv2D layer equipped with 1 filter and a kernel size of (3,3), followed by sigmoid activation for final mask generation.

D. Region identification using ELA

After identifying Regions of Interest (ROIs) in the manipulated image, differentiating between these ROIs in the genuine and tampered sections poses a challenge. To tackle this issue, the Error Level Analysis (ELA) technique is employed to categorize areas within an image as either genuine or tampered ELA highlights discrepancies in compression levels within an image, as areas that have been modified often display distinct error levels compared to their surroundings. JPEG compression plays a crucial role here, introducing compression artifacts that are utilized for analysis purposes. Additionally, the absolute difference is calculated by subtracting the compressed image from the original one to generate a difference image. From the classification layer, the predicted output determines the ROIs. ELA is then computed separately for these ROIs. The proposed method primarily focuses on discerning intensity differences. Subsequently, a threshold is applied to the ELA values to pinpoint regions exhibiting significant disparities, thus enabling the identification of pristine and manipulated areas.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The experiment is implemented using python 3.11 and TensorFlow2.0 for deep learning. The work is carried out on intel core i5 12th gen. and16GB RAM. The model has been trained with different epochs and empirically found that epoch=100 is the best fit. The learning rate for the model is 1e-2. The loss function 'binary_crossentropy' used to find the loss. During training, the model's parameters are adjusted to minimize the binary cross-entropy loss using the 'Adam' optimizer. The 'Accuracy' metric is used to calculate the accuracy of model.

B. Results for MICC-F2000 and CoMoFoD

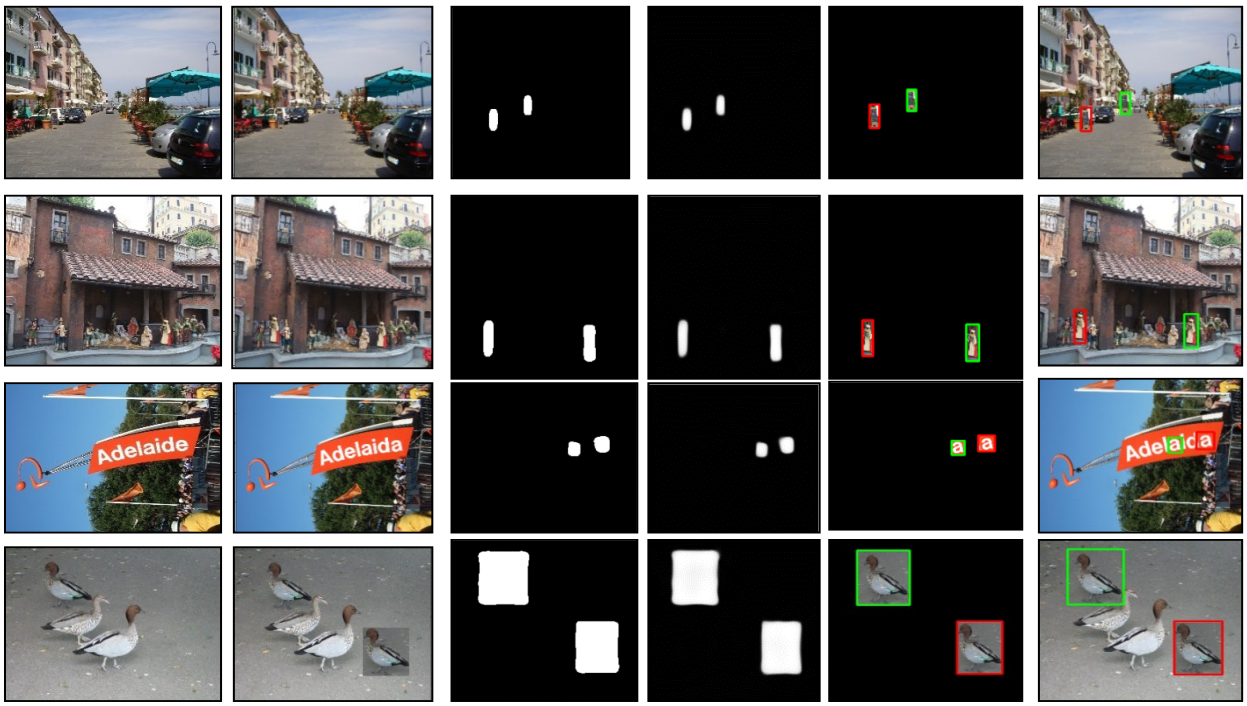
The model is tested using various images. Figure 4 and Figure 5 depict the testing results of the MICC-F2000 and CoMoFoD datasets, respectively, for sample images. In figure 4 and 5 (a) represents genuine image (b) showcases corresponding tampered images, while (c) and (d) depict the binary mask and predicted mask respectively. The binary mask delineates Regions of Interest (ROIs), which are further analyzed to identify genuine and tampered regions within each image. (e) presents tampered and genuine regions overlaid on the binary image with bounding boxes. Tampered regions are highlighted by red boxes, while genuine regions are marked by green boxes. And (f) represents output images of proposed method.
The effectiveness of the proposed model is demonstrated in Figure 6, which accurately identifies genuine and tampered regions, even in images with orientations such as rotation and scaling. Furthermore, Figure 7 showcases precise identification and classification of regions in images with post-processing effects such as noise and blur. The robustness of the proposed model is cross-validated using images from outside the dataset. Figure 8 illustrates the results from other dataset.

