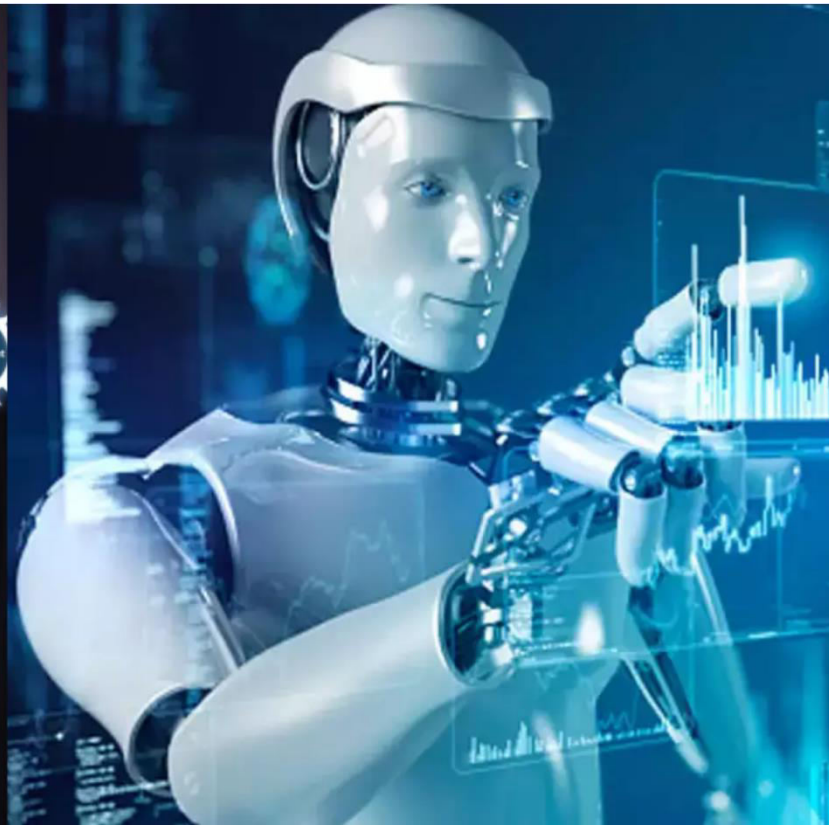
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

AI-Powered Image Forgery Detection using CNN

Janardhana Rao Alapati, Swapna Sri Malineni, Nagendra Nagidi, Venkata Sampath Kodati, Tarun Jasti

Assistant Professor, Department of Computer Science and Engineering (AI & ML), Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Research Scholar, Department of Computer Science and Engineering (AI & ML), Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Research Scholar, Department of Computer Science and Engineering (AI & ML), Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Research Scholar, Department of Computer Science and Engineering (AI & ML), Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Research Scholar, Department of Computer Science and Engineering (AI & ML), Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

ABSTRACT: In today's digital landscape, images play a crucial role in sharing information across social media platforms. However, this widespread use has led to a significant challenge—advanced software capable of generating manipulated images to spread misinformation. To address this issue, prior research has examined various techniques for detecting digital image forgery. Nonetheless, many existing approaches focus on identifying only specific types of forgery, such as image splicing or copy-move, which may not effectively capture the complexity of real-world scenarios.

This study presents an innovative method to enhance digital image forgery detection by utilizing deep learning through transfer learning. The objective is to identify two different categories of image forgery simultaneously. Ensuring the authenticity of digital images is essential for forensic analysis, media integrity, and cybersecurity. This paper introduces a Convolutional Neural Network (CNN)-based model combined with Error Level Analysis (ELA) to classify images as genuine or tampered. The model is trained on a dataset containing both manipulated and authentic images, achieving high accuracy in detecting forgeries. Additionally, this paper explores the dataset, preprocessing steps, model design, experimental findings, and potential future enhancements.

KEYWORDS: Image Forgery Detection, Deep Learning, Convolutional Neural Networks, Error Level Analysis, Fake Image Detection

I. INTRODUCTION

Since the emergence of photography, individuals and organizations have continuously sought ways to alter images to mislead viewers. In the past, such modifications required extensive expertise and long hours of work by skilled technicians. However, with the rise of digital photography, editing images has become effortless and widely accessible, allowing anyone to create professional-looking alterations with minimal effort. As a result, this accessibility has led to social concerns, including the credibility of images in the media and the digital enhancement of models' appearances to conform to certain beauty standards. The increasing number of available image manipulation techniques has growing interest in image forgery detection, both in academic research and professional settings.

An algorithm with a high accuracy rate may also produce a significant number of false positives. Additionally, while execution time plays a crucial role in determining an algorithm’s efficiency and usability, discussions on this aspect are often limited to academic settings rather than real-world applications. To simplify this complex process, algorithms will be classified into five key categories: JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

Detection, and Light & Color Anomaly Detection. Each category will be explored in-depth, evaluating the overall effectiveness of the respective algorithms. If a method is found to be reliable, an algorithm from that category will be implemented. These classifications are based on the fundamentally different detection techniques they utilize, ensuring a diverse range of results depending on the type of image manipulation.

Additionally, variations of each algorithm will be tested, as different parameter settings can significantly influence their performance. In this research, we present a deep learning-based approach that incorporates Error Level Analysis (ELA) with CNN architectures to identify various forgery techniques, including copy-move and splicing. Our model is designed to work with diverse datasets and is deployed through a Flask-based web application, facilitating real-world usability.

Furthermore, the impact of image forgery extends beyond social media, affecting journalism, legal proceedings, and financial transactions, where altered images and documents can be exploited for fraudulent activities. In response to this growing challenge, our study aims to develop a scalable, automated, and robust solution to enhance the credibility of digital images.

II. LITERATURE REVIEW

The advancements in deep learning (DL) over the past decades have established it as a leading technology across multiple fields. In digital image forensics, a growing number of studies focus on utilizing DL-based methods to detect and analyze manipulated regions within images. This comprehensive review categorizes and evaluates cutting-edge DL-based techniques for image forgery detection, considering factors such as document type, forgery category, detection approach, validation datasets, assessment metrics, and performance results.

Deep learning, especially Convolutional Neural Networks (CNNs), has shown remarkable efficiency in image classification and anomaly identification, making it highly suitable for detecting image forgeries. Research has demonstrated that transfer learning using pre-trained architectures like VGG16, ResNet, and Inception enhances detection accuracy. Additionally, hybrid approaches that integrate multiple detection methodologies have gained traction due to their improved performance.

1. General Overview of Image Forgery Detection: The literature indicates that most research in forgery detection is centered on images, with foundational studies contributing to the evolution of diverse detection techniques. These range from conventional methodologies to deep learning-based solutions and feature-based analysis.
2. Detection of Document Forgery: While image manipulation remains a core research focus, some pioneering studies have extended their scope to identifying forgeries in official documents, thereby advancing detection accuracy in administrative records.
3. Copy-Move Forgery Detection (CMFD): A recent technical review presents significant progress in CMFD methods, introducing an updated process pipeline. This offers researchers a structured approach to understanding and improving CMFD techniques.
4. Deep Learning in Image Forgery Detection: The role of deep learning in detecting forged images is substantial. This survey explores various DL-based models, particularly those focused on identifying copy-move and spliced forgeries—two of the most common types of image manipulation. Studies show that DL techniques, including CNNs, RCNNs, and LSTMs, significantly outperform traditional non-DL approaches in detecting image alterations.
5. Classification Framework: The literature survey provides a structured classification system that considers document type, forgery method, detection technique, validation dataset, performance metrics, and experimental results. This classification approach offers a detailed perspective on different aspects of forgery detection research.
6. Emerging Trends and Research Gaps: The review highlights the significant impact of deep learning on forgery detection and the advancements it has facilitated. However, challenges in detecting document forgery remain an area that requires further exploration.

III. RESEARCH METHODOLOGY

1. Image Enhancement:

Error-level analysis (ELA) is a preprocessing technique for detecting alterations in JPEG images by analyzing variations in compression levels. This method helps identify regions that may have been manipulated. Additionally, an advanced sharpening filter is applied using the Pillow library in Python. This filter enhances pixel contrast, particularly

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

in areas susceptible to distortion during image modifications, such as edges and lines, making potential forgeries more noticeable.

2. CNN Architecture:

The Convolutional Neural Network (CNN) architecture is systematically structured to process and analyse images efficiently. It begins with an input layer that receives the images, followed by convolutional layers that extract essential features. Pooling layers are incorporated to minimize spatial dimensions, while fully connected layers perform classification through a SoftMax activation function. The architecture is fine-tuned to capture hierarchical features and patterns. Finally, the model's performance is evaluated on the testing dataset to determine its effectiveness in differentiating between authentic and tampered images.

