Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Digital Image Forgery Detection Using CNN and Error Level Analysis (ELA)

Dr. Ch. Shashi Kumar[1], Dr. R. Srilatha[1], Dr. Vuppala Lakshmi Narayana[2], P. Rajasekhar[3]

[1]Assistant Professor, Department of Mathematics, VNR Vignana Jyothi Institute of Engineering and Technology, Telangana, India.
[2]Assistant Professor, Department of Mathematics, Vardhaman College of Engineering, Telangana, India.
[3]Assistant Professor, Department of Mathematics, University College of Engineering, JNTUK, Kakinada, Andhra Pradesh, India

Digital images are a primary source of information on social media, making them prime targets for malicious forgery. Existing forgery detection techniques often focus on a single type of forgery, limiting their practical applicability. This paper presents an enhanced digital image forgery detection approach using deep learning and transfer learning to simultaneously detect image splicing and copy-move forgeries. The proposed method identifies discrepancies in compression quality between forged and authentic regions. A deep learning model calculates differences between the original and compressed images, producing a feature map for a pre-trained model with a newly fine-tuned classifier. Comparing eight pre-trained models for binary classification, our results show that MobileNetV2 achieves the highest detection accuracy of 95% with faster training times. This paper also introduces an approach using Python and Convolutional Neural Networks (CNNs) with Error Level Analysis (ELA) for preprocessing. Our CNN model achieves 98% training accuracy and 92% validation accuracy on a dataset of 12,615 images, effectively identifying tampered regions. This combined approach significantly advances digital image forgery detection, with broad applicability in areas where image authenticity is crucial.

Keywords: Deep Neural Network (DNN), Image compression, Image forgery, Detection (IFD), Error Level Analysis (ELA).

1. Introduction

In the digital era, the manipulation of visual content has become widespread, posing significant challenges in verifying the authenticity of digital images. This paper addresses this issue by leveraging deep learning and image analysis techniques to detect forgeries.The increasing ease of using image editing tools has led to a rise in digital image manipulation, affecting fields like journalism, forensics, social media, and e-commerce, where the credibility of visual content is crucial. This paper aims to develop robust methods to detect manipulated images, thus maintaining trust and integrity in digital visual information.

The proposed solution combines Convolutional Neural Networks (CNNs), a leading deep learning architecture [10][15][19], with Error Level Analysis (ELA), a potent image analysis method. This hybrid approach is designed to accurately and reliably identify tampered images, distinguishing them from authentic ones.

Beyond detection, this project is vital for preserving the authenticity of digital images and preventing the spread of falsified visual information. Its implications are broad: They range from maintaining the reliability of news sources to assisting law enforcement in forensic investigations and ensuring the trustworthiness of e-commerce product image. This paper will detail its architecture, methodology, advantages, and potential future developments, aiming to provide a comprehensive solution for assessing digital image authenticity in an age of rapidly proliferating digital content.

The development of the Multiple Image Splicing Dataset (MISD)[1][2][3], aiming to address the limitations of existing datasets for image forgery detection. Existing datasets primarily focus on single image splicing, lacking multiple spliced images. The MISD, comprising 300 high-quality, annotated, and realistic multiple spliced images, fills this gap. It provides a ground truth mask for these images, offering researchers a valuable resource for advancing forgery detection techniques in this critical area of research.

M. A. Elaskily, M. H. Alkinani [2] introduces a novel approach for detecting copy move forgery in digital images using Deep Learning [17][22], specifically Convolutional Neural Networks (CNN)[8][11][16] and Convolutional Long Short-Term Memory (Conv LSTM) networks. By extracting image features through a sequence of convolutional layers, Conv LSTM layers[27][31], and pooling layers, the model effectively identifies copy move forgery. The algorithm is evaluated on four publicly available datasets and demonstrates high accuracy, reaching up to 100% for certain datasets with a low testing time of approximately 1 second. Additionally, the study compares the performance of the proposed hybrid ConvLSTM-CNN model with using CNN alone, highlighting the effectiveness of the combined approach.