C. Analysis

The proposed model gives 99.72% training accuracy and 98.59% validation accuracy for MICC-F2000 dataset as shown in figure 9 and 99.37% training accuracy and 98.39% validation for CoMoFoD dataset shown in figure 10. The proposed model is tested for both the dataset. Figure 11 presents the results as confusion matrix. For MICC-F2000 and CoMoFoD dataset, 100 images are taken for testing. The model yields accuracy of 99% for images from MICC-F2000 and 98% for images from CoMoFoD dataset. Here, the proposed model is trained only on tampered images therefore, the testing has been done on tampered images. The dataset has been trained on VGG16 model [36], but VGG16 is not deeper architecture comparatively to ResNet50. Whereas, deeper architectures have potential to capture more complex features and representations from data which leads to better performance of model. The residual network employs skip connections, where the original input is added to the output of a convolutional layer. This approach effectively addresses the issue of vanishing and exploding gradients commonly encountered in traditional CNN models [39].

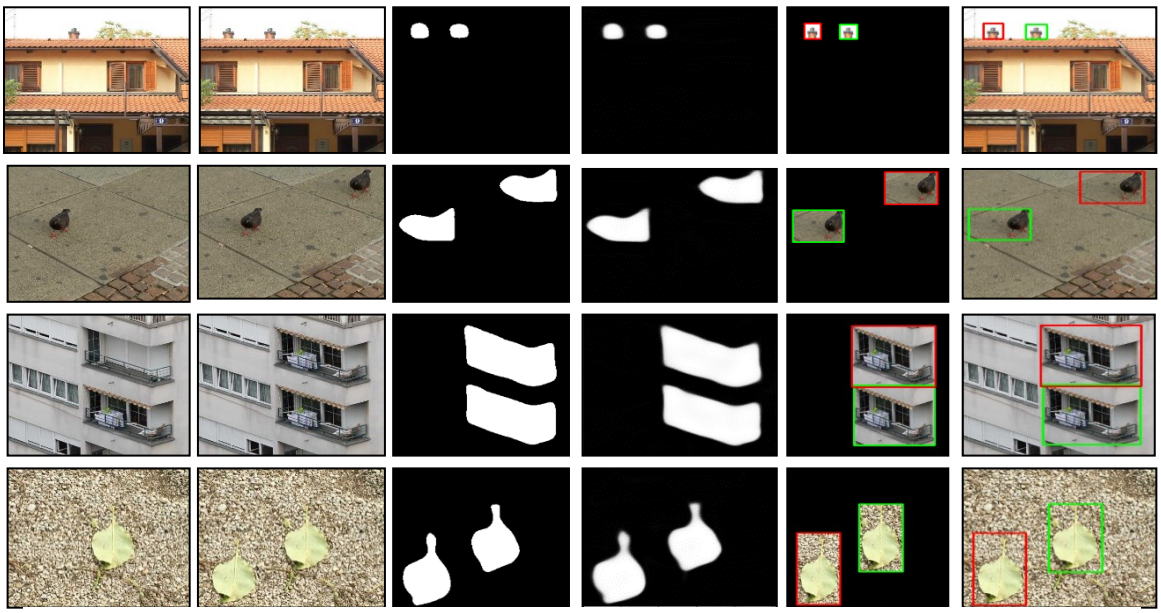
Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024



(a) (b) (c) (d) (e) (f)

Figure 4: Results for MICC-F2000 dataset (a): Genuine image (b): Tampered image (c): Binary Mask (d): Predicted Mask (e) : identified tampered (red box) and genuine (green box) (f) : Output image (Tampered and genuine regions identification)



(a) (b) (c) (d) (e) (f)

Figure 5: Results for MICC-F2000 dataset (a): Genuine image (b): Tampered image (c): Binary Mask (d): Predicted Mask (e) : identified tampered (red box) and genuine (green box) (f) : Output image (Tampered and genuine regions identification)

Figure 6: Row1 : Tampered image Row2 : Identified regions (Source :MICC-F2000 dataset)

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

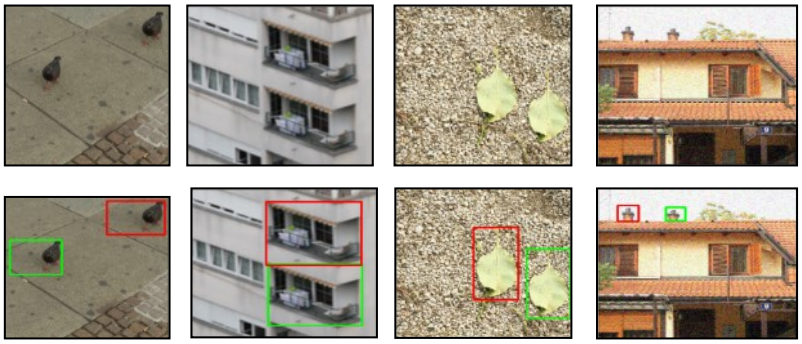


Figure 7 : Row1 : Tampered image Row2 : Identified regions (Source : CoMoFoD dataset)

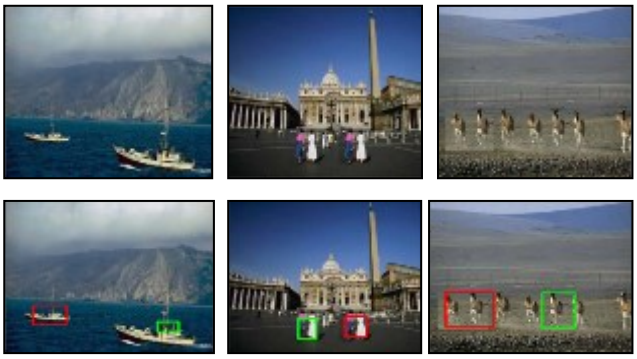


Figure 8: Sample images from other dataset, Row1 : Tampered Image Row2 : Identified regions

