OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
*Abbriviate Tittle- Ind J Multi Res*
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.12671607
INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

## Research Article

Volume-04|Issue-03|2024

# Enhancing Forgery Detection in Images through Advanced Machine Learning Techniques

**Nagabhushan M K[1], Anjan Kumar N[2], Monish N[3], Mahesh Kamath[4], Mrs. V. R. Srividhya*[5]**

[1,2,3,4]Student, Department of Computer Science and Engineering, RV Institute of Technology and Management, Visvesvaraya Technological University, Bengaluru, Karnataka, India.
[5]Assistant Professor, Department of Computer Science and Engineering, RV Institute of Technology and Management, Visvesvaraya Technological University, Bengaluru, Karnataka, India.

**Article History**
Received: 20.05.2024
Accepted: 05.06.2024
Published: 30.06.2024

**Citation**
Nagabhushan, M. K., Kumar, A. N., Monish, N., Kamath, M. & Srividhya, V. R. (2024). Enhancing Forgery Detection in Images through Advanced Machine Learning Techniques. *Indiana Journal of Multidisciplinary Research*, *4*(3), 91-97.

**Abstract:** In the present era of digital alteration or manipulation, the verification of original images has become challenging. This project presents an innovative approach to image forgery identification with the help of deep learning methods integrated with Error Level Analysis (ELA). We put forward a convolutional neural network (CNN) architecture designed especially to detect diverse kinds of image falsifications, especially copy-move, splicing, and retouching. CNN models demonstrate impressive performance, our system gives a sturdy evaluation framework. To enhance the precision, the integration of ELA allows for improving detection accuracy by highlighting regions of interest within the images. We check our methods using the standard datasets and illustrate their capability in accurately identifying manipulated areas with highest accuracy and retrieval rate. Our technique demonstrates superior performance based on experimental results estimated to existing approaches, highlighting its viability and indicating its latent ability for pragmatic application in forensic analysis and image verification.

**Keywords:** Pretrained models, Image Forgery Detection (IFD), Convolutional Neural Network, Deep Learning, Error Level Analysis.



## INTRODUCTION

The tampering of digital images that cannot be detected by the naked eye is called image forgery. These Forgeries are done by adding unusual patterns to the original image. Nowadays with the aid of assorted social networking platforms such as Facebook, Twitter, etc, these images are used to mislead and spread fake news in the context of society. Various software editing tools such as Pixlr, Adobe Photoshop GIMP, etc are used for tampering with the digital image. To detect such forgeries various techniques and algorithms are used especially when the original content is not available.

In the forged image we can find heterogeneous variation in the image property and unusual distribution of image features. This is due of the addition of unusual patterns to the original image. Fig 1 shows the approaches used in image forgery.

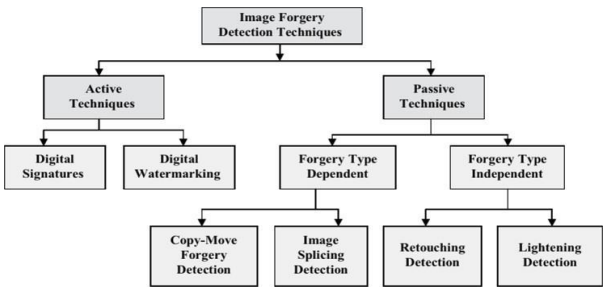


**Figure 1:** Digital Image Forgery Classification

Active approaches are the approaches utilized during the creation and distribution of an image with some intention of detecting and preventing future manipulation or forgery. This approach requires some essential information regarding the image for the verification process. This approach includes digital watermarking in which a unique signature is embedded into image data usually done during the acquisition or processing phase and digital signature in which additional information in the form of cryptographic code is embedded into the image. This is usually completed during the closure of the acquisition phase.

Passive image forgery approaches do not require any past information about the image. Tampering actions using this approach modifies the contents of information in pictures that can facilitate the forgery detection.

**Copy-move forgery** is the prevalent technique used to manipulate images, it is also the most complex forgery to uncover because of the complexity of copying and replicating an object or section of the image with identical properties and feature distributions and pasting it within the image itself. Additionally, some post-processing techniques like rotation, and JPEG compression can be done that make detection further difficult and complex.