3. **Transfer Learning:**

Transfer learning is implemented using pre-trained models, specifically VGG16 and ResNet50, which are well-regarded for their effectiveness in image recognition tasks. These models provide a strong foundation by utilizing previously acquired features to improve performance in forgery detection. To ensure efficient training and thorough evaluation, the dataset is divided into 40% for training, 30% for validation, and 30% for testing. The selected models undergo training on the training dataset, with their performance assessed on the validation set. This process includes fine-tuning hyperparameters to optimize them for forgery detection. For ResNet50, the final layer is modified to align with the dataset's classification categories (authentic or tampered).

IV. PROPOSED SYSTEM

The proposed system enhances image forgery detection by integrating deep learning techniques with Error Level Analysis (ELA) as a preprocessing step. Given the increasing ease of digital image manipulation, this system is designed to tackle the challenge of detecting tampered content. It operates through three primary stages: data preprocessing, deep learning model implementation, and model evaluation.

In the data preprocessing stage, input images are resized and normalized to maintain uniform dimensions and pixel values, ensuring optimal model training. ELA is then applied to highlight manipulated regions by analyzing compression inconsistencies. Since altered areas tend to exhibit irregular compression patterns, this technique accentuates potential forgeries, enabling the deep-learning model to detect subtle modifications more effectively.

In the final evaluation phase, the system's performance is assessed using key metrics, including precision, recall, and F1-score. Precision evaluates the accuracy of identifying forged images, while recall measures the model's ability to detect all instances of tampering. The F1 score provides a balanced assessment of both precision and recall, ensuring a comprehensive evaluation. The results highlight the benefits of combining ELA with deep learning, showcasing higher detection accuracy and reduced false positives compared to conventional techniques.

1. Dataset

The system leverages publicly available datasets containing both authentic and manipulated images, ensuring a diverse and well-rounded training environment. These datasets are meticulously selected to encompass various forgery techniques, including copy-move, splicing, and retouching, allowing the model to recognize a broad spectrum of image alterations. To further strengthen the model's robustness, data augmentation techniques are applied to expand the training dataset artificially. Methods such as rotation, flipping, scaling, and colour adjustments introduce variations, reducing the risk of overfitting..

2. Feature Extraction Using ELA

Error Level Analysis (ELA) is an essential preprocessing method used to detect inconsistencies in image compression. When a JPEG image is saved, different areas experience varying compression levels. Altered sections tend to have different compression characteristics compared to unmodified regions. ELA helps expose these discrepancies by generating a grayscale heatmap, where manipulated areas appear with distinct brightness variations. This heatmap acts as a visual indicator, guiding the deep learning model to focus on potentially forged regions. By leveraging these highlighted areas, the model improves its ability to accurately identify image manipulations.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

3. CNN Model Architecture

The system utilizes a Convolutional Neural Network (CNN) architecture, which excels in image analysis by automatically learning spatial features. The CNN's input layer processes images that have been resized, normalized, and enhanced using ELA. Hidden layers include multiple convolutional layers with ReLU (Rectified Linear Unit) activation functions, allowing the model to capture intricate patterns. Pooling layers, such as max-pooling, help reduce the spatial dimensions of feature maps, improving computational efficiency. A fully connected layer follows, consolidating the extracted features for classification. Finally, the output layer generates probability scores, determining whether an image is genuine or manipulated, enabling precise forgery detection.

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 124, 124, 32)	2,432
conv2d_1 (Conv2D)	(None, 120, 120, 32)	25,632
max_pooling2d (MaxPooling2D)	(None, 60, 60, 32)	0
dropout (Dropout)	(None, 60, 60, 32)	0
flatten (Flatten)	(None, 115200)	0
dense (Dense)	(None, 256)	29,491,456
dropout_1 (Dropout)	(None, 256)	0
dense_1 (Dense)	(None, 2)	514

4. Model Training & Hyperparameters

The model is trained using a carefully selected set of hyperparameters to ensure optimal performance. The training process runs for 20 epochs, allowing the model to iteratively learn from the dataset without overfitting. A batch size of 32 is used, striking a balance between computational efficiency and the stability of gradient updates during training. The Adam optimizer is employed due to its adaptive learning rate capabilities, achieving faster convergence and better performance. The loss function used is categorical cross-entropy, suitable for binary classification tasks like distinguishing between authentic and forged images. These hyperparameters are chosen to maximize the model's accuracy and ensure efficient training, ultimately leading to a robust and reliable image forgery detection system.
Total params: 29,520,034 (112.61 MB), **Trainable params:** 29,520,034 (112.61 MB)

5. ARCHITECTURE

The development of a deep learning model follows a structured sequence to ensure efficient implementation and deployment. The process begins with defining the problem and collecting relevant data. Once the dataset is acquired, it undergoes preprocessing, which includes handling missing values, scaling features, and encoding categorical variables. The dataset is then split into training and testing sets to facilitate proper evaluation of the model's performance. After this, an appropriate algorithm is chosen based on the problem type and data characteristics. The selected model is trained using the training dataset, where its parameters are optimized to improve accuracy. Once training is complete, the model is evaluated on the testing dataset using performance metrics such as accuracy and F1-score

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

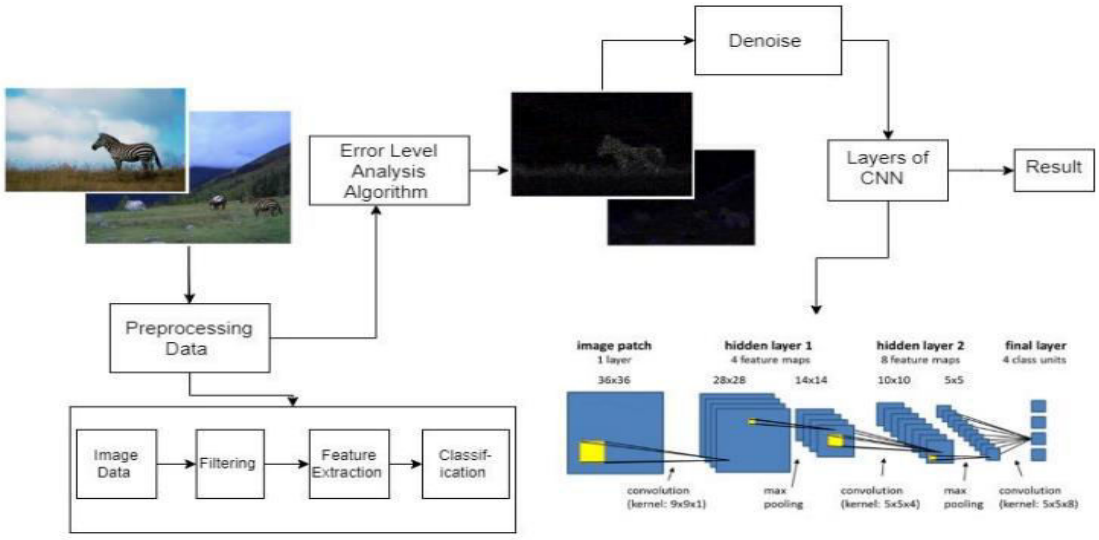


Fig.1 System architecture for Image Forgery Detection

Fig.1. System architecture of the proposed system

5.1. Preprocessing: - In deep learning, preprocessing involves a series of crucial steps to clean, format, and structure raw data before it is used for model training. This process typically includes handling missing values, scaling numerical features, encoding categorical data, and removing unnecessary or redundant information. Proper preprocessing techniques, such as normalization and standardization, enhance the model's performance by making it more resilient and capable of identifying significant patterns and relationships within the dataset.

5.2. Feature Extraction: -Feature extraction is the process of converting raw data into a refined set of essential attributes that capture the most significant information for analysis and model training. This method helps reduce dataset dimensionality while preserving key characteristics that define underlying patterns. These descriptors, vectors derived from image data, offer high discriminative power. In the context of Copy-Move Forgery (CMF), it is crucial that both the original and duplicated regions produce feature descriptors that exhibit strong similarity or correlation

5.3. Classification: - In deep learning, classification is a crucial task that involves assigning predefined labels or categories to input data by recognizing patterns learned during training. This process requires building a predictive model that can effectively differentiate between various classes within a dataset. The model is trained using labeled examples, where it extracts meaningful features and associates them with the correct output categories. Common algorithms used for classification include Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs), both of which excel in identifying complex patterns and making accurate predictions.