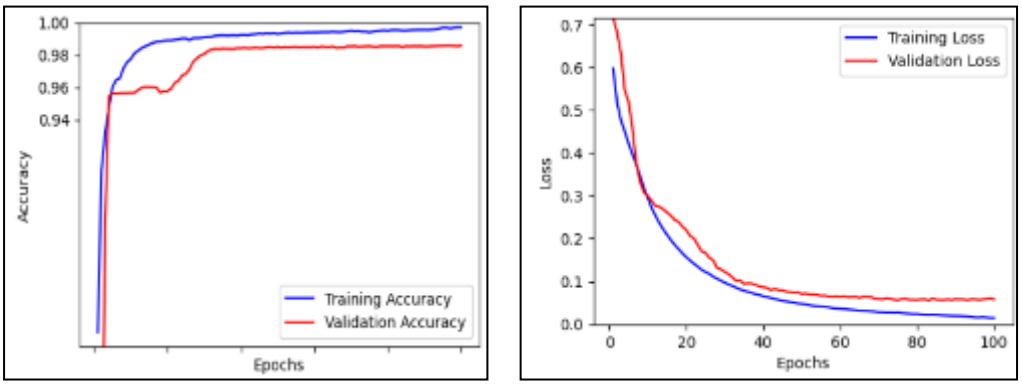


Figure 9: Performance analysis of the proposed model for MICC-2000 dataset

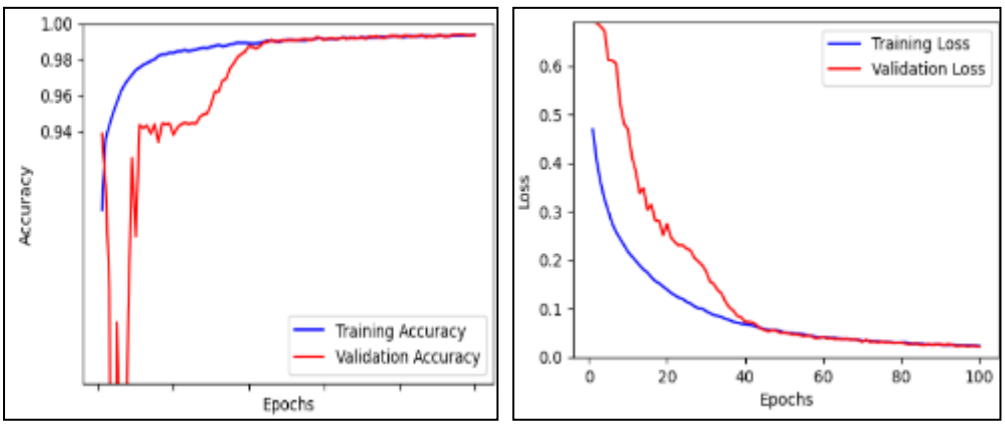


Figure 10: Performance analysis of the proposed model for CoMoFoD dataset

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

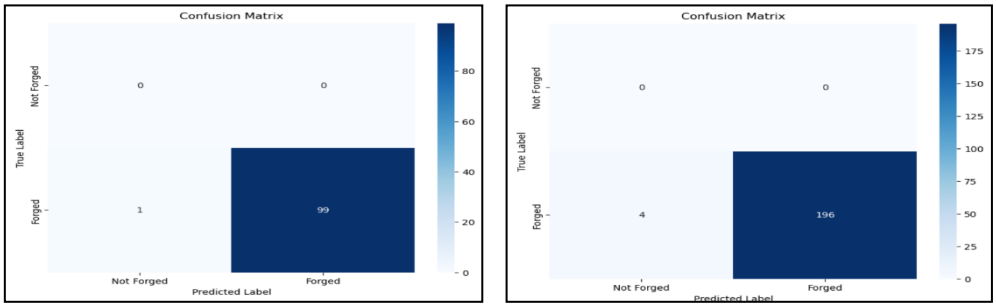


Figure 11 : Confusion Matrix for model testing for MICC-F2000 and CoMoFoD dataset

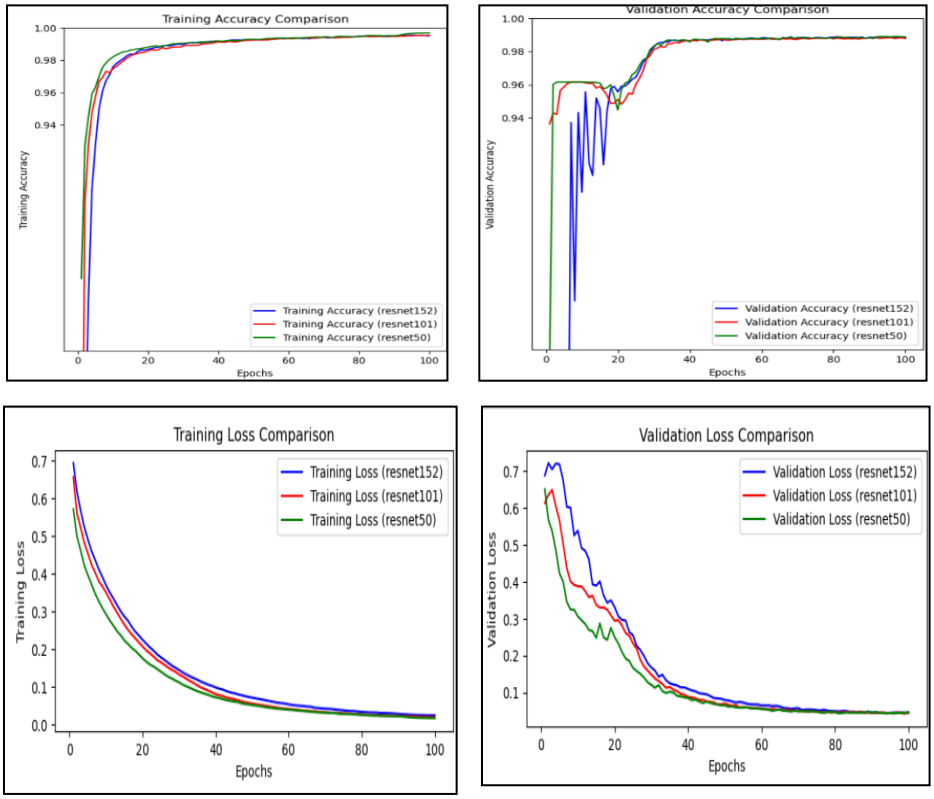


Figure 12. Comparison of ResNet50, ResNet101 and ResNet152 Network

Even the experiments are performed using ResNet101 and ResNet152 [40] architectures (figure 12) and it is observed that there is no significant difference between accuracy and loss. However, the complexity of model increases due to depth of layers and increases training time comparative to ResNet50. Deeper networks are more prone to overfitting, especially when the training dataset is limited. ResNet50's shallower architecture led to better performance in the proposed scenario where dataset is comparatively small.

D. Comparative analysis

The experimental study demonstrates the effectiveness of the proposed approach compared to other approaches. Table 1 provides a comparative analysis of the proposed method with other methods in the literature using MICC-F2000 dataset for performing experiments. And Table 2 presents the comparison wherein CoMoFoD dataset is used. The proposed method yields higher accuracy for the corresponding datasets.

In Table 1 and Table 2, the proposed methods are compared with both single image forgery detection and deep learning-based forgery detection. The methods [2,41,25,32] refer to single image forgery and remaining represent the neural network approach. However, these methods don't classify between genuine and tampered region. The proposed method and method presented by Wu et.al [36] identify between genuine and tampered region.

Table 1 : Comparative Analysis for MICC-F2000 dataset

Author	**Accuracy**
Amerini [41]	94.86
Amerini[2]	93.42
Elaskily et.al[20]	98.40
Ye et.al. [25]	98.5
Ahmed Sedik et.al[28]	94
Vaishali, Sharma et.al,[29]	97.63
Selvaraj et.al. [27]	89.74
Nidhi Goel et al [14]	96
Proposed Method	**99**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Table 2 : Comparative Analysis for CoMoFoD

Author	Accuracy
Wu et.al [36]	80.49
Selvaraj et.al [27]	78
Emre Gürbüz et.al. [23]	97.5
R. Thakur et.al [12]	95.97
Niyishaka, P., et.al [32]	96.84
B. Wen et.al [24]	72
Proposed method	**98**

V. CONCLUSION

Image forgery detection is a challenging task. The article presents a novice approach for copy move tampering detection without relying on any reference image. The proposed method utilizes a ResNet50 pre-trained neural network for feature extraction because of the advantage provided by the network about skip connections. Next, Self-correlation is used to find similarity between features using the input image and corresponding mask. The potential features are then collected using Percentile Pooling, and a Mask Decoder is employed to up-sample feature maps to the original picture size. Next, Error Level Analysis (ELA) is calculated for ROIs within the image to distinguish the genuine region and tampered region from the image. The experiment is performed on MICC-2000 and CoMoFoD. The evaluated results demonstrate that the proposed method outperforms state-of-the-art methods by a large margin, and is also robust against various known CMFD attacks such as blurring and noise. Followed by the orientations like rotation and scaling. Even model is cross verified dataset CASIA 1.0. The model has been trained on fewer number of images. Therefore, in the future, the work could be extended to large datasets.

REFERENCE

[1] Vincent Christlein, Christian Riess and Elli Angelopoulou, “On Rotation Invariance In Copy-Move Forgery Detection”, 2010 IEEE International Workshop on Information Forensics and Security, 12-15 Dec. 2010

[2] Irene Amerini; Lamberto Ballan; Roberto Caldelli; Alberto Del Bimbo; Giuseppe Serra ,“A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery”, IEEE Transactions on Information Forensics and Security (Volume: 6, Issue: 3, September 2011)

[3] Esha Tripathi, Upendra Kumar, Surya Prakash Tripathi, “Comparative Analysis of Techniques Used to Detect CopyMove Tampering for Real-World Electronic Images”, INTERNATIONAL JOURNAL OF INTEGRATED ENGINEERING VOL. 15 NO. 4 (2023) 201-225

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

[5] Wenyu Chen, Yanli Zhao, Wenzhi Xie and Nan Sang, "An improved SIFT algorithm for image feature-matching," 2011 International Conference on Multimedia Technology, Hangzhou, 2011, pp. 197-200, doi: 10.1109/ICMT.2011.6003022.

[6] G. G. Rajput and S. B. Ummapure, "Script identification from handwritten documents using SIFT method," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 520-526, doi: 10.1109/ICPCSI.2017.8392348

[7] Zanardelli, Marcello, et al. "Image forgery detection: a survey of recent deep-learning approaches." Multimedia Tools and Applications 82.12 (2023): 17521-17566.

[8] Kunj Bihari Meena & Vipin Tyagi, “A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms”, Multimedia Tools and Applications, https://doi.org/10.1007/s11042-019-08343-0, Springer Science+Business Media, LLC, part of Springer Nature 2020

[9] Hesham A. Alberry, et al “A fast SIFT based method for copy move forgery detection”, Future Computing and Informatics Journal 3 (2018) 159-165F

[10] Azra Parveen, Zishan Husain Khan, Syed Naseem Ahmad, “Block-based copy–move image forgery detection using DCT”, Iran Journal of Computer Science https://doi.org/10.1007/s42044-019-00029-y, Received: 22 June 2018 / Accepted: 8 January 2019 © Springer Nature Switzerland AG 2019

[11] Chengyou Wang , Zhi Zhang and Xiao Zhou, “An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features”, Symmetry 2018, 10, 706; doi:10.3390/sym10120706

[12] R. Thakur and R. Rohilla, "Copy-Move Forgery Detection using Residuals and Convolutional Neural Network Framework: A Novel Approach," 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India, 2019, pp. 561-564, doi: 10.1109/PEEIC47157.2019.8976868.

[13] Wujian Ye , Qingyuan Zeng , Yihang Peng, Yijun Liu and Chin-Chen Chang, “A two-stage detection method of copy-move forgery based on parallel feature fusion”, Eurasip Journal on wireless communications and networking, Springer Open, 2022

[14] Nidhi Goel, Samarjeet Kaur, Ruchika Bala, Dual branch convolutional neural network for copy move forgery detection, IET Image Processing

[15] Nagaveni K. Hebbar and Ashwini S. Kunte, “TRANSFER LEARNING APPROACH FOR SPLICING AND COPY-MOVE IMAGE TAMPERING DETECTION”, ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, MAY 2021, VOLUME: 11, ISSUE: 04ISSN: 0976-9102 (ONLINE) DOI: 10.21917/ijivp.2021.0348

[16] Yaqi Liu, Chao Xia, Song Xiao, Qingxiao Guan, Wenqian Dong, Yifan Zhang, Nenghai Yu, “CMFDFormer: Transformer-based Copy-Move Forgery Detection with Continual Learning”

[17] Aditya Pandey, Anshuman Mitra, “Detecting and Localizing Copy-Move and Image-Splicing Forgery”, F

[18] Ruchi Gupta, Pushpa Singh, Tanweer Alam & Shivani Agarwal, “A deep neural network with hybrid spotted hyena optimizer and grasshopper optimization algorithm for copy move forgery detection”, Springer Science+Business Media, LLC, part of Springer Nature 2022

[19] Ankit Kumar Jaiswal and Rajeev Srivastava, “Copy Move Forgery Detection Using Shift Invariant SWT and Block Division Mean Features”, Proceedings of IC3E 2018

[20] Elaskily, M.A., Elnemr, H.A., Dessouky, M.M. et al. Two stages object recognition based copy-move forgery detection algorithm. Multimed Tools Appl 78, 15353–15373 (2019). https://doi.org/10.1007/s11042-018-6891-7

[21] Osamah M. Al-Qershi,Bee Ee Khoo, “Enhanced block-based copy-move forgery detection using k-means clustering”, Multidimensional Systems and Signal Processing, © Springer Science+Business Media, LLC, part of Springer Nature 2018

[22] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.

[23] Emre Gürbüz, Guzin Ulutas, Mustafa Ulutas, "Detection of Free-Form Copy-Move Forgery on Digital Images", Security and Communication Networks, vol. 2019, Article ID 8124521, 14 pages, 2019. https://doi.org/10.1155/2019/8124521

[24] B. Wen, Y. Zhu, R. Subramanian, T. -T. Ng, X. Shen and S. Winkler, "COVERAGE — A novel database for copy-move forgery detection," 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA, 2016, pp. 161-165, doi: 10.1109/ICIP.2016.7532339.

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

[26] Mohamed A. Elaskily & Heba A. Elnemr & Ahmed Sedik & Mohamed M. Dessouky & Ghada M. El Banby & Osama A. Elshakankiry & Ashraf A. M. Khalaf & Heba K. Aslan& Osama S. Faragallah & Fathi E. Abd El-Samie, “A novel deep learning framework for copy-move forgery detection in images”, @Springer Science+Business Media, LLC, part of Springer Nature 2020

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

[27] Selvaraj, Arivazhagan & Shebiah, Newlin & M, Saranyaa & R, Shanmuga. (2024). CNN-based Approach for Robust Detection of Copy-Move Forgery in Images. Inteligencia Artificial. 27. 80-91. 10.4114/intartif.vol27iss73pp80-91.

[28] Ahmed Sedik, Yassine Maleh, Ghada M. El Banby, Ashraf A.M. Khalaf, Fathi E. Abd El-Samie, Brij B Gupta, Konstantinos Psannis, Ahmed A. Abd El-Latif, AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities, Technological Forecasting and Social Change,
Volume 177, 2022, 121555, ISSN 0040-1625,

[29] Vaishali, Sharma & Neetu, Singh. (2023). Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. Multimedia Tools and Applications. 1-25. 10.1007/s11042-023-15724-z.

[30] Sumaira Bibi et.al. "Digital Image Forgery Detection Using Deep Autoencoder and CNN Features", August 2021 Human-centric Computing and Information Sciences 11(32) DOI:10.22967/HCIS.2021.11.032

[31] Noh, H., Hong, S., Han, B.: Learning deconvolution network for semantic segmen tation. In: Proceedings of the IEEE International Conference on Computer Vision. pp. 1520–1528 (2015)

[32] Niyishaka, P., Bhagvati, C. Copy-move forgery detection using image blobs and BRISK feature. Multimed Tools Appl 79, 26045–26059 (2020). https://doi.org/10.1007/s11042-020-09225-6

[33] Junlin Ouyang, Yizhi Liu, Miao Liao "Copy-Move Forgery Detection Based on Deep Learning", 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI 2017)

[34] Kaur, N., Jindal, N. & Singh, K. A deep learning framework for copy-move forgery detection in digital images. Multimed Tools Appl 82, 17741–17768 (2023). https://doi.org/10.1007/s11042-022-14016-2

[35] D. Prabakar, R. Ganesan, D. L. Rani, P. Neti, N. Kalyani and S. K. Mudradi, "Hybrid Deep Learning Model for Copy Move Image Forgery Detection," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 1023-1028, doi: 10.1109/I-SMAC55078.2022.9987319.

[36] Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization. In: Ferrari, V., Hebert, M., Sminchisescu, C., Weiss, Y. (eds) Computer Vision – ECCV 2018. ECCV 2018. Lecture Notes in Computer Science(), vol 11210. Springer, Cham. https://doi.org/10.1007/978-3-030-01231-1_11

[37] Badal Soni, Debalina Biswas, "Image Forensic using Block-based Copy-move Forgery Detection", 978-1-5386-3045-7/18/$31.00 ©2018 IEEE

[38] Tralic D., Zupancic I., Grgic S., Grgic M., "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013

[39] V. Sharma and N. Singh, "Deep Convolutional Neural Network with ResNet-50 Learning algorithm for Copy-Move Forgery Detection," 2021 7th International Conference on Signal Processing and Communication (ICSC), Noida, India, 2021, pp. 146-150, doi: 10.1109/ICSC53193.2021.9673422

[40] Vaishali, S., Neetu, S. Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. Multimed Tools Appl 83, 10839–10863 (2024). https://doi.org/10.1007/s11042-023-15724-z

[41] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, Giuseppe Serra, Copy-move forgery detection and localization by means of robust clustering with J-Linkage, Signal Processing: Image Communication, Volume 28, Issue 6, 2013, Pages 659-66