***Corresponding Author:** Mrs. V. R. Srividhya

**Splicing Forgery** involves combining or blending of two images to get an unprecedented image. The source image may include dissimilar color, lighting, texture, and noise levels based on various factors. Filtering or some other image processing missions are done as post-processing steps to match visual attributes like the shape size and color of the target image so that the spliced image looks realistic. These include Retouching, cropping, resizing, etc.

**Retouching Forgery** involves the manipulation of images to hide or highlight certain features such as brightness, background, color, contrast, and other visual attributes. It aims at enhancing visual quality of the image.

**Resampling Forgery** involves altering dimensionality like size, orientation, and resolution of a particular object or section within the image to present misleading information. It includes actions such as scaling, rotating, or changing the aspect ratio of an image.

**Morphing Forgery** involves blending of two images to create a hybrid image that contains an entirely new scene, this can be done using the graphical software. These major types of tampering methods are Copy Move, Image Splicing, and Retouching Forgery.

Digital image forgery detection is a classification of images either as authentic or forged. So, it is a binary classification of images. Overall, the usage of deep learning can help to upgrade the precision and effectiveness of image forgery detection, which helps in forensic investigation.

## LITERATURE SURVEY

Syed Sadaf Ali's study, "Image Forgery Detection Using Recompressing Images," [1] The methods employed are customized to meet the unique requirements, passions, and inclinations of the user or community. To minimize the file size for fraud detection, image compression entails lowering a picture's pixels, size, or color components.

Sophisticated picture optimization methods are able to identify the more significant visual elements and eliminate the less significant ones.

Image Forgery Detection Using a Support Vector Machine (SVM) developed by J. Malathi [2] presents a technique that utilizes illuminant color inconsistency and machine learning methods like Support Vector Machine (SVM). SVM is a supervised classification algorithm used to differentiate between two seperate categories by delineating a boundary between them. In this approach, the illuminant color of visual input is estimated, and illuminant maps are produced for every individual image. Additionally, all faces in one image and corresponding faces in other individual images are extracted for examination. However, this technique may contain certain drawbacks, such as requiring clear textural and inclination highlights and potentially impacting the recognized content of the image.

It is imperative to note that there are many other forgery detection methods available that use different strategies, such as image forensics, watermarking, and deep learning-based methods. Each technique presents its own set of advantages and limitations, and the selection of an appropriate method depends on multiple factors such as the approach of forgery, the available data, and the desired level of accuracy.

F. Marra, in the work titled "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection" [6], introduces a CNN-based framework for identifying image forgery. The framework comprises a feature extraction module and a classification module, both employing CNNs, and processes full-resolution images. Real and forged images, encompassing different types of forgery approaches, are used to train and test the framework. The proposal also includes a data augmentation method to enhance the framework's robustness.

S. B. G. T. Babu and C. S. Rao, in their work "Statistical Features-based Optimized Technique for Copy Move Forgery Detection" [8], propose a novel stratergy for identifying copy move forgeries in digital visual data. This approach leverages statistical features to represent the image and uses an optimized iterative voting technique to detect forgeries. The proposed method is tested using various benchmark datasets, and the results demonstrate high accuracy in detecting copy-move forgeries.

M. H. Alkawaz, in the work "Digital Image Forgery Detection Based on the Expectation-Maximization Algorithm" [9], presents an approach for identifying digital image forgeries using the expectation-maximization (EM) algorithm. This approach models the likelihood distribution of the forgery and original image, utilizing it to estimate distribution parameters and detect forgery.

S. al-Zahir and R. Hammad, in their work "Image Forgery Detection Using Image Similarity" [10], propose an approach that assesses the similarities between different regions of an image and utilizes a clustering algorithm to identify forged areas. The proposed method is tested on multiple benchmark datasets, and the results demonstrate high accuracy in detecting image forgeries.

H. Chen, X. Yang, and Y. Lyu, in their work "Copy-move forgery detection based on keypoint clustering and a similar neighborhood search algorithm" [12], present an algorithm that employs a clustering

***Corresponding Author:** Mrs. V. R. Srividhya

technique to group similar key points based on scale and color, then matches them to identify tampered regions. To precisely locate the tampered regions, a novel localization algorithm compares the close neighborhoods of matching pairs using two similarity measures and iteratively marks tampered regions in the image pixels. This algorithm appears to be designed to identify tampered areas in images with high accuracy and efficiency.

**Proposed Approach**

Digital image forgery detection with the help of deep learning incorporates ELA (Error Level Analysis) for identifying forged images. This process involves scaling, which entails compressing the image to low quality, re- saving it at higher quality, and then comparing the difference in pixel values between the two image versions. The resulting ELA image illuminates areas that have undergone manipulation or editing.

Convolutional Neural Network (CNN) is a often used method for detecting forged images due to its capacity to learn patterns and attributes from the training dataset (authentic and forged). Once trained, CNN can classify images as either manipulated or real.

To implement the forgery detection of image using ELA, the following steps can be followed:

1. Convert the input image into an ELA image during the pre-processing phase. This is achieved by:

$$Fdiff = F - Fcomp \quad (1)$$

Here, F represents the forged image, which is compressed to produce a compressed version, denoted by Fcomp. The difference between the forged image and its compressed version, denoted by Fdiff, is calculated using mathematical subtraction.

2. Pre-process the ELA image and prepare it for input into the pre-trained CNN model, which classifies the image as either authentic or forget. If the image is categorized as forged, further analysis is required to which type of forgery used. While ELA is useful for detecting tampered or forged images and highlighting manipulated areas, it is not foolproof and may result in false positives or negatives. Thus, combining ELA with other techniques and methods leads to a more accurate and robust detection system.

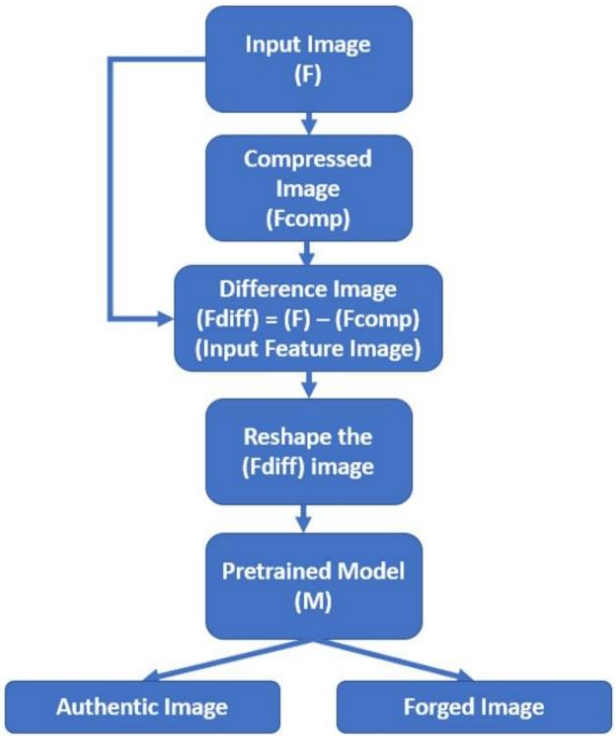


**Figure 2:** Flowchart of proposed system

**System Architecture**

The proposed system architecture for image forgery detection have several steps, starting with preparing the dataset. The open image dataset's annotations are transformed into a format accessible for model training. The testing phase involves converting the image to ELA image format, computing the noise-to-signal ratio, denoising the image, and transforming it to grayscale.

The model is divided into two datasets with the help of train/test method, allocating 80% for training and 20% for testing. The CNN model is applied to high-risk regions of the image for forgeries. A confusion matrix summarizes the performance of the classification algorithm. A table plots all predicted and actual classifier

***Corresponding Author:** Mrs. V. R. Srividhya

values, and a confidence score is calculated as an evaluation standard.

The confidence score measures the likelihood of correct image detection by the algorithm, expressed as a percentage. If the confidence score falls below the required threshold (e.g., 0.9), decisions may be deferred. Limiting predictions can substantially enhance model accuracy. Each label is assigned a numerical value called Confidence, while Predict evaluates an Issue.

Overall, the proposed system architecture offers a robust approach to detecting image fraud, incorporating multiple steps to prepare and validate the model's accuracy. The utilization of a confusion matrix technique and confidence scores provides an additional layer of assessment, verifying the reliability of the algorithm's predictions before making any decisions.

**Convolutional Neural Network**

Convolutional Neural Networks (CNNs) have become a favored tool for detecting forged images. CNNs are basically deep learning algorithms that can be trained to extract image features and classify them into distinct categories. Drawing inspiration from the human visual system, they are composed of different interconnected layers that perform convolution methods on input images to capture features.

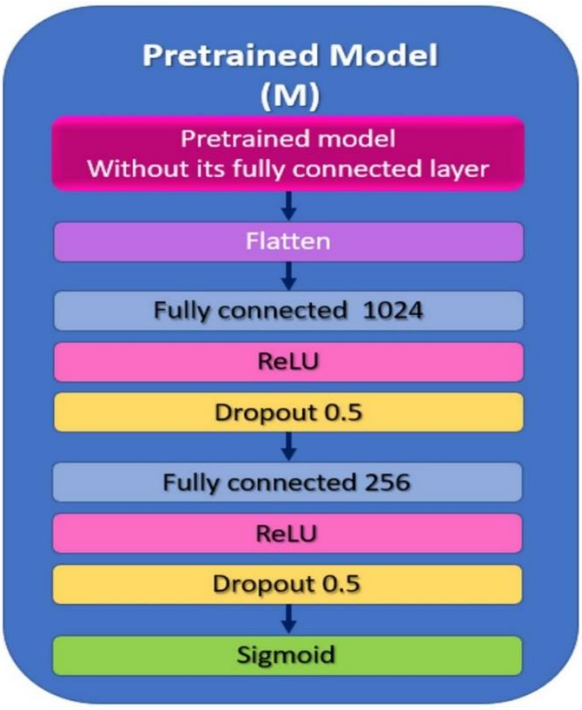


**Figure 3:** Detailed view of layers of the pre-trained CNN model

A key advantage of utilizing CNNs for image forensics is their ability to identify subtle artifacts undetectable to the naked eye. For instance, when an image is manipulated, such as through copy-pasting fragments from one image to another, slight variations in pixel values or textures can indicate manipulation. CNNs are trained to discern these differences and classify the picture as either authentic or fake.

CNNs have shown notable promise in a range of computer vision and image processing applications, including image forensics. With growing prevalence of digital manipulation, the ability to detect forged images has become increasingly important, and CNNs provide a powerful tool and methods for this purpose.

The input layer of a convolutional neural network (CNN), receives images from the dataset. These images are typically structured as 3-dimensional arrays, with the first two dimensions representing the height and width (pixel count), and the third dimension representing the red, green, and blue (RGB) colors within each pixel.

In the feature-extraction stage of the CNN architecture, the input image goes through a series of convolutional layers where, a set of learnable filters are used to extract image features. Each filter generates a feature map that highlights a distinct pattern or feature within the input image. These feature maps are then sent through activation functions like ReLU to introduce non-linearity and prevent the vanishing gradient problem.

Following the feature extraction phase, the output from the final convolutional layer is flattened into a 1-dimensional vector and passed through a array of fully connected layers which is utilized for classification. These fully connected layers use the extracted features to foretell the class of the input image. The final output layer generally uses the function called as softmax to generate a probability distribution across classes, indicating the most likely class for the input image.

**Convolutional layer:** This layer applies filters to the input image or feature map, generating output feature maps. Each filter detects a specific pattern or feature in the input, and the output feature maps highlight areas where these characteristics are found. Stacking multiple convolutional layers enables the network to grasp more intricate and abstract features.

**Pooling layer:** This layer reduces both the spatial size and number of parameters count within the output feature maps derived from the convolutional layer. The most common form of pooling is max pooling, which selects the maximum value in a tiny region of the feature map. This method helps capture the important features while minimizing redundant information and improves the network's robustness to variations in input position and scale.

**Fully-connected layer:** In this layer, the flattened outcome of the previous layer and a group of weights are applied to create a vector of class probabilities. These weights are learned during training through backpropagation and gradient descent. The softmax activation function ensures the output probabilities sum

***Corresponding Author:** Mrs. V. R. Srividhya

to 1, enabling the network to make a single prediction for the input image. The count of neurons in the fully connected layer matches the count of output classes.

## SYSTEM METHODOLOGY

The identification of fake images is done by using convolutional neural networks (CNNs). CNNs facilitate the identification of tampered images and emphasize improving the precision of detecting such altered images.

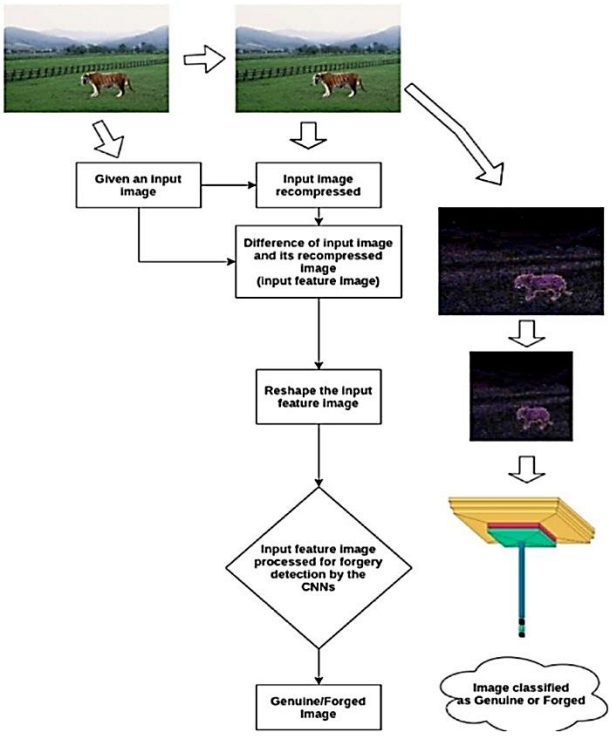


**Figure 4:** System Architecture

**Image Processing:** The obtained image goes through several steps, including ELA conversion, grayscale conversion, thresholding, and confidence calculation.

Error Level Analysis (ELA) is one of a method used to detect modified areas within an image. This method generates a difference map by compressing and decompressing the image using a low-quality JPEG algorithm. Altered areas of the image will display varying compression rates and manifest as bright spots on the difference map.

Grayscale conversion is commonly used to simplify the image and minimize its complexity. This process converts the image to a black-and-white or grayscale format, with each pixel's value representing its intensity.

Thresholding is a technique that converts the grayscale image into a binary image, making each pixel either black or white. This process aids in removing image noise and can improve the precision of the detection algorithm.

Confidence: A confidence score spans from 0 to 1 and can be evaluated for each input, reflecting the algorithm's certainty in its classification for that class.

**SYSTEM IMPLEMENTATION**

**Software and Hardware**

- The system requirements for running an image fraud detection system using a CNN model implemented in Python
- 3.7.X (IDLE) and the CASIA dataset. It is recommended that the computer system has at least:
- RAM: 8GB or more
- Hard Disk Drive (HDD): 80GB or more
- Processor: i5 or higher

***Dataset***

The CASIA v2.0 database contains 10,000 images, split evenly into a training set of 5,000 images and a testing set of 5,000 images. These subsets include images from eight categories: article, architecture, character, nature, plant, animal, scene, and texture. The images are generally stored in JPEG format and have dimensions of either 256 x 384 or 384 x 256 pixels. The majorly used dataset for image forgery detection is CASIA v2.0.

Table 1. CASIA.2.0 Image Forgery Database Specification

| | Authentic | Forged | | Total | Size | Format |
|---|---|---|---|---|---|---|
| | | Copy-move | Splicing | | | |
| Number of images | 7491 | 3274 | 1849 | 12614 | 320x240 900x600 | BMP, JPEG, TIFF |
| Total | 7491 | 5123 | | 12614 | | |

**Table 2.** Details Division of CASIA-V2 Dataset in the Experiments

| | Authentic | Forged | Total |
|---|---|---|---|
| CASIA-V2 | 7491 | 5123 | 12614 |
| Training Set 80% | 5993 | 4098 | 10091 |
| Testing Set 20% | 1498 | 1025 | 2523 |

The dataset consists of two classes: actual photos and tampering detection. A total of 7,354 images are classified into real images and altered images, all in JPG format. Tampered images in CASIA v2 were generated by blending two different authentic images or modifying the same authentic image. The modified sections underwent processes such as distortion, rotation, and scaling to produce a realistic appearance, including blurring the edges of the spliced regions.

***Confusion Matrix:***

A confusion matrix is a table frequently used to appraise a classification algorithm's performance by analysing its predicted labels with the original labels from a test dataset. The matrix shows the number of true positives, false positives, true negatives, and false negatives generated by the algorithm.

***Corresponding Author:** Mrs. V. R. Srividhya

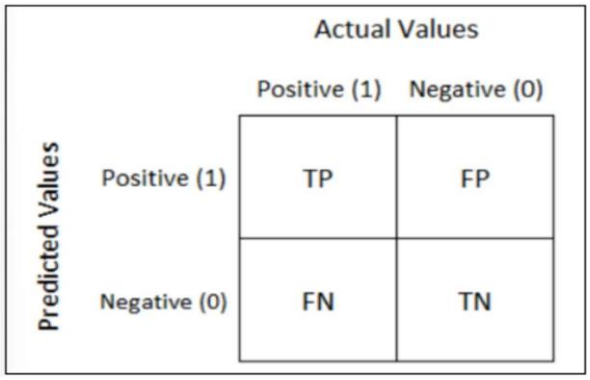


**Figure 5:** Confusion Matrix

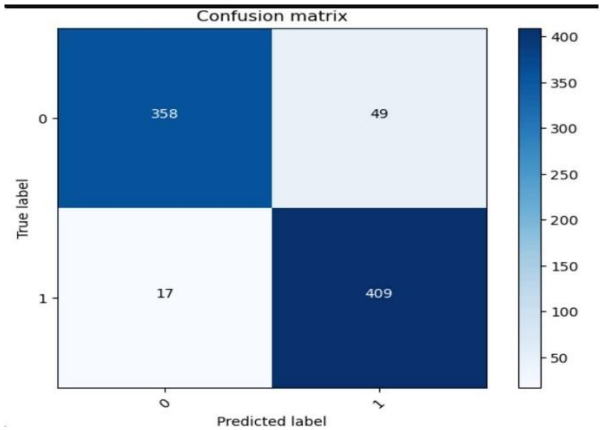


**Figure 6:** Confusion Matrix of Proposed Model

A confusion matrix is a table used to appraise the effectiveness of a classification model on a test dataset withknown true class labels.

## RESULT AND DISCUSSION

The outcome of the proposed model is assessed using several metrics:

**Accuracy:** Accuracy measures the proportion of correctly classified instances from both classes out of the totalinstances in the dataset. It is calculated using the formula. (2)

Accuracy = [(TP + TN) / (TP + FN + FP + TN)] × 100

**Recall:** Recall indicates the percentage of tampered images that were correctly identified out of the total number ofactually tampered images. The formula for recall is: (3)

Recall = TP / (TP + FN)

**Precision:** Precision measures the proportion of images identified as forged that are truly forged. The formula is: (4)

Precision = TP / (TP + FP)

**F1 score:** The F1 score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance. It is calculated using the formula:

F1 score = [(2 × Recall × Precision) / (Recall + Precision)] × 100

| | |
|---|---|
| Accuracy: | 0.92 |
| Precision: | 0.89 |
| Recall: | 0.92 |
| F-Measure: | 0.92 |

**Figure 7:** Performance of Proposed Model

The performance metrics of the proposed system is shown in Figure 7. The model's testing and validation accuracy and is represented in the Figure 8. Figure 9 represents the model loss in the proposed system.


**Figure 8:** Testing and validation accuracy of the model

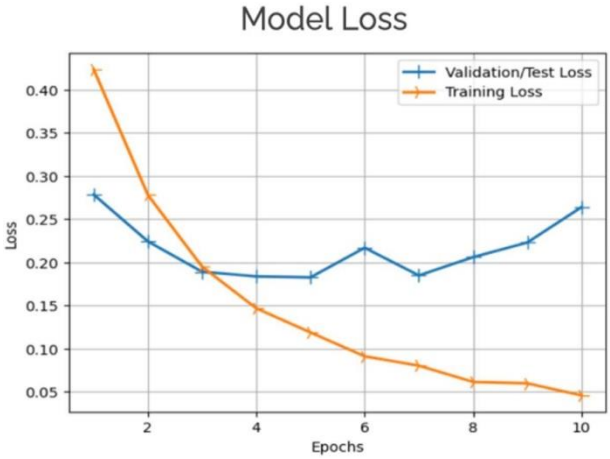


**Figure 9:** Model Loss in the proposed system

## CONCLUSION

The image forgery detection system with the help of deep learning methods is implemented with the CASIAv2.0 dataset. Original images are transformed into black-and-white grayscale images by the ELA technique. By combining the Convolutional Neural

***Corresponding Author:** Mrs. V. R. Srividhya

Network (CNN) architecture with Error Level Analysis (ELA), the project demonstrates a sturdy system that effectively detects digital image forgeries with high accuracy. The synergy of both methods ensures adaptability and reliability in various forgery detection scenarios. The proliferation of digital image editing technique necessitates the urgency for reliable techniques of dependable techniques to detect image forgeries.

This paper utilizes Python and a Convolutional Neural Network (CNN) model architecture to introduce an innovative approach to image forgery detection. The core element of our system, the CNN model, exhibits remarkable performance with a training accuracy of 98% and a validation accuracy of 92%, effectively distinguishing between manipulated and genuine photos. The study's dataset consists of 12,615 images, split into 7,492 genuine and 5,123 manipulated images, providing a comprehensive and varied testing environment. As part of preprocessing, Error Level Analysis (ELA) is applied to enhance the accuracy of our method.

After resizing each image to a consistent 256x256 resolution, Error Level Analysis (ELA) is applied to detect regions with varying levels of compression within the image. An intact image should exhibit uniform compression throughout, while any inconsistency might indicate manipulation. Processed images are stored as NumPy arrays for subsequent analysis. Our proposed solution leverages the combined strengths of deep learning through CNNs and the detailed insights provided by ELA. This synergy allows the model to achieve high accuracy and deliver information on specific areas of an image pixels that may have been tampered with.

## REFERENCES


1. 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.
2. Malathi, J., Swamy, B. N., & Musunuri, R. (2019). Image forgery detection by using machine learning. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(6S4), 561-563.
3. Matern, F., Riess, C., & Stamminger, M. (2019). Gradient-based illumination description for image forgery detection. *IEEE Transactions on Information Forensics and Security*, *15*, 1303-1317. doi:10.1109/TIFS.2019.2935913.
4. Barad, Z. J., & Goswami, M. M. (2020, March). Image forgery detection using deep learning: a survey. In *2020 6th international conference on advanced computing and communication systems (ICACCS)* (pp. 571-576). IEEE. doi:10.1109/ICACCS48705.2020.9074408.
5. Singh, A., & Singh, J. (2021, August). Image forgery detection using deep neural network. In *2021 8th International conference on signal processing and integrated networks (SPIN)* (pp. 504-509). IEEE. DOI:10.1109SPIN525336.2021.9565953.
6. Marra, F., Gragnaniello, D., Verdoliva, L., & Poggi, G. (2020). A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection. *IEEE Access*, *8*, 133488-133502. doi:10.1109/ACCESS.2020.3009877.
7. Agarwal, R., Khudaniya, D., Gupta, A., & Grover, K. (2020, May). Image forgery detection and deep learning techniques: A review. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1096-1100). IEEE. doi:10.1109/ICICCS48265.2020.9121083.
8. Babu, S. T., & Rao, C. S. (2020, July). Statistical features based optimized technique for copy move forgery detection. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE. doi:10.1109/ICCCNT49239.2020.9225426.
9. Alkawaz, M. H., Veeran, M. T., & Bachok, R. (2020, February). Digital image forgery detection based on expectation maximization algorithm. In *2020 16th IEEE international colloquium on signal processing & its applications (CSPA)* (pp. 102-105). IEEE. doi:10.1109/CSPA48992.2020.9068731.
10. alZahir, S., & Hammad, R. (2020). Image forgery detection using image similarity. *Multimedia Tools and Applications*, *79*(39), 28643-28659.
11. Hosny, K. M., Mortda, A. M., Fouda, M. M., & Lashin, N. A. (2022). An efficient cnn model to detect copy-move image forgery. *IEEE Access*, *10*, 48622-48632. doi:10.1109/ACCESS.2022.3172273.
12. Chen, H., Yang, X., & Lyu, Y. (2020). Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm. *IEEE Access*, *8*, 36863-36875. doi:10.1109/ACCESS.2020.2974804


***Corresponding Author:** Mrs. V. R. Srividhya