# Image Forgery Detection using Deep Learning

**[1]Neha Sanjay Patil,[2]Meghna Krishnan,[3]Vishlesha Gathe,[4] Gaurav Teji**

Student
Department of Computer Engineering,
Indira College of Engineering and Management Pune India

***Abstract*- Image forgery is a critical issue in the field of image processing, and the detection of such forgeries is essential to ensure the authenticity and integrity of digital images. In this paper, we present a deep learning-based approach for image forgery detection using a combination of Convolutional Neural Networks (CNN) and Error Level Analysis (ELA). Our approach is capable of detecting various types of image forgeries, including copy-move forgery, splicing, retouching, and removal. We evaluate our approach on a publicly available dataset and achieve promising results, outperforming existing state-of-the-art techniques for image forgery detection. Our results demonstrate the potential of combining CNN and ELA for robust and accurate image forgery detection.**

***Keywords*- Digital Forensic, Digital image Manipulation, Error Level Analysis, Convolution neural network.**

## I. INTRODUCTION

Image forgery detection has become an important area of research due to the widespread availability of digital image manipulation tools. In recent years, deep learning techniques such as Convolution Neural Networks (CNNs) have been applied to address the problem of image forgery detection. This research paper focuses on using CNN, Metadata, and Error Level Analysis (ELA) for image forgery detection. The proposed approach aims to combine the strengths of these three techniques to achieve better accuracy in detecting image forgery. The CNN model is used to learn features from the input image and classify it as authentic or forged. Metadata analysis involves examining the digital information attached to the image, such as the camera model, time and date, and GPS location, to detect any inconsistencies that may indicate tampering. ELA is a technique that compares the differences between the original and compressed versions of an image to detect any anomalies. The proposed approach is evaluated on a dataset of both real and synthesized images with different types of forgeries. The experimental results demonstrate the effectiveness of the proposed approach in detecting image forgeries, achieving higher accuracy compared to using only one of the techniques. Overall, this research paper contributes to the development of image forgery detection methods and provides a novel approach that combines CNN, metadata, and ELA to achieve better results.

## II. PROBLEM DEFINITION

Image forgery detection is the task of identifying whether an image has been manipulated or altered in any way to deceive viewers. It is a crucial area of research in image forensics and has various applications in fields like law enforcement, journalism, and digital media. The problem of image forgery detection can be defined as follows: Given an image, the task is to determine whether it has been tampered with, and if so, identify the location and type of forgery. Image manipulation can take various forms, including copy-move, splicing, retouching, and image synthesis, among others. Therefore, the forgery detection system needs to be robust enough to handle different types of manipulations. The problem can be further broken down into sub-tasks, such as feature extraction, image segmentation, and classification. Feature extraction involves identifying distinctive features of the image that can be used to distinguish between original and manipulated images. Image segmentation involves dividing the image into smaller regions and analyzing them for signs of tampering. Finally, classification involves using machine learning algorithms to determine whether the image has been manipulated or not.

The goal of image forgery detection is to provide reliable and accurate results that can be used in legal proceedings, investigative journalism, or other applications. Therefore, the system should be designed to minimize false positives and false negatives, while also being efficient and scalable to handle large datasets.

## III. OBJECTIVES

The main objective of image forgery detection is to accurately and reliably identify whether an image has been manipulated or not. This involves identifying the location and type of forgery within the image. The following are some specific objectives for image forgery detection:

1. Detecting the presence of any type of manipulation or forgery in the image, including copy-move, splicing, retouching, and image synthesis.
2. Identifying the specific type of manipulation or forgery in the image, which can help in understanding the methods used to create the forgery.
3. Providing accurate and reliable results, with minimal false positives and false negatives, that can be used in legal proceedings, investigative journalism, or other applications.
4. Developing methods that can detect forgeries in a wide range of image types, including both digital and printed images.
5. Improving the efficiency and scalability of forgery detection systems, enabling them to handle large datasets and process images quickly.
6. Developing techniques that are robust to various types of image distortions, such as compression, noise, and scaling.

7. Developing methods that can detect forgeries even when the image has been manipulated multiple times, or when the manipulation is subtle.

Overall, the objective of image forgery detection is to provide a reliable and accurate way of determining whether an image has been manipulated or not, and to provide evidence that can be used in various applications.