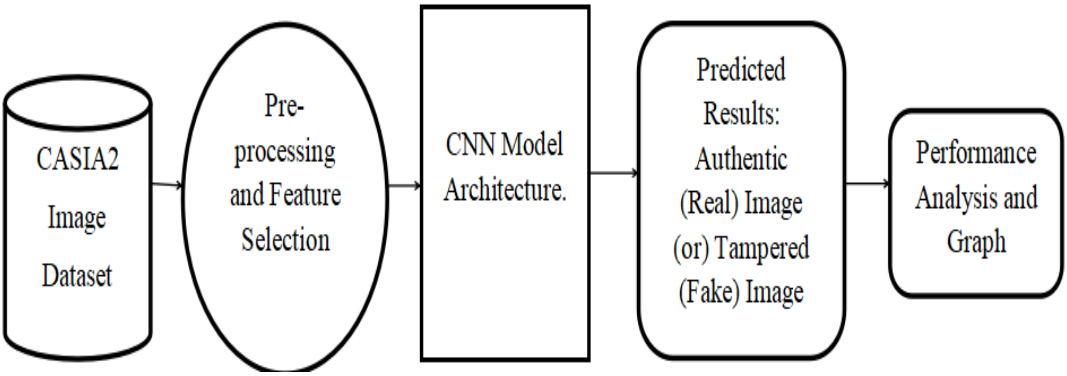
The paper [3] provides a comprehensive review of digital image forgery detection techniques, acknowledging the ubiquitous role of digital images across various domains such as clinical imaging, media broadcasting, and crime analysis. It emphasizes the historical perception of images as irrefutable evidence and highlights the contemporary challenge of image authenticity due to the widespread availability of image manipulation tools. By analyzing recent forgery detection methods and detailing the approaches employed in each stage, the paper aims to offer researchers valuable insights and updated information to facilitate ongoing progress in this field. Additionally, comparison tables are included for quick reference, enhancing the accessibility of the review.

The paper[4] presents a review of passive image forensics techniques[6], focusing on universal methods for detecting image tampering. Acknowledging the advancements in machine learning and deep learning-based approaches [24][31] in this field, the authors advocate for the evolution of fusion and reinforcement-based learning techniques[13]. To provide researchers with a comprehensive understanding of the domain, the review covers various directions, outcomes, and analyses of universal image forensics approaches. Unlike existing surveys that primarily focus on specific types of image manipulation like splicing or copy-move detection, this review explores type-independent techniques for detecting image tampering[33], including resampling, compression, and inconsistency-based detection methods. The paper outlines the approach used for the review, presents an analysis of the literature, and concludes with remarks on the subject. Additionally, the review identifies and enumerates various resources such as journals and datasets beneficial for the research community. Finally, This paper proposes an innovative reinforcement learning-based model for image forensics.

2. Proposed Method

Error Level Analysis (ELA) detects image manipulation by comparing compression levels at various quality settings. Initially, when an image is saved in JPEG format, it undergoes compression. If the image is subsequently edited and saved again, it undergoes additional compression. ELA calculates the difference in compression levels between the original and edited versions of an image. This method helps reveal discrepancies between forged and authentic images that may not be apparent to the naked eye. By analyzing the average difference in the quantization tables for luminance and chrominance, ELA can identify areas of manipulation in an image. Original images captured by digital cameras typically have higher ELA values, indicating minimal compression. However, subsequent edits and resaves result in decreased image quality, reflected in lower ELA values. ELA highlights areas of modification as regions with higher ELA levels, allowing for the detection of image alterations. This provides insights into how ELA operates and its significance in identifying forged images.

2.1 System Architecture


CASIA2 Image Dataset
Pre-processing and Feature Selection
CNN Model Architecture.
Predicted Results: Authentic (Real) Image (or) Tampered (Fake) Image
Performance Analysis and Graph

2.2 Details of Data Set

The first module of the Digital Image Forgery Detection system focuses on data collection, a crucial step in developing a machine learning model. The quality and quantity of the data obtained significantly impact the performance of the model. Various techniques,include web scraping or manual interventions can be employed for data collection. In this project, the dataset, comprising 12,615 digitally Image forged images, is sourced from Kaggle, a well-known repository for standard datasets commonly used by researchers. The dataset is stored in the model folder of the project for further processing and analysis.