6. Implementation and Performance Evaluation

To assess the effectiveness of our proposed approach, multiple simulation runs were performed, and the outcomes were compared with cutting-edge forgery detection techniques. The experimental findings highlight the robustness and accuracy of our method in identifying manipulated images. Additionally, the accuracy curve reveals that validation accuracy stabilizes after 10 epochs, affirming the reliability of our training methodology. The model demonstrated strong classification performance in differentiating between genuine and altered images. The confusion matrix analysis shows that 305 forged images and 303 real images were accurately classified, while 21 manipulated images were incorrectly identified as authentic, and 34 genuine images were misclassified as tampered.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

V. EXPERIMENTAL RESULTS

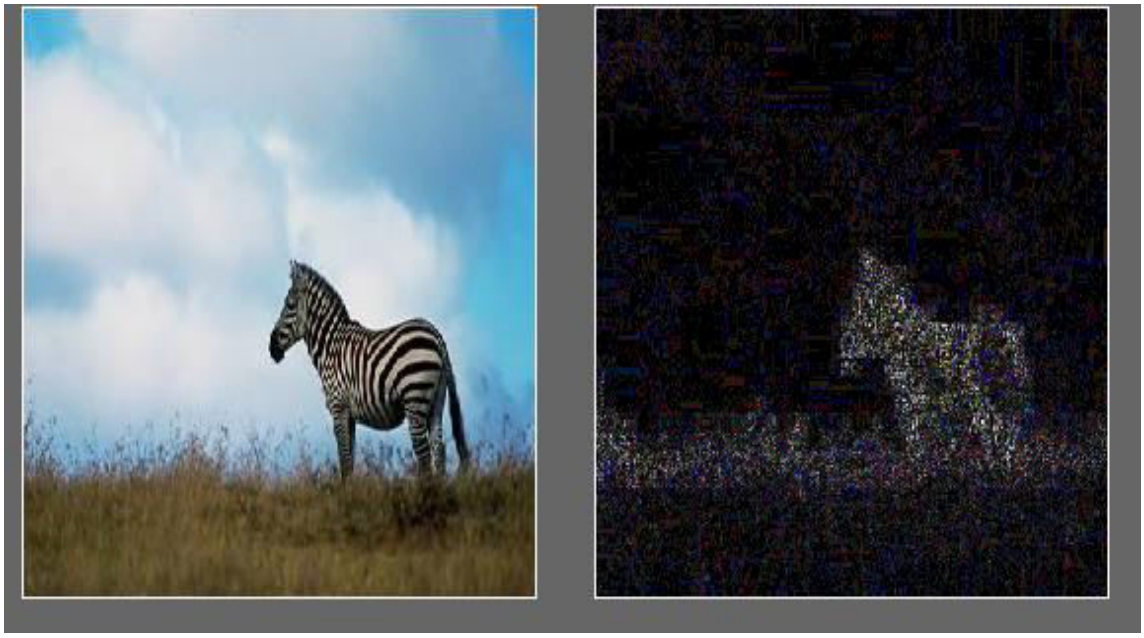


Fig.2. original image & ELA image

Fig.3. Highlighted image of Tampered Image

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

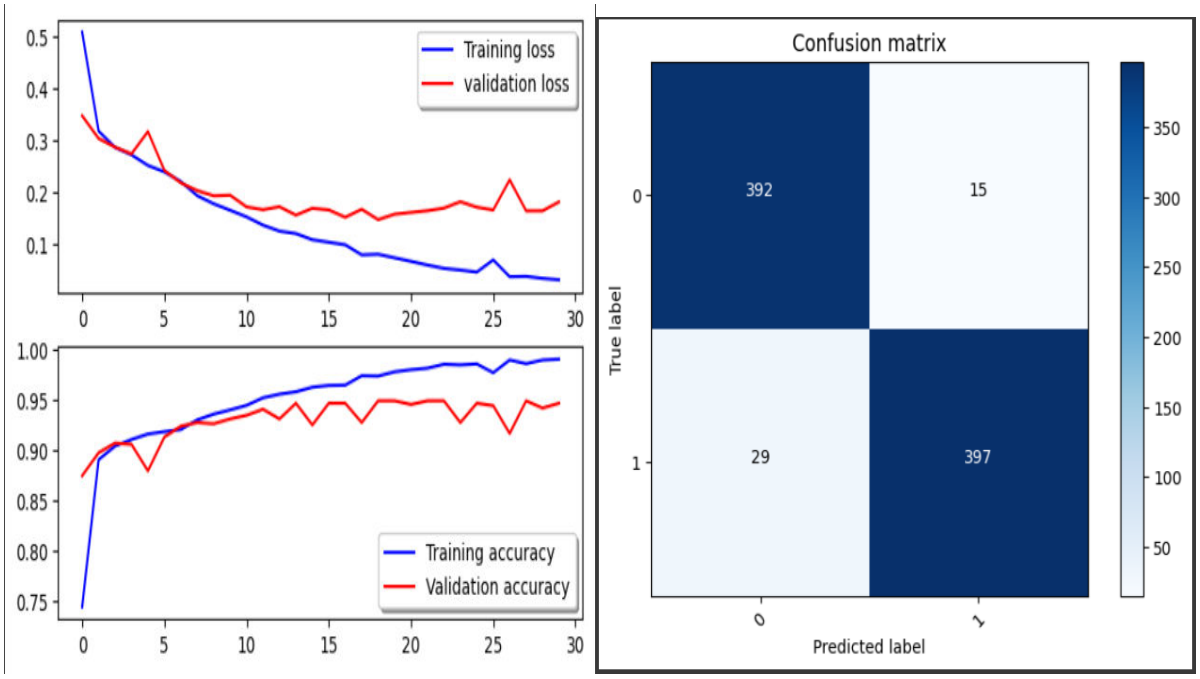


Fig.4. Training curve & Confusion Matrix

Your image is Forged

Detailed Analysis

Confidence Level	99.98%
ELA Variance	Low (Variance: 24.89)
Noise Consistency	Low (Std Dev: 4.99)
Metadata	Size: 773x573 Format: JPEG Mode: RGB File Size: 189.76 KB Creation Date: 2009:08:29 22:46:32 Modification Date: 2009:08:29 22:46:32 Camera Make: NIKON CORPORATION Camera Model: NIKON D200 Software: Adobe Photoshop CS Windows Aperture: N/A Shutter Speed: N/A ISO: N/A Focal Length: 24.0 mm Orientation: Horizontal (normal) Location: N/A, N/A (Timestamp: N/A) Validation Results: - Timestamp Mismatch: Yes - GPS Data Valid: No - Editing Software: Yes

Fig.6. Metadata Analysis of tampered image

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403171|

VI. CONCLUSION

Although the ELA-CNN model delivers outstanding performance, certain limitations require further improvement. The effectiveness of ELA results can be influenced by factors such as image compression and resizing, which may impact the model's overall accuracy. Future research could explore alternative preprocessing techniques. Additionally, testing the model on larger and more diverse datasets would help assess its generalization ability and resilience against evolving forgery techniques. The results of this study highlight the advantages of deep learning in identifying manipulated images, showcasing the effectiveness of integrating ELA with a CNN-based approach for image forgery detection.

The integration of deep learning techniques for image forgery detection presents a highly effective approach with the potential to enhance our ability to identify, prevent, and address this issue of public trust. As outlined in this research, the combination of deep learning with advanced detection methods enables real-time forgery identification, predictive modelling, and a deeper insight into image manipulation. With advancements in technology and the refinement of data collection techniques, the ability to detect forged images at an early stage will continue to improve. By leveraging these state-of-the-art technologies, we can make substantial progress toward reducing digital image manipulation and trustworthy digital environment.

REFERENCES

[1] Y. Zhang and X. Li, "Deep learning-based digital image forgery detection system," *Applied Sciences*, vol. 12, no. 6, p. 2851, 2022.
[2] Mushtaq, S., & Mir, A. H. (2018).” Image Copy Move Forgery Detection: A Review”. International Journal of Future Generation Communication and Networking, 11(2), 11–22.
[3] Xiaoqiang Zhang and Xuesong wang, (November 2018), “Digital Image Encryption Algorithm Based on Elliptic Curve 2. 2. Public Cryptosystem.” IEEE Access, vol.6.
[4] N. Kanwal, J. Bhullar, L. Kaur, and A. Girdhar, A Taxonomy and Analysis of Digital Image Forgery Detection Techniques, Journal of Engineering, Science & Management Education, vol. 10, pp. 35–41, 2017.
[5] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[6] Dhivya, S., Sangeetha, J., Sudhakar, B.,2020. Copy-move forgery detection using surf feature extraction and SVM supervise deep-learning technique. Soft Computing24,14429–14440.
[7] M. Qureshi and M. G. Qureshi, Image Forgery Detection & Localization Using Regularized U-Net. Singapore: Springer, 2021.
[8] 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.
[9] K. B. Meena and V. Tyagi, Image Splicing Forgery Detection Techniques: A Review. Cham, Switzerland: Springer, 2021.
[10] 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.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details