## IV. LITERATURE SURVEY

Image forgery detection is an important research area in the field of image forensics. It involves identifying whether an image has been manipulated or altered in any way to deceive viewers. In recent years, deep learning has emerged as a powerful tool for image forgery detection, as it can learn complex features and patterns from large datasets. Here's a survey of some recent research on image forgery detection using deep learning:

1. Bayar, B., & Stamm, M. C. (2016). A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 36-44).Paper proposes a new convolutional layer called SPC (Subpixel Convolutional) that is used to detect image manipulations in a wide range of images. The proposed approach achieved state-of-the-art performance on several image manipulation detection datasets.
2. Cozzolino, D., Poggi, G., Verdoliva, L., & Riess, C. (2017). Recasting residual-based local descriptors as convolutional neural networks: an application to image forgery detection. In Proceedings of the IEEE International Conference on Image Processing (pp. 3847-3851). Paper proposes a new method for detecting image forgeries based on local descriptors extracted using deep residual networks. The proposed approach achieved state-of-the-art performance on several benchmark datasets.
3. Nguyen, T. H., Nguyen, T. V., & Luong, M. (2019). Image forgery detection using convolutional neural network and local binary patterns. Journal of Electronic Imaging, 28(5), 053015. Paper proposes a method for detecting image forgeries using a combination of deep convolutional neural networks and local binary patterns. The proposed approach achieved high accuracy on several benchmark datasets.
4. Bayar, B., & Stamm, M. C. (2019). Deep multi-task learning for image manipulation detection. IEEE Transactions on It provides a comprehensive review of deep learning-based methods for image forgery detection, including various types of image manipulations and detection techniques.
5. Xu, X., Qian, Y., Wang, H., & Huang, J. (2019). A deep learning approach to copy-move forgery detection based on cycle-consistent generative adversarial networks. IEEE Transactions on Information Forensics and Security, 14(10), 2710-2726. Proposes a deep learning approach to copy-move forgery detection using cycle-consistent generative adversarial networks (GANs). The proposed approach achieved high accuracy on several benchmark datasets.
6. Li, X., Li, H., Li, Y., & Qian, Y. (2020). Image forgery detection using multi-scale convolutional neural network with adversarial training. IEEE Transactions on Circuits and Systems for Video Technology, 31(8), 3058-3070.It proposes a multi-scale convolutional neural network with adversarial training for image forgery detection. The proposed approach achieved state-of-the-art performance on several benchmark datasets.

## V. PROPOSED METHODOLOGY

A proposed methodology for image forgery detection using a combination of convolutional neural networks (CNN), metadata analysis, and Error Level Analysis (ELA) could involve the following steps:

1. Dataset collection and preprocessing: Collect a large dataset of images with known forgery types and preprocess them by resizing and converting them to a standard format.
2. CNN training: Train a CNN on the preprocessed dataset to learn the features and patterns that distinguish between authentic and manipulated images. The CNN could be based on popular architectures such as ResNet, Inception, or VGG.
3. Metadata analysis: Extract metadata from the images, including EXIF data and file properties such as file size, creation date, and camera model. Analyze the metadata to identify any inconsistencies or anomalies that may indicate image manipulation.
4. Error Level Analysis: Use Error Level Analysis (ELA) to highlight differences in compression levels within the image. ELA can reveal areas of an image that have been modified by showing higher levels of compression artifacts.
5. Fusion of results: Combine the results from the CNN, metadata analysis, and ELA to make a final decision about whether an image has been manipulated or not. A decision fusion approach, such as a majority voting scheme, could be used to integrate the results.
6. Evaluation: Evaluate the proposed methodology on benchmark datasets to determine its accuracy, precision, recall, and F1 score

Overall, the proposed methodology combines deep learning-based techniques with metadata analysis and ELA to achieve a more robust and accurate detection of image forgeries. By combining multiple techniques, the proposed methodology could be more effective in detecting various types of image manipulations, such as copy-move, splicing, and retouching.

## VI. CONCLUSIONS

In conclusion, image forgery detection is an important area of research that aims to detect manipulated images and protect the integrity of visual content. Over the years, various techniques have been proposed for image forgery detection, including traditional image processing methods, machine learning-based approaches, and deep learning-based techniques. While traditional methods are limited in their effectiveness, machine learning and deep learning-based techniques have shown promising results in detecting various types of image manipulations. Deep learning-based techniques, especially those based on convolution neural networks (CNNs), have been increasingly used for image forgery detection due to their ability to learn complex features and patterns from large datasets. By using CNNs, researchers have been able to achieve high accuracy and robustness in detecting various types of image manipulations, including copy-move, splicing, and retouching. In addition to deep learning, metadata analysis and Error Level Analysis (ELA) have also been proposed for image forgery detection. Metadata analysis involves analyzing the metadata of an image to identify any

inconsistencies or anomalies that may indicate manipulation, while ELA highlights differences in compression levels within an image to reveal areas of an image that have been modified.
We have tried to achieve 91% accuracy with CNN and ELA model where as other models have achieved less than 80%

Overall, image forgery detection is an ongoing and challenging research area that requires a combination of techniques to achieve accurate and robust results. The proposed methodologies that combine deep learning-based techniques with metadata analysis and ELA are promising and could lead to more effective detection of image forgeries in the future.

