Enhanced Forgery Detection in Digital Images Using Deep Learning

CH. Lakshmi Kumari[1], Bellam Saikumar[2], Tharigoppula Shivaram[3]
[1]*Assistant Professor, Mahatma Gandhi Institute of Technology*
[2,3]*UG Student, Mahatma Gandhi Institute of Technology*

Abstract- **In today's digital era, social media platforms rely heavily on the sharing of images, making them a primary mode of communication and information dissemination. However, this prevalence has also given rise to the misuse of images through malicious tampering, such as creating fake or misleading information. Image forgery, a process that manipulates an image to deceive viewers, has significant implications for spreading false information, cybercrime, and even legal disputes. To counter this challenge, deep learning has proven to be a strong solution for image forgery detection. Convolutional Neural Networks (CNNs), a type of deep learning model, are especially good at identifying subtle inconsistencies in images. CNNs can analyze images at a pixel level, examining pixel-by-pixel data to identify unnatural patterns, inconsistencies, or tampering artifacts. CNN-based models can detect typical forgery types like splicing, copy-move, and image retouching by extracting and analyzing features such as edges, textures, and lighting inconsistencies.**

Of numerous detection methods, Error Level Analysis (ELA) with Convolutional Neural Network (CNN) architectures has proven to be a viable method for detecting image tampering. The flexibility of CNNs to be trained on vast datasets of forged and real images enables proper classification and even the localization of tampered areas. This positions deep learning as a strong and effective weapon against the increasing threat of image forgery, facilitating increased trust in digital media.

***Keywords*: Image forgery, Pixel-level analysis, Splicing, Copy-move, Image retouching, Error Level Analysis (ELA), Convolutional Neural Networks (CNNs), Tampering artifacts.**

INTRODUCTION

Images are crucial in communication today, especially on social media, but the increase in image forgery has become a significant challenge. Image forgery is manipulating or altering images to deceive or mislead. Advanced editing tools have made it easy for non-experts to create convincing forgeries. The consequences are very serious in fields such as media, law, science, and personal interactions. Digital image forgery is introduced by introducing anomalous patterns that cause inconsistencies in the properties of the image. Image forgery detection techniques can be broadly classified into active and passive approaches.

- Active approaches depend on additional information that is incorporated into the image during acquisition. Two common techniques are digital signatures, which introduce data to an image at the end of the acquisition process, and digital watermarking, inserted during image acquisition or processing.
- Passive methods do not require any a priori knowledge of the image and work on detecting tampering by analyzing the changes in the inherent features of the image. These methods detect distortions created by changes such as Copy-Move Forgery (CMF), Splicing Forgery, and Retouching Forgery.
- Copy-Move Forgery (CMF) is about copying a region of the image and pasting it somewhere else. It is very hard to detect because it has identical properties.
- Splicing Forgery is a technique where different images are merged together, with the color, lighting, and noise being altered, making it harder to detect.
- Retouching Forgery involves changing brightness, color, or contrast in order to either enhance or hide certain features.

The challenge of detecting forgeries has increased with the development of sophisticated editing tools that can make seamless alterations without leaving visible traces. This underlines the need for automated, reliable systems that can intelligently identify and localize image manipulations with high accuracy, crucial for ensuring image authenticity in various domains.

A. Problem Statement.

Images have been one of the principal media in communicating and information-sharing across all available platforms: social media, news outlets, and online messaging in the digital age. Easy access to sophisticated editing tools has given rise to massive image manipulation leading to digital image forgeries. These are mostly used for the spread of false information, alteration of public opinion, frauds, and changing evidence in a case in a court. The real-world implications of image forgery are significant. Fake images can contribute to the spread of fake news, reputational damage, and even political and social decisions. In legal and forensic settings, manipulated images can mislead investigations and compromise justice. Furthermore, the speed at which manipulated content is disseminated on social media increases its impact, making it difficult to control and verify authenticity in real-time. As forgeries become more sophisticated and harder to detect, the need for effective solutions to ensure the authenticity and integrity of digital images has become increasingly critical. This is essential in maintaining trust in digital content and mitigating the harmful effects of image forgery on individuals, organizations, and society as a whole.

I. EXISTING SYSTEM

The current systems in digital image forgery detection mainly revolve around using deep learning techniques to enhance the accuracy and efficiency of detection. The approach aims to overcome the limitations of detecting multiple forgery types, specifically image splicing and copy-move forgery, in real-life scenarios.

The proposed model is primarily based on the concept of analysing compression inconsistencies in images. The methodology involves creating a difference image that would highlight any differences between the original and its recompressed version. That difference image is used as input to pre-trained models, which have been fine-tuned for classification tasks as authentic or forged images.

Eight pre-trained models, including VGG16, VGG19, ResNet50, ResNet101, ResNet152, MobileNetV2, Xception, and DenseNet, were evaluated. Among these, MobileNetV2 demonstrated the highest accuracy (approximately 95%) while maintaining computational efficiency. The pre-trained models were adapted by replacing their classification layers with fine-tuned classifiers suitable for binary classification, optimizing detection performance.

This system significantly improved over traditional techniques by overcoming the challenges of computational complexity, post-processing manipulations, and detecting multiple types of forgery simultaneously. The results showed the effectiveness of transfer learning in enhancing digital image forgery detection.

II. LITERATURE SURVEY

This paper introduces novel detection of the digital image forge, focusing precisely on two splicing and two copy-move images. The developed approach relies upon a deep-learning model with extended transfer learning which enhances the chances of better image detection accuracy. The key idea is to analyse the difference in compression qualities between the forged and authentic regions of an image, which is typically undetectable by the human eye but can be detected through deep learning methods. They employ eight pre-trained models—VGG16, VGG19, ResNet50, ResNet101, ResNet152, MobileNetV2, Xception, and DenseNet—adapted for binary classification after fine-tuning. The results demonstrate that MobileNetV2 provides the highest detection accuracy (around 95%) with fewer training parameters, leading to faster training times and reduced computational costs. The proposed method significantly outperforms previous state-of-the-art techniques in terms of accuracy, precision, recall, F1 score, and AUC. Furthermore, the technique is designed to be lightweight, making it suitable for deployment in environments with limited computational resources. The study concludes the combination of transfer learning with analysis of image compression as offering robust solutions for image forgery detection in real-time, and thus future work lies in generalization to unseen data and incorporation of localization of the forged areas.[1]

The authors proposed a hybrid approach to detect SURF, A-KAZE, and DBSCAN clustering-based copy-move forgery. This approach identifies the tampered region clearly and is robust to rotation, scaling, and post-processing. Comparing the original image with the affine-transformed version, it will detect with great accuracy areas forged. When compared with datasets like Ardizzone and CoMoFoD, it stands tall in recognizing the tampered parts, mostly on smooth surfaces that other algorithms could not mark out. The technique greatly minimizes the complexity of computations at the expense of high precision, recall, and F1 scores. The effectiveness, efficiency, and resilience against complex manipulations make this an important tool in digital forensics.[2]

This hybrid framework of the Reptile Search Algorithm combined with deep learning for the purpose of detecting copy-move forgery is proposed by the authors. RSA optimizes feature selection with a reduced dimensionality without compromising the important information. Then, these features are passed to the deep learning model for the purpose of forgery classification and localization. The above approach shows greater robustness against occlusion, complex forgeries, and post-processing artifacts. Tested on benchmark datasets, this outperforms existing methods in precision, recall, and F1 score. However, the present model lacks runtime analysis and resilience against adversarial attacks; hence, a further exploration is needed for real-world application.[3]

With this paper, an active methodology capable of detecting image forgeries, especially from the perspective of social media, is proposed. The authors deal with the problems arising from compressed, low-quality images that such digital platforms commonly used. A modified U-NET model architecture is adopted here, which is further optimized by the Grasshopper Optimization Algorithm (GOA) that enhances segmentation performance. The U-NET model is primarily used in the biomedical image segmentation field and has been adapted to highlight the forged regions in the digital images. Some of the modifications included here are the addition of a few convolutional layers to both encoder and decoder pipelines, batch normalization, and better weight connections to enhance its accuracy and stability. The GOA optimizes hyper-parameters such as learning rates and mini-batch sizes to attain maximum performance. The authors show the robustness of their algorithm with the CASIA dataset concerning copy-move and splicing forgeries. The experimental results show that their proposed method performed better than existing models in terms of precision, recall, and F1 scores with better accuracy and segmentation results. The study merits the possibility of further validation on different datasets and real-time applications. The paper contributes greatly to the field by using deep learning together with optimization techniques for forgery detection.[4]

A robust trained system proposed for image forgery detection through deep learning techniques, especially splicing manipulation. Authors made use of ResNet50v2 architecture for their training and used transfer learning with pre-trained weights from a YOLO CNN model. This made the system capable of extracting meaningful features effectively, thus reducing training time and computational complexity. The proposed system was trained and tested on two benchmark datasets, CASIA_v1 and CASIA_v2, having labelled examples of authentic and forged images. After a series of experiments, the authors verified that the system achieved an elegant 99.3% accuracy on the CASIA_v2 dataset. Such performance is unprecedented when compared to results without transfer learning, thus reinforcing the usefulness of pre-trained models. The results of this study summarize the efficiency and reliability of the proposed method in spliced image detection. However, they also emphasize the need for further validation in quite diverse forgery scenarios and data sets. Their work sets the stage for further development of the system toward various types of digital image manipulation.[5]

The authors introduce a new two-stage hybrid approach for the detection of copy-move forgeries in digital images. The authors combined CNN architectures with the CenSurE keypoint detection algorithm to enhance the robustness and accuracy of forgery detection. The approach handles challenges related to geometric transformations, such as scaling and rotation, and post-processing operations, such as JPEG compression, noise addition, and brightness adjustments. The first step uses the CenSurE keypoint detector and FREAK descriptors to detect possible forged regions. RANSAC is then used to filter out outliers using the Random Sample Consensus. In the second step, the CNN model extracts image features with a deep learning-based classifier to enhance the detection and localization performance. Large-scale experiments were carried out on seven benchmark datasets, obtaining better results in various forgery scenarios. The hybrid model achieved high F1 scores while maintaining computational efficiency, processing images faster than existing methods. The findings highlight the approach's ability to detect forgeries in images with smooth, dense, or self-similar textures, making it a robust solution for multimedia forensics. Future work could explore further real-time scalability and adversarial robustness.[6]

III. PROPOSED SYSTEM

The proposed methodology puts forth a strong method of detecting digital image forgery with the integration of the strengths of Convolutional Neural Networks (CNNs) and Error Level Analysis (ELA). This enables the system to have high detection accuracy with local knowledge of where in an image forgery might take place.

Pre-processed images, upon being reconverted to a NumPy array, are experimented with using different CNN architectures, i.e., MobileNet, VGG, DenseNet, and a pre-trained CNN architecture. The integration of ELA's local knowledge and CNNs' pattern recognition ability enables the system not only to identify forgeries but to precisely outline spliced areas. This is a technique that overcomes main flaws of current techniques by enhancing precision and dependability.

The proposed system integrates CNNs and ELA for enhancing digital image forgery detection. By leveraging CNNs' feature extraction capabilities and ELA's accuracy for identifying compression inconsistency, the system achieves high accuracy with fewer false positives. The preprocessing step with ELA increases robustness towards different types of forgeries, from simple editing to elaborate splicing and pixel manipulation.

Comparative evaluation between MobileNet, VGG, DenseNet, and the current CNN model will identify the best approach to forgery detection. The flexible CNN framework can be adapted to a variety of forensic, media, and research applications. In comparison with traditional methods, this method reduces detection errors through the utilization of the complementary strengths of CNNs and ELA. The system's flexibility makes it possible to detect localized and generalized forgery, marking the manipulated areas efficiently for forensic and investigative examination. With its efficient, effective, and balanced strategy, this solution is designed to fight digital image forgery in contemporary digital environments.

CONCLUSION

The proposed system for Digital Image Forgery Detection using Deep Learning effectively deals with the emerging challenge of image tampering in the digital age. The integration of Convolutional Neural Networks (CNNs) with Error Level Analysis (ELA) enhances the accuracy, robustness, and adaptability of detection across various forgery techniques. The use of ELA as a preprocessing step helps identify compression inconsistencies, and CNNs extract complex features for reliable and precise detection of manipulations, such as copy-move, splicing, and retouching forgeries.

This method overcomes the limitations of current approaches because it provides localized insight into the regions that are tampered with, reduces false positives, and gives a much more comprehensive and automated solution. The experimental evaluation confirmed the system's high performance in detecting sophisticated forgeries and therefore is an effective application for use in media, forensics, and digital security.

Future improvements may focus on optimizing computational efficiency, addressing adversarial attacks, and expanding dataset diversity for real-world deployment. Overall, this system contributes significantly to digital forensics and image authenticity verification, strengthening trust in visual media.

REFERENCE

[1] H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash, "Enhancing Digital Image Forgery Detection Using Transfer Learning," in *IEEE Access*, vol. 11, pp. 91583-91594, 2023, doi: 10.1109/ACCESS.2023.3307357

[2] Fu, G.; Zhang, Y.; Wang, Y. Image Copy-Move Forgery Detection Based on Fused Features and Density Clustering. *Appl. Sci.* 2023, *13*, 7528.

[3] M. Maashi *et al.*, "Modeling of Reptile Search Algorithm with Deep Learning Approach for Copy Move Image Forgery Detection," in *IEEE Access*, vol. 11, pp. 87297-87304, 2023, doi: 10.1109/ACCESS.2023.3304237.

[4] Ghannad, N.; Passi, K. Detecting Image Forgery over Social Media Using U-NET with Grasshopper Optimization. *Algorithms* 2023, *16*, 399.

[5] Qazi, E.U.H.; Zia, T.; Almorjan, A. Deep Learning-Based Digital Image Forgery Detection System. *Appl. Sci.* 2022, *12*, 2851.

[6] Diwan and A. K. Roy, "CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection," in *IEEE Access*, vol. 12, pp. 43809-43826, 2024, doi: 10.1109/ACCESS.2024.3380460.