International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0327

e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2248-2258

Image Forgery Detection Using Deep Learning

Prof. D. D. Pukale[1], *Prof. V. D. Kulkarni*[2], *Julekha Bagwan*[3], *Pranali Jagadale*[4], *Sanjivani More*[5], *Renuka Sarmokdam*[6]

[1]*HoD, Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women's, Dhankawadi, India.*

[2]*Assistant Professor, Bharati Vidyapeeth's College of Engineering for Women's, Dhankawadi, India.*

[3,4,5,6]*B.E. Computer Engineering Students of Bharati Vidyapeeth's College of Engineering for Women's, Dhankawadi, India.*

Emails: *dhondiram.pukale@bharatividyapeeth.edu*[1], *vinaya.kulkarni@bharatividyapeeth.edu*[2], *julekhabagwan5402@gmail.com*[3], *pranujagadale11@gmail.com*[4], *sanjivani.s.more@gmail.com*[5], *renuka9688@gmail.com*[6]

Abstract

Image forgery is a big problem in digital media, making it important to have strong detection methods to fight misinformation and keep trust in visual content. In this project, we introduce an advanced image forgery detection system using VGG16, a powerful convolutional neural network, and Error Level Analysis (ELA) algorithms. Our goal is to create an efficient and accurate system that can identify real images from fake ones, especially focusing on detecting splicing and copy-move forgeries. By examining pixel intensities and patterns, our system can accurately find tampered areas, improving the integrity and trustworthiness of digital images. We use a diverse dataset of real and fake images from different sources to train and test the VGG16-ELA model. We aim to find the percentage of forgery, highlighting the forged areas and generating the mask of forged area. Through this effort, we aim to increase trust in visual content in fields like forensics, journalism, and social media, helping to ensure the reliability of digital information.

Keywords: *Convolutional Neural Network; Copy Move Forgery; Deep Learning; Error Level Analysis (ELA); Forensic Analysis; Image Forgery Detection; Splicing Forgery; VGG16.*

1. Introduction

The advent of deep learning methodologies has ushered in a new era of innovation in image forgery detection, with VGG16 and Error Level Analysis (ELA) algorithms emerging as pivotal tools in this field. Image forgery, characterized by the deliberate alteration or manipulation of visual content, poses significant challenges in various domains, including forensics, media authentication, and digital content integrity. Detecting forged images and localizing tampered areas are paramount for preserving the credibility and authenticity of digital media in today's information-driven society. In recent years, the deep learning community has witnessed remarkable progress, fueled by advances in convolutional neural networks (CNNs) such as VGG16. VGG16, a deep convolutional neural network architecture, has demonstrated exceptional performance in image classification tasks by virtue of its deep hierarchical structure and large receptive fields. With its ability to learn rich hierarchical representations directly from raw pixel data, VGG16 is poised to revolutionize image forgery detection by extracting intricate features indicative of manipulation. Complementing the prowess of VGG16, Error Level Analysis (ELA) algorithms offer invaluable insights into image authenticity. ELA exploits variations in error levels introduced during image compression to identify regions potentially subjected to alterations. By analyzing discrepancies in error levels across different areas of an image, ELA can pinpoint suspicious regions and anomalies, providing critical clues for detecting image forgeries[1-7]. The objective of this project is to leverage the synergies between VGG16 and ELA algorithms to develop an advanced image forgery detection system. Our system aims to detect a wide spectrum of forgery techniques, including splicing and copy-move, by integrating cutting-edge deep learning methodologies with ELA-based analysis. By enhancing the accuracy, sensitivity, and specificity of forgery detection, we empower users to identify and mitigate the proliferation of manipulated images effectively. Moreover, a central focus of this project involves the development of a user-friendly graphical user interface (GUI) that simplifies the process of uploading, analyzing, and interpreting image data. The intuitive interface streamlines interaction with the forgery detection system, making it accessible to users with diverse levels of technical proficiency. Through user-centric design principles, we endeavor to democratize forgery detection and foster widespread adoption of reliable tools for combating digital misinformation.

2. Method

This section details the methodology employed in developing our robust image forgery detection system. The process is outlined chronologically, including the research design, research procedure and data acquisition.