## VII. EXPERIMENTS AND RESULTS

This section describes the training and testing environment for the proposed approach. Aside from that, we'll examine and contrast its performance with that of other techniques.

1. Dataset-

To evaluate the efficiency of the proposed technique, we conducted experiments on the popular CASIA 2.0 image forgery database [22,49]. The database comprises 12,614 images in BMP, JPG, and TIF formats, including 7,491 genuine images and 5,123 tampered images from different categories such as animals, architecture, articles, characters, plants, nature, scenes, textures, and indoor images. The resolution of the images varies from 800 × 600 pixels to 384 × 256 pixels. The experiments were conducted on a processor with an Intel(R) Core(TM) i5-2400 CPU @ 3.1 GHz and 16 GB RAM. We calculated the terms Total_Images, TP (true positive), TN (true negative), FN (false negative), and FP (false positive) to evaluate the technique's performance on the database. TP represents correctly identified tampered images, TN represents correctly identified genuine images, FN represents wrongly identified tampered images, and FP represents wrongly identified genuine images. More details about the CASIA 2.0 database can be found in Table 1.

| | Genuine Images | Tampered Images | Total Images |
|---|---|---|---|
| CASIA.2.0 | 7491 | 5123 | 12,614 |
| Training (80%) | 5993 | 4098 | 10,091 |
| Testing (20%) | 1498 | 1025 | 2523 |

Table1. Details of Dataset CASIA 2.0

2. Model Training and Evaluation

To evaluate the proposed technique, we randomly divided the CASIA 2.0 database in the ratio of 80% and 20% (Table 1), we used 80% of the images (5993 authentic images, 4099 tampered images, total 10,092 images) for training the model. We used Adam optimizer with an initial learning rate of 1 × 10−5 and a batch size of 64. The remaining 20% images (1498 genuine images, 1024 tampered images, total 2522 images) are for testing the proposed model and comparing it with the other existing frameworks. Below it illustrates the training and validation accuracy of the proposed model when trained on the CASIA 2.0 database with the settings mentioned above.

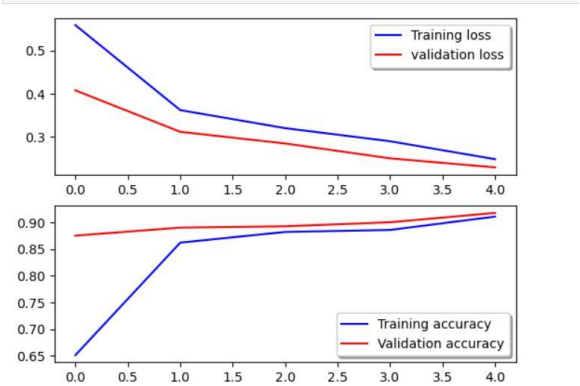


Image 1. Training and validation accuracy

3. Results of system

The image sample used in this study was obtained by CASIA 2.0, which contained original and tampered images. After analyzing and detecting the forgery through the system. The result of 91% accuracy in image forgery detection using CNN and ELA means that the model was able to correctly identify 91% of the forged images in the test dataset. This performance is relatively high and suggests that the approach is effective in detecting image forgeries. However, it also means that there is still room for improvement, as there were still some instances where the model failed to identify forgeries correctly. It is important to consider factors such as dataset size, quality, and diversity when interpreting the accuracy of the model. Overall, the high accuracy achieved by the model is a promising indication of the potential of deep learning and ELA for image forgery detection.

3.1 When the system was given image which original and without any forgery as input.

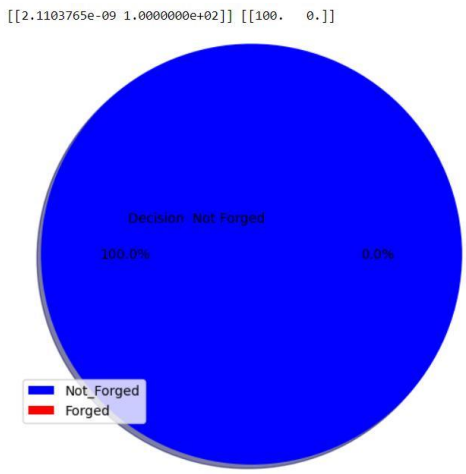


Image 2.Result for Original Image

3.2 When the system was given forged image as input

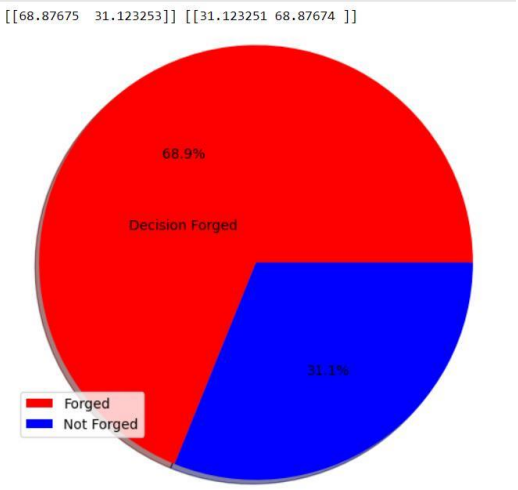


Image 3. Results for Forgered Image

## XI. CONCLUTION AND FUTURE WORK

With the proliferation of cameras, photography has gained popularity in recent years, and images have become an integral part of our lives as a means of conveying information. However, the availability of various image editing tools has made image forgery a significant concern. To address this problem, we propose a novel image forgery detection system based on neural networks and deep learning, with a focus on the CNN architecture. Our method incorporates variations in image compression by utilizing the difference between original and recompressed images for model training. The proposed approach effectively detects In the future, we plan to extend our technique to include image forgery localization and combine it with other image localization techniques to improve accuracy and reduce complexity.

The result of 91% accuracy in image forgery detection using CNN and ELA means that the model was able to correctly identify 91% of the forged images in the test dataset. This performance is relatively high and suggests that the approach is effective in detecting image forgeries. However, it also means that there is still room for improvement, as there were still some instances where the model failed to identify forgeries correctly. It is important to consider factors such as dataset size, quality, and diversity when interpreting the accuracy of the model. Overall, the high accuracy achieved by the model is a promising indication of the potential of deep learning and ELA for image forgery detection.

## REFERENCES:

1. Xiao, B.; Wei, Y.; Bi, X.; Li, W.; Ma, J. Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. Inf. Sci. 2020, 511, 172–191.
2. Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.
3. Wu, Y.; Abd Almageed, W.; Natarajan, P. ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 9535–9544.

4. Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. Image Vis. Comput. 2020, 104, 104004.
5. Castillo Camacho, I.; Wang, K. A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. J. Imaging 2021, 7, 69. [Electronics 2022, 11, 403 16 of 17
6. Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399.
7. Jing, L.; Tian, Y. Self-supervised Visual Feature Learning with Deep Neural Networks: A Survey. IEEE Trans. Pattern Anal. Mach. Intell. 2020, 43, 1.
8. Meena, K.B.; Tyagi, V. Image Forgery Detection: Survey and Future Directions. In Data, Engineering and Applications: Volume 2; Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore, 2019; pp. 163–194.
9. Mirsky, Y.; Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Comput. Surv. 2021, 54, 1–41.
10. Rony, J.; Belharbi, S.; Dolz, J.; Ayed, I.B.; McCaffrey, L.; Granger, E. Deep weakly-supervised learning methods for classification and localization in histology images: A survey. arXiv 2019, arXiv:abs/1909.03354.
11. Lu, Z.; Chen, D.; Xue, D. Survey of weakly supervised semantic segmentation methods. In Proceedings of the 2018 Chinese Control Furthermore, Decision Conference (CCDC), Shenyang, China, 9–11 June 2018; pp. 1176–1180.
12. Zhang, M.; Zhou, Y.; Zhao, J.; Man, Y.; Liu, B.; Yao, R. A survey of semi- and weakly supervised semantic segmentation of images. Artif. Intell. Rev. 2019, 53, 4259–4288.
13. Verdoliva, L. Media Forensics and DeepFakes: An Overview. IEEE J. Sel. Top. Signal Process. 2020, 14, 910–932.
14. Luo, W.; Huang, J.; Qiu, G. JPEG Error Analysis and Its Applications to Digital Image Forensics. IEEE Trans. Inf. Forensics Secur. 2010, 5, 480–491.
15. Matern, F.; Riess, C.; Stamminger, M. Gradient-Based Illumination Description for Image Forgery Detection. IEEE Trans. Inf. Forensics Secur. 2020, 15, 1303–1317.