We will utilize Python as its primary programming language. Initially, essential libraries like

Keras for constructing the main model, scikit-learn for partitioning training and test data, and PIL for image-to-array conversion will be imported. Additionally, other critical libraries such as pandas, numpy, matplotlib, and tensorflow will be included to facilitate various data processing and analysis tasks.

2.3 Retrieving the images

The process involves retrieving images from the dataset and converting them into a suitable format for model training and testing. This includes reading, resizing, and normalizing the pixel values of the images. Initially, both the images and their corresponding labels are retrieved. Subsequently, the images are resized uniformly to dimensions of (200, 200) to ensure consistency across all samples. Finally, the images are converted into numpy arrays for further processing and analysis.

2.4 ELA image analysis

The process starts by fetching images from the data set and preparing them for model training and testing. This includes reading, resizing, and normalizing pixel values. Images and labels are initially retrieved, followed by resizing to (200, 200) for consistency. Finally, images are converted into numpy arrays for analysis.

2.5 Splitting the dataset

The image dataset will be divided into training and testing sets, with an 80-20 split. This division allows for model training on a subset of the data, validation of performance, and testing on unseen data to assess accuracy.

The Keras sequential model is used to build a convolutional neural network (CNN). Initially, two Conv2D layers with 32 filters and a (5,5) kernel are added. This is followed by a MaxPool2D layer with a (2,2) pool size, halving the image dimensions, and a dropout layer with a 25% dropout rate. These layers are repeated with parameter adjustments. A flatten layer then converts 2-D data to a 1-D vector, followed by dense, dropout, and dense layers. The final dense layer has 2 nodes with softmax activation for probabilistic brain tumor prediction.

2.6 Convolutional Neural Networks

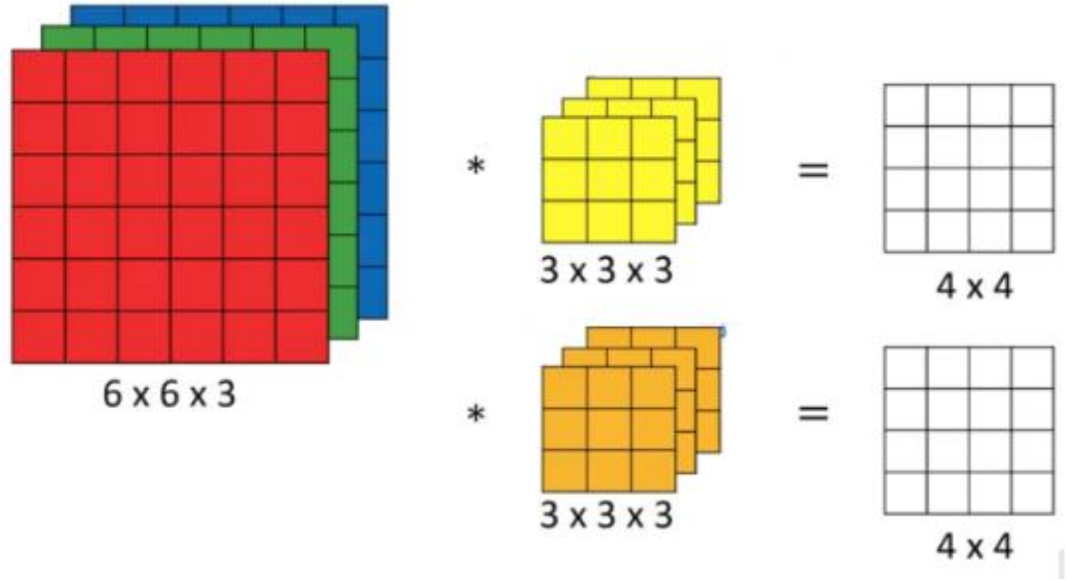
The process of convolving an input of 6 X 6 dimensions with a 3 X 3 filter yields a 4 X 4 output. This can be generalized for an input of n X n with a filter size of f X f, resulting in an output size of (n-f+1) X (n-f+1). However, this method presents two primary drawbacks: the image size shrinks with each convolution operation, and corner pixels are underutilized, risking information loss. To address these issues, padding is introduced, adding pixels around the image edges. Padding allows maintaining the original image size, preventing information loss during convolution. Two common padding options are Valid (no padding) and Same (padding to maintain input size). For Same padding, the padding value (p) is calculated as (f-1)/2. Using padded convolution ensures minimal information loss and image size preservation. This sets the stage for implementing strided convolutions in the subsequent discussion.

Trided Convolutions: By selecting stride of 2, the convolution process skips every other pixel horizontally and vertically. The resulting dimensions with stride s are calculated as

$$\left[\frac{n+2p-1}{s}+1\right]X\left[\frac{n+2p-f}{s}+1\right].$$

Stride efficiently reduce image size.

Convolutions Over Volume: For a 3-D input image of shape 6 X 6 X 3, a 3 X 3 X 3 filter is utilized. The dimensions represent height, width, and channels. The output shape is 4 X 4, achieved by convolving across all channels. Multiple filters, detecting different features, result in a changed output dimension, such as 4 X 4 X 2 with two filters.



Generalized Convolution Dimensions: Input dimensions are defined as n X n X n_c , while filter dimensions are f X f X n_c^1. Padding, stride, and output dimensions are calculated accordingly, considering the number of channels in the input and filters (n_c) and the number of filters (n_c^1).

One Layer of a Convolutional Network:A single layer in a CNN involves convolving input data with filters, adding biases, and applying activation functions constitutes one layer. Parameters are independent of image size, solely depending on filter size. For instance, with 10 filters of 3 X 3 X 3 shape, the total parameters are 280. Notations include f[l] for filter size, p[l] for padding, s[l] for stride, and n[c][l] for the number of filters.

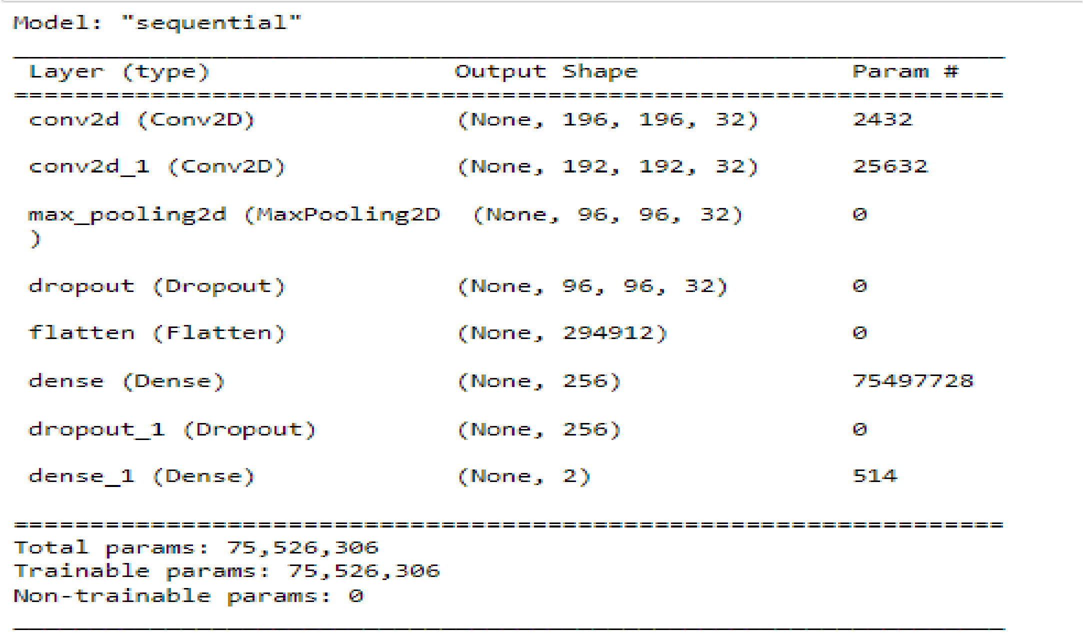
Convolutional Neural Network : In this example, a convolutional neural network (CNN) processes an input image of size 32 X 32 X 3. Initially, the image is convolved with 10 filters of size 3 X 3, resulting in an output of 37 X 37 X 10. Subsequent convolutions yield a final output of 7 X 7 X 40. These outputs are then flattened into a vector and fed into a classifier for predictions.

Hyperparameter Tuning: Various hyperparameters such as the number and size of filters, stride, and padding can be adjusted to optimize network performance. As the network progresses, image size typically decreases while the number of channels increases.

Pooling Layers Overview: In Convolutional Neural Networks (CNNs), pooling layers serve to reduce input size, accelerating computation. Max pooling, for instance, selects the maximum value within consecutive blocks. Average pooling calculates the average instead. Hyperparameters for pooling include filter size, stride, and pooling type.

CNN Example: A CNN comprises convolution and pooling layers initially, followed by fully connected layers and a softmax classifier for classification. Defined hyperparameters are crucial for network performance. As layers progress, input dimensions decrease while channel numbers increase.

3. Model Application and Accuracy/Loss:

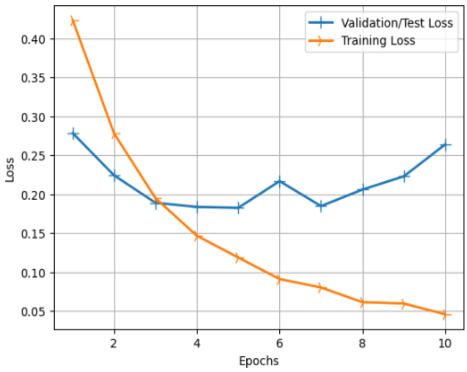


```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 196, 196, 32)      2432

 conv2d_1 (Conv2D)           (None, 192, 192, 32)      25632

 max_pooling2d (MaxPooling2D  (None, 96, 96, 32)       0
 )

 dropout (Dropout)           (None, 96, 96, 32)        0

 flatten (Flatten)           (None, 294912)            0

 dense (Dense)               (None, 256)               75497728

 dropout_1 (Dropout)         (None, 256)               0

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 75,526,306
Trainable params: 75,526,306
Non-trainable params: 0
_________________________________________________________________
```

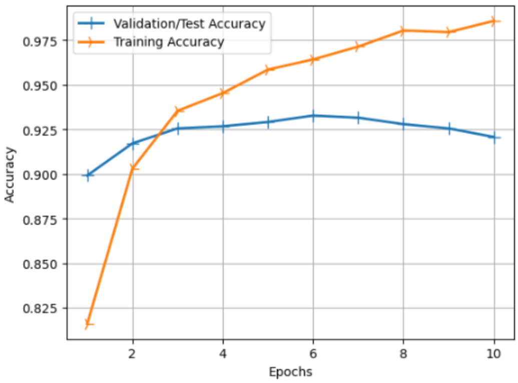
Upon constructing the model, it's evaluated on the validation set to measure accuracy and loss. This includes plotting these metrics against the epochs to visualize performance. The model is compiled and applied using the fit function with a batch size of 10. Graphs illustrating accuracy and loss are generated, showcasing an average training accuracy of 98%.

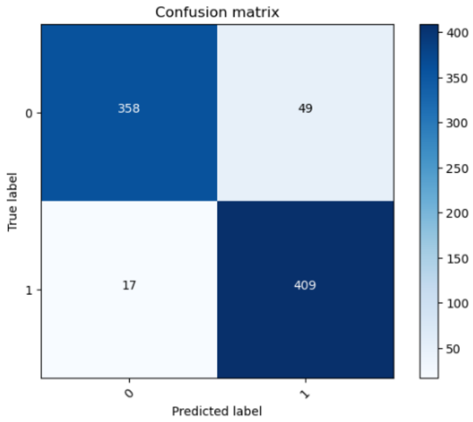
Test Set Accuracy: Following training and evaluation on the validation set, the model's accuracy is evaluated on the test set, a crucial metric for performance assessment. The model achieves a test set accuracy of 92%, indicating its effectiveness in generalizing to unseen data and its strong performance in forgery detection.

Model Loss



Model Accuracy





Metric	Value
Accuracy	0.92
Precision	0.89
Recall	0.92
F-Measure	0.92

4. Conclusion

The "Digital Image Forgery Detection Using CNN and ELA" paper introduces a powerful solution for addressing the critical concern of ensuring the authenticity and integrity of digital images. By combining Convolutional Neural Network (CNN) model architecture with Error Level Analysis (ELA), the system achieves high accuracy and adaptability in detecting digital image forgeries. Its utilization of a diverse dataset enables effective performance in real-world scenarios, with the added benefit of real-time implementation potential for seamless integration into various platforms. With the capability to identify both simple and complex forgeries, the proposed system significantly contributes to preserving image authenticity and combating digital manipulation. As a practical tool for forensic analysts, content moderators, and individuals verifying digital visual content credibility, this project represents a substantial advancement in the field of digital image forensics.

References

[1] K.D. Kadam, S.Ahirrao, and K.Kotecha, ‘‘Multiple image splicing dataset (MISD): A dataset for multiple splicing,’’ Data, vol. 6, no. 10, p. 102, Sep. 2021.

[2] M. A. Elaskily, M. H. Alkinani, A. Sedik, and M. M. Dessouky, ‘‘Deep learning based algorithm (ConvLSTM) for copy move forgery detection,’’ J. Intell. Fuzzy Syst., vol. 40, no. 3, pp. 4385–4405, Mar. 2021.

[3] A. Mohassin and K. Farida, ‘‘Digital image forgery detection approaches: A review,’’ in Applications of Artificial Intelligence in Engineering. Singapore: Springer, 2021.

[4]R. Agarwal, O. P. Verma, A. Saini, A. Shaw, and A. R. Patel, ‘‘The advent of Deep Learning-based,’’ in Innovative Data Communication Technologies and Application. Singapore: Springer, 2021.

[5] K.B. Meena and V. Tyagi, Image Splicing Forgery Detection Techniques: A Review. Cham,Switzerland: Springer, 2021.

[6] S. Gupta, N. Mohan, and P. Kaushal, ‘‘Passive image forensics using universal techniques: A review,’’ Artif. Intell. Rev., vol. 55, no. 3, pp. 1629–1679, Jul. 2021.

[7] W. H. Khoh, Y. H. Pang, A. B. J. Teoh, and S. Y. Ooi, ‘‘In-air hand gesture signature using transfer learning and its forgery attack,’’ Appl. Soft Comput., vol. 113, Dec. 2021, Art. no. 108033.

[8] Abhishek and N. Jindal, ‘‘Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation,’’ Multimedia Tools Appl., vol. 80, no. 3, pp. 3571–3599, Jan. 2021.

[9] M. M. Qureshi and M. G. Qureshi, Image Forgery Detection & Localization Using Regularized U-Net. Singapore: Springer, 2021.

[10] Y. Rao, J. Ni, and H. Zhao, ‘‘Deep learning local descriptor for image splicing detection and localization,’’ IEEE Access, vol. 8, pp. 25611–25625, 2020.

[11] K. M. Hosny, A. M. Mortda, N. A. Lashin, and M. M. Fouda, ‘‘A new method to detect splicing image forgery using convolutional neural network,’’ Appl. Sci., vol. 13, no. 3, p. 1272, Jan. 2023.

[12] F. Li, Z. Pei, W. Wei, J. Li, and C. Qin, ‘‘Image forgery detection using tamper-guided dual self-attention network with multi resolution hybrid feature,’’ Secur. Commun. Netw., vol. 2022, pp. 1–13, Oct. 2022

[13] C. Haipeng, C. Chang, S. Zenan, and L. Yingda, ‘‘Hybrid features and semantic reinforcement network for image,’’ Multimedia Syst., vol. 28, no. 2, pp. 363–374, 2021.

[14] Q. Li, C.Wang, X. Zhou, and Z. Qin, ‘‘Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN,’’ Sci. Rep., vol. 12, no. 1, Sep. 2022, Art. no. 14987.

[15] A. K. Jaiswal and R. Srivastava, ‘‘Detection of copy-move forgery in digital image using multi-scale,multi-stage Deep Learningmodel,’’ Neural Process. Lett., vol. 54, no. 1, pp. 75–100, Aug. 2021.

[16] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq, and K. Kumar, ‘‘An efficient approach for copy-move image forgery detection using convolution neural network,’’ Multimedia Tools Appl., vol. 81, no. 8, pp. 11259–11277, Mar. 2022.

[17] S. S. Ali, I. I. Ganapathi, N.-S. Vu, S. D. Ali, N. Saxena, and N. Werghi, ‘‘Image forgery detection using Deep Learning by recompressing images,’’ Electronics, vol. 11, no. 3, p. 403, Jan. 2022.

[18] K. Kadam,S. Ahirrao, K. Kotecha, and S. Sahu, ‘‘Detection and localization of multiple image splicing using MobileNet v1,’’ IEEE Access, vol. 9, pp. 162499–162519, 2021.

[19] E. U. H.Qazi,T.Zia, and A. Almorjan, ‘‘Deep learning-based digital image forgery detection system,’’ Appl. Sci., vol. 12, no. 6, p. 2851, Mar. 2022.

[20] A.R.Gu, J.H. Nam, and S.-C. Lee, ‘‘FBI-Net: Frequency-based image forgery localization via multitask learning with self-attention,’’ IEEE Access, vol. 10, pp. 62751–62762, 2022.

[21] K. D. Kadam, S. Ahirrao, and K. Kotecha, ‘‘Efficient approach towards detection and identification of copy move and image splicing forgeries using mask R-CNN with MobileNet v1,’’ Comput. Intell. Neurosci., vol. 2022, pp. 1–21, Jan. 2022.

[22] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O’Neill, and B. Lee, ‘‘Lightweight deep learning model for detection of copymove image forgery with post-processed attacks,’’ in Proc. IEEE 19th World Symp. Appl. Mach. Intell. Informat. (SAMI), Jan. 2021, pp. 125–130.

[23] C. D. P. Kumar and S. S. Sundaram, ‘‘Metaheuristics with optimal deep transfer learning based

copy-move forgery detection technique,'' Intell. Autom. Soft Comput., vol. 35, no. 1, pp. 881–899, 2023.

[24] N.Krishnaraj, B. Sivakumar, R. Kuppusamy, Y. Teekaraman, and A. R. Thelkar, ''Design of automated Deep Learning - based fusion model for copy-move image forgery detection,'' Comput. Intell. Neurosci., vol. 2022, pp. 1–13, Jan. 2022.

[25] S Jabeen, U. G. Khan, R. Iqbal, M. Mukherjee, and J. Lloret, ''A deep multimodal system for provenance filtering with universal forgery detection and localization,'' Multimedia Tools Appl., vol. 80, no. 11, pp. 17025–17044, May 2021.

[26] D. Mallick, M. Shaikh, A. Gulhane, and T. Maktum, ''Copy move and splicing image forgery detection using CNN,'' in Proc. ITM Web Conf., vol. 44, 2022, Art. no. 03052.

[27] K.Simonyan and A.Zisserman, ''Very deep convolutional networks for large-scale image recognition,'' 2014, arXiv:1409.1556.

[28] T.H. Nguyen, T.-N. Nguyen, and B.-V. Ngo, ''A VGG-19 model with transfer learning and image segmentation for classification of tomato leaf disease,'' AgriEngineering, vol. 4, no. 4, pp. 871–887, Oct. 2022.

[29] K. He, X. Zhang, S. Ren, and J. Sun, ''Deep residual learning for image recognition,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770–778.

[30] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, ''Densely connected convolutional networks,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 2261–2269.

[31] F. Chollet, ''Xception: Deep learning with depthwise separable convolutions,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 1800–1807.

[32] R.Indraswaria, R. Rokhanab, and W. Herulambang, ''Melanoma image classification based on MobileNetV2 network,'' in Proc. 6th Inf. Syst. Int. Conf. (ISICO), 2022, pp. 198–207.

[33] J.Dong, W. Wang, and T. Tan, ''CASIA image tampering detection evaluation database,'' in Proc. IEEE China Summit Int. Conf. Signal Inf. Process., Jul. 2013, pp. 422–426.