2.1. System Architecture

The system architecture depicts the overall comprehensive process for detecting forged images using a combination of image preprocessing techniques, convolutional neural networks (CNN), error level analysis (ELA), and post-processing methods. Following Figure 1 shows a simplified system architecture diagram for image forgery detection using CNN [8-12]. The process starts with utilizing an image dataset alongside a test image. The images within the dataset are subjected to various preprocessing steps such as resizing, normalization, and conversion to grayscale.

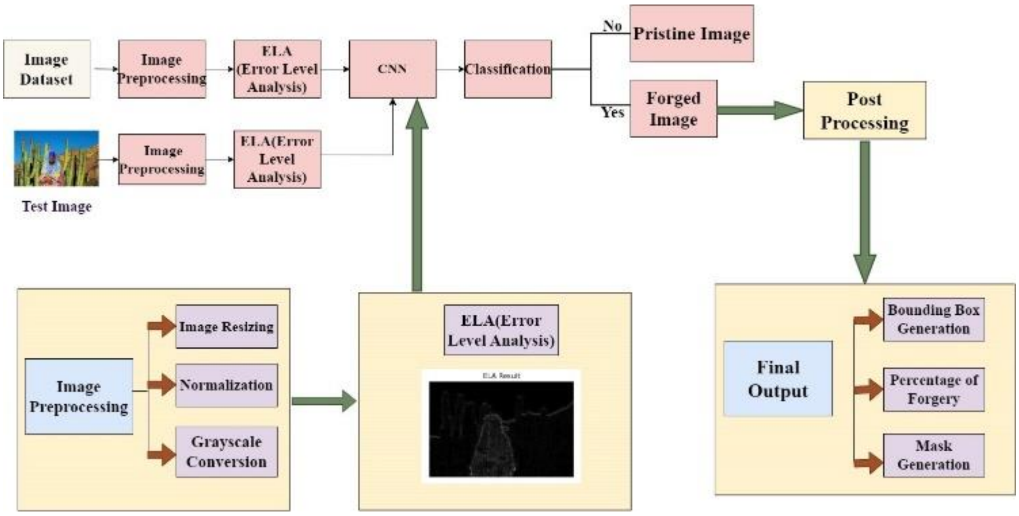


Figure 1 System Architecture

After this preprocessing, the images undergo ELA (Error Level Analysis) to detect potential tampering or manipulation by analyzing the compression levels within the images. The results of the ELA, which indicate error levels, are then used as input features for training a CNN model to classify images as either unaltered or forged. Similarly, the test image undergoes a comparable preprocessing pipeline involving resizing, normalization, and conversion to grayscale. Subsequently, the preprocessed test image is analyzed using ELA to produce a heatmap that highlights regions with potential forgery or manipulation. The test image's ELA result undergoes further analysis using post-processing techniques, which involves identifying the forged area within the image, determining the percentage of forgery present, and creating an ELA mask that visually displays the potentially manipulated regions. The comprehensive assessment of whether the test image has been forged or not is derived from combining the classification result from the CNN (pristine or forged) and the post-processing analysis. Moreover, visual aids such as the highlighted forged area, the percentage of forgery, and the ELA mask are provided to facilitate forgery detection and localization. This process leverages the strengths of both deep learning (CNN) and traditional image forensics (ELA) to accurately identify forged images and provide detailed information about the nature and extent of the forgery.

2.2. Proposed Methodology

The identification of forgeries involves a comprehensive dataset comprising images from CASIA 1.0 and CASIA 2.0, encompassing a variety of forgeries such as copy-move and spliced images. Initially, the dataset goes through pre-processing steps to standardize the images, which involve resizing them to a consistent size, normalizing pixel values for uniformity, and converting them to grayscale for simplified analysis. After pre-processing, the dataset images undergo Error Level Analysis (ELA) [13-17]. ELA is a critical step in identifying potential tampering by examining the variations in compression levels across different areas of the images. This analysis provides valuable insights into areas where forgeries may have occurred based on differences in compression artifacts. The preprocessed dataset is used to train a VGG16 deep learning model concurrently. The VGG16 model aims to differentiate between authentic and manipulated images by utilizing the features extracted during ELA and other preprocessing stages. Throughout the training process, the model's parameters are fine-tuned to effectively classify images as genuine or manipulated, considering the intricacies inherent in copy-move and spliced forgeries.Once the VGG16 model is trained, it is ready for inference on new, unseen images, including the test image in question. Similar preprocessing steps are applied to the test image, preparing it for ELA analysis. The ELA results provide a heatmap highlighting suspicious areas that may indicate forgery or manipulation within the test image. The preprocessed test image and its corresponding ELA heatmap are input for the VGG16 model, which then conducts classification to identify if the image is authentic or altered. If the classification indicates the image is altered, further post-processing steps are executed (Figure 2a & Figure 2b). These steps include recognizing and emphasizing the altered areas within the image, calculating the proportion of forgery present based on the detected manipulation, and producing an ELA mask to display the potentially modified areas. The final output of the forgery detection process includes the classification label (pristine or forged), if forged then the highlighting the forged areas, the percentage of forgery detected, and the ELA mask illustrating the suspicious regions.

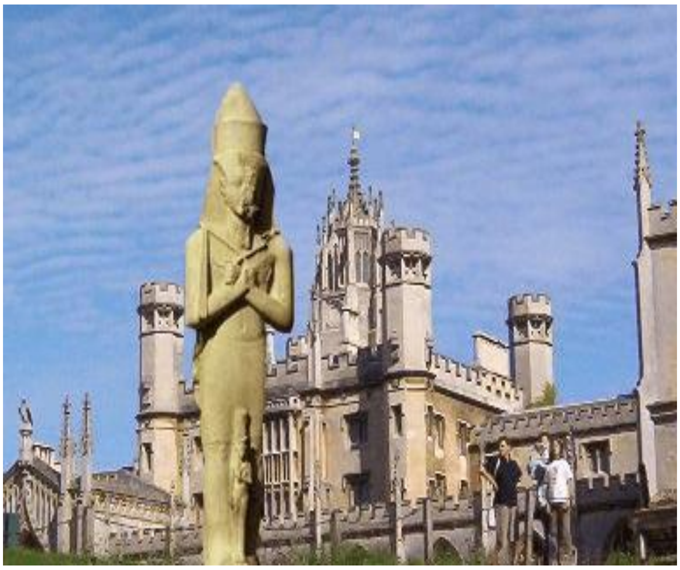


Figure 2 (a) Image

Figure 2 (b) Generated ELA Image

This comprehensive methodology integrates deep learning techniques with traditional image forensics, enabling the model to detect various types of forgeries with accuracy and provide detailed insights into the nature and extent of the detected manipulations. **ELA:-** Error Level Analysis (ELA) is a method in digital image forensics that is utilized to identify possible instances of manipulation or forgery in images. It operates by examining the changes in compression levels that happen when an image is saved or edited repeatedly. ELA points out areas with notable differences in error levels, indicating potential areas where modifications like copy-move or splicing may have taken place [18-21]. This approach is valuable for pinpointing questionable regions within images and is frequently employed as a preliminary stage in forgery detection algorithms, offering insights into potentially altered areas for further examination.

2.3. Pre-Processing

In order to prepare the dataset for training the deep learning model for image forgery detection, it is crucial to have a thorough pre-processing pipeline. The dataset contains images with genuine and altered samples, and the pre-processing steps are aimed at improving image quality and extracting relevant features to accurately detect and localize forged areas. The main objective of pre-processing is to improve image quality by eliminating or minimizing irrelevant and extra elements in the background of the images. The application of filters helps to eliminate noise and high-frequency components that could impact detection accuracy. Furthermore, improving image contrast, brightness, and sharpness highlights important features and enhances visibility. Techniques like histogram equalization or adaptive histogram equalization can be utilized to enhance image contrast.

2.3.1. Image-Resizing

Resizing an image involves altering its width and height to achieve consistency, particularly when working with datasets containing images of different sizes. The aim is usually to scale down larger images to match the dimensions of smaller ones, thus conserving computational resources and processing time. In our case, the CASIA v1.0 and CASIA v2.0 datasets feature images of various sizes, so we are standardizing the images to a constant size of 128 X 128. Various interpolation methods or techniques are applied, enabling the estimation of new pixel values based on surrounding known pixels, resulting in a smooth and coherent appearance of the modified image.

2.3.2. Normalization

Image normalization is a common preprocessing step in many computer vision and image processing tasks. It involves transforming the pixel values of an image to a common scale or range, typically between 0 and 1 or -1 and 1. The main purpose of normalization is to ensure that the pixel values are within a consistent range, which can improve the performance and convergence of various algorithms that operate on the image data. Min-Max Normalization: This technique linearly scales the pixel values to a specified range, usually [0, 1] or [-1, 1]. The formula for min-max normalization is - x_norm = (x - min(x)) / (max(x) - min(x)) Where x is the original pixel value, min(x) and max(x) are the minimum and maximum pixel values in the image, respectively, and x_norm is the normalized pixel value.

2.3.3. Greyscale Conversion

Grayscale conversion is a fundamental operation in image processing, where a color image is converted into a grayscale (or monochrome) image. This process involves reducing the color information of each pixel to a single intensity value, representing the brightness or luminance of that pixel. Grayscale images are often used in computer vision and image analysis tasks, as they simplify the data and can enhance certain features or patterns in the image.

2.4.Dataset

In this project, we leveraged the renowned CASIA 1.0 and CASIA 2.0 datasets for image forgery detection. The CASIA datasets are widely regarded in the field of image forensics, offering a rich collection of authentic and manipulated images essential for training and evaluating forgery detection algorithms. CASIA 1.0 provided a solid foundation with its diverse forgery types such as copy-move and splicing, serving as a benchmark for our initial model development. As we progressed, incorporating CASIA 2.0 enriched our dataset with more complex forgery scenarios, enabling us to enhance the robustness and accuracy of our forgery detection system. CASIA 1.0: - CASIA 1.0 contains a diverse collection of digital images, including both authentic (pristine) images and images that have been manipulated or forged. The dataset covers various types of forgeries, such as copy-move, splicing, and other digital manipulations (Figure 3a & Figure 3b). CASIA 1.0 was created to facilitate research and development in image forgery detection and digital forensics. It serves as a benchmark dataset for evaluating the performance of forgery detection algorithms. The images in CASIA 1.0 exhibit different levels of complexity in terms of forgery techniques, making it suitable for testing the robustness and accuracy of forgery detection models. CASIA 2.0: - CASIA 2.0 is an extension and enhancement of the CASIA 1.0 dataset, offering a larger and more diverse collection of images. Compared to CASIA 1.0, CASIA 2.0 includes a broader range of forgery types and scenarios, including more sophisticated manipulations and realistic forgery challenges. Researchers and practitioners often use CASIA 2.0 to validate and improve forgery detection algorithms, as it provides a more comprehensive and challenging dataset for testing algorithm performance. Similar to CASIA 1.0, CASIA 2.0 serves as a benchmark dataset in the field of image forensics, enabling comparative studies and advancements in forgery detection techniques.

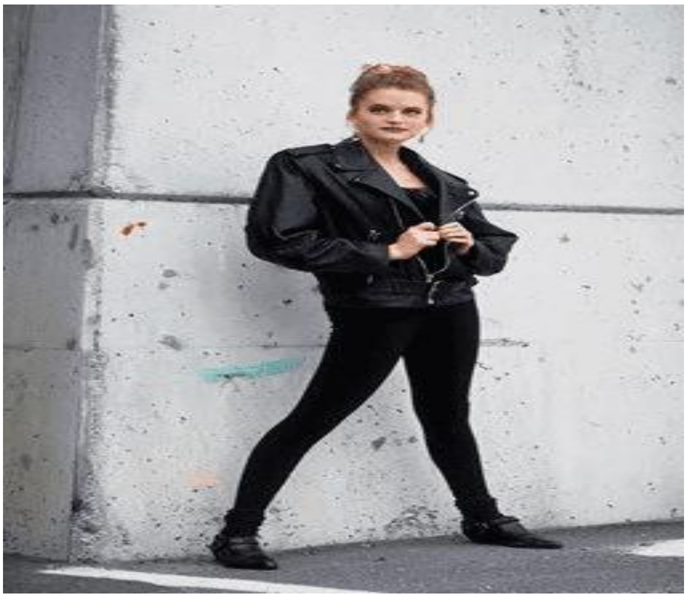


Figure 3 (a) Original Image

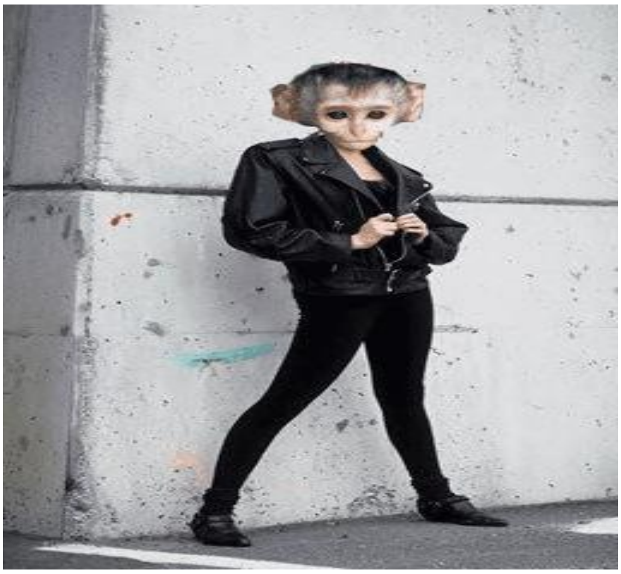


Figure 3 (b) Forged Image

3. Results and Discussion

In this section, we present the results obtained from training three deep learning models CNN and VGG16 on a combination of CASIA1 and CASIA2 datasets for the task of image forgery detection. We provide a comprehensive analysis of the training and validation performance of each model, including accuracy metrics, loss curves, and confusion matrices. Additionally, we discuss the implications of these results and draw insights into the effectiveness of each model for detecting forged images.

3.1.Model Training and Validation

We first trained the CNN and VGG16 models using a dataset comprising authentic and forged images extracted from the CASIA1 and CASIA2 datasets. The training process involved optimizing the models' parameters to minimize the binary cross-entropy loss function while maximizing classification accuracy. The dataset was split into training and validation sets, with a portion of the data reserved for model evaluation. The training metrics, including loss and accuracy, for each model are visualized below. These plots provide insights into the training progress and performance of each model throughout the training process. The training and validation accuracy curves for VGG16 are depicted in Figure 4 & Figure 5. The model exhibits a steady increase in both training and validation accuracy, reaching a peak accuracy of 98.29% on the validation set. So, with a learning rate of 0.0001 and trained over 100 epochs, the confusion matrix reveals a training accuracy of 97.14% for VGG16. Figure 6 illustrates the training and validation loss curves for the CNN model. Similar to VGG16, the model shows a decreasing trend in both training and validation loss with slight fluctuations. Also the threshold for both models was kept as 50%, i.e. if model predicts accuracy of authenticity as greater than 50%, then it will be labelled as forged else authentic.

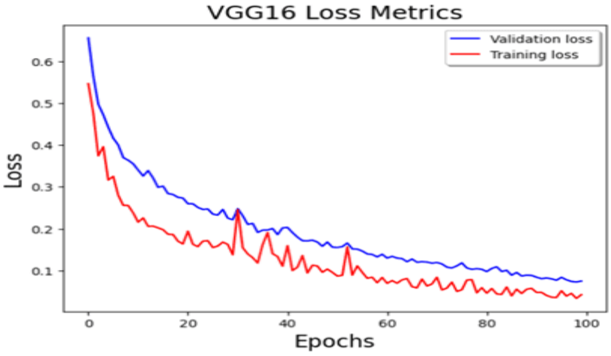


Figure 4 VGG16 Loss Graph

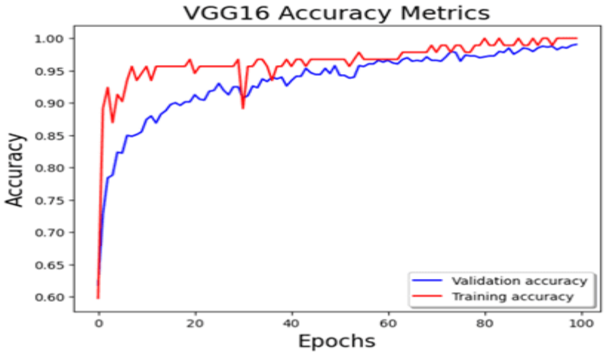


Figure 5 VGG16 Accuracy Graph

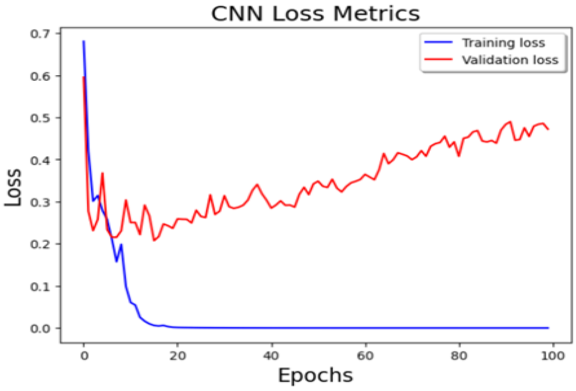


Figure 6 CNN Loss Graph

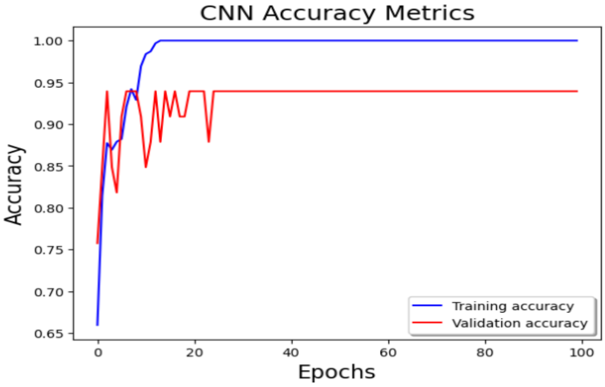


Figure 7 CNN Accuracy Graph

The training and validation accuracy curves for CNN are presented in Figure 7. Despite some variations, the model achieves a notable accuracy of 88.16% on the validation set.

3.2.Confusion Matrix

The confusion matrix below offers a detailed insight into the model's performance, showing the counts of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN), Figure 8. In the context of image forgery detection, TP represents the number of correctly identified forged images, FP indicates the count of authentic images misclassified as forged, TN reflects the accurate identification of authentic images, and FN signifies the forged images incorrectly labeled as authentic [22-25]. These metrics illustrate the accuracy of identifying authentic and forged images, along with any misclassifications.

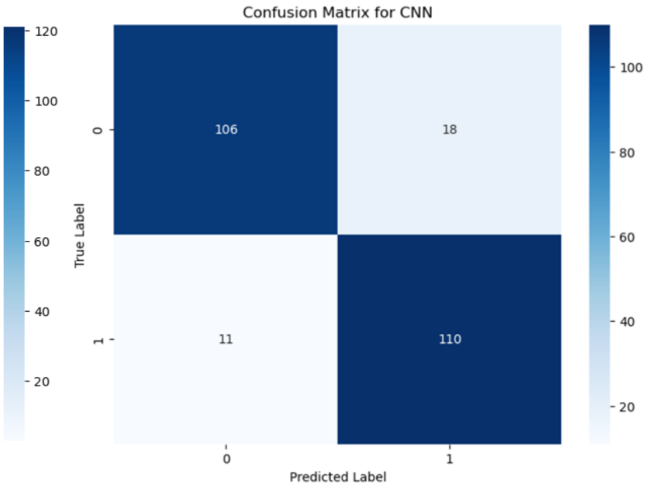


Figure 8 Confusion Matrix for CNN

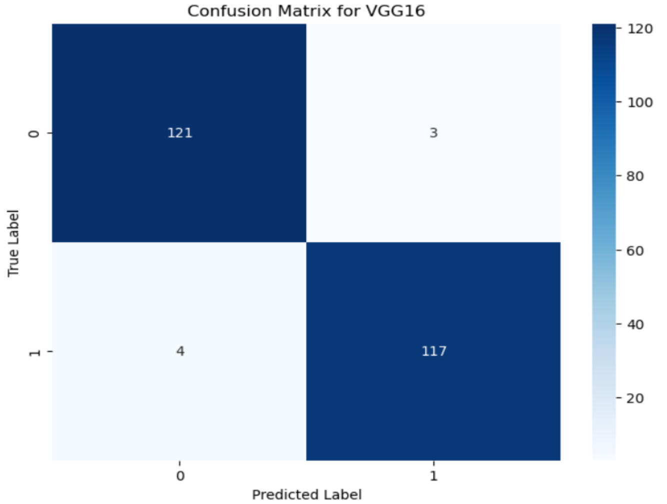


Figure 9 Confusion Matrix for VGG16

Precision, a measure of the model's exactness in predicting positive instances, is calculated as the ratio of TP to the sum of TP and FP. In our study, precision quantifies the accuracy of the VGG16 model in correctly identifying forged images among all images classified as forged. With an overall model accuracy of 97.14%, the precision of the model is 97.50%. For the CNN, model has achieved accuracy of 88.16% and 85.94% as precision, Figure 9. Recall, also known as sensitivity, measures the model's ability to identify all positive instances, calculated as the ratio of TP to the sum of TP and FN. For our VGG16 model, recall indicates its effectiveness in capturing all forged images from the entire dataset of forged images. The recall for the VGG16 model is 96.69% and for the CNN is 90.91%. The F1 score, a harmonic mean of precision and recall, provides a balanced assessment of the model's performance. It considers both false positives and false negatives and is calculated as 2 * (precision * recall) / (precision + recall). In our analysis of the VGG16 model, the F1 score synthesizes precision and recall into a single metric, offering insight into the overall effectiveness of the model in detecting forged images while minimizing misclassifications, Figure 10 & Figure 11. The F1 score for the VGG16 model is 97.09% and for the CNN is 88.35%, and the outcomes are shown in Figure 12, Figure 13 & Figure 14.

3.3.Comparison Between VGG16 and CNN

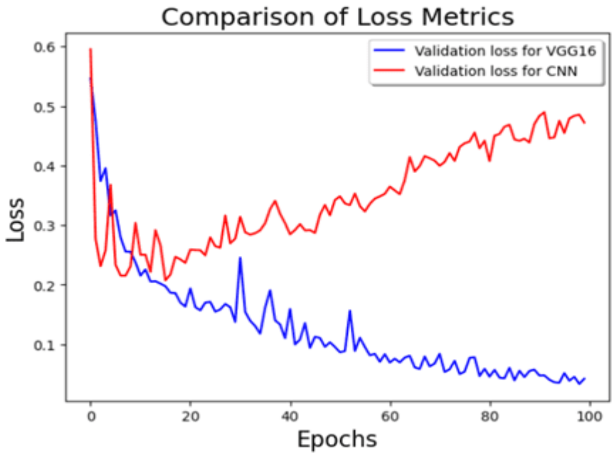


Figure 10 Comparison of Loss Metrics

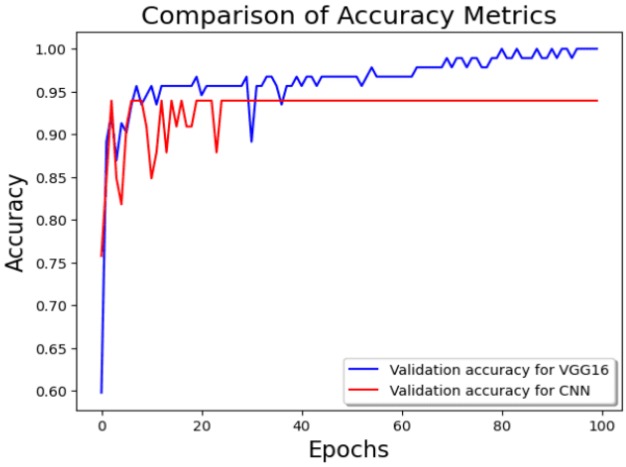
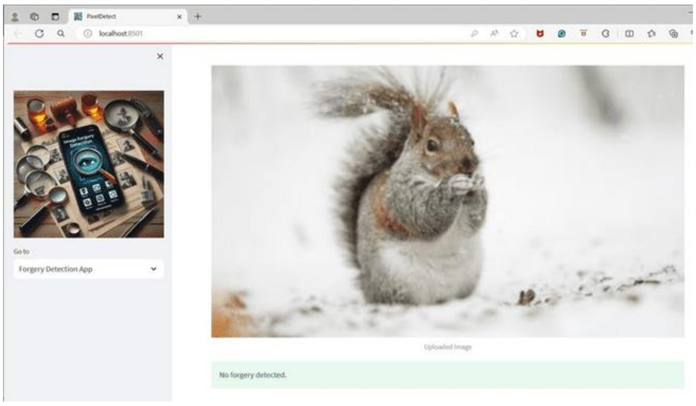


Figure 11 Comparison of Accuracy Metrics

Table 1 Comparative Analysis of Accuracy Metrics of Models

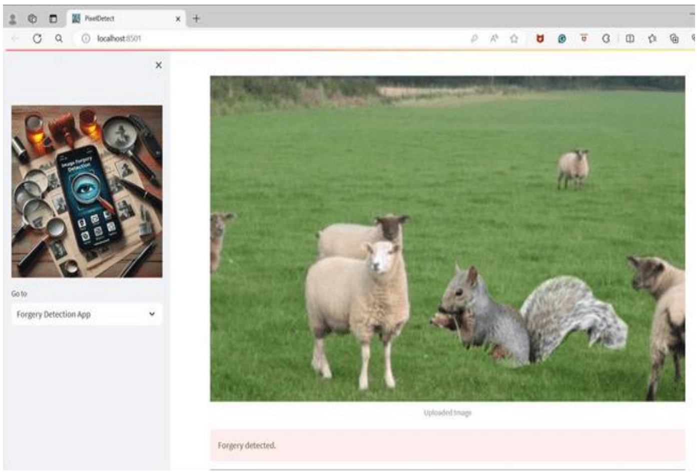
Model	Accuracy	Precision	Recall	F1-score
1. Base Paper [25]	71.6%	75.69%	72.59 %	74.09 %
2. CNN	88.16%	85.94%	90.91 %	88.35 %
3.VGG16	97.14%	97.50%	96.69 %	97.09 %

3.4.Outcome Analysis



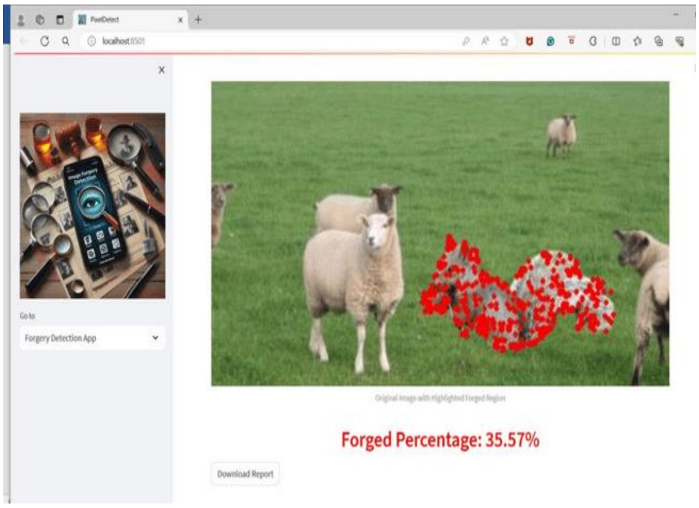
No forgery detected.

Figure 12 Original Image (without any forgery)



Forgery detected.

Figure 13 The Image with Forgery Detecting as a Forged Image



Forged Percentage: 35.57%

Figure 14 Highlighting the Forged Area Along with the Percentage of Forgery

3.5.Applications

1. Device Detection: Identifying forged images that have been altered to appear as if they were taken from a specific device.
2. Copy-Moving Detection: Detecting images where parts have been moved from one location to another within the same image.
3. Fake Colorization Detection: Identifying images that have been artificially colorized.
4. JPEG Post-Processing Detection: Detecting images that have undergone generic contrast adjustments after JPEG compression.
5. Contrast Enhancement Detection: Identifying images where contrast has been artificially enhanced.
6. Image Manipulation Detection: Detecting images that have been manipulated at the pixel or image level.
7. Industrial Object Detection: Identifying forged images in industrial settings, such as those created through physics-based rendering.

3.6. End Users

1. Forensic Scientists: Utilize deep learning for detecting forgeries in legal cases and investigations.
2. Security Companies: Implement deep learning-based systems to ensure the integrity of digital images and prevent misinformation.
3. Copyright Holders: Protect their intellectual property by detecting unauthorized use or alteration of their images.
4. Social Media Platforms: Use deep learning to monitor and remove fake images from their platforms.

3.7.Advantages

1. High Accuracy: Deep learning models can achieve high accuracy in detecting forgeries, especially when trained on large datasets.
2. Automation: Reduces the need for manual intervention, saving time and resources.
3. Adaptability: Can adapt to different types of image forgeries and processing methods.
4. Scalability: Capable of processing large volumes of images efficiently.

3.8.Disadvantages

1. Dependence on Dataset Selection: The effectiveness of deep learning models heavily depends on the selection and utilization of datasets
2. Cumbersome Algorithms and Wrong Classifiers: Many models suffer from cumbersome algorithms and incorrect classifiers, leading to poor performance.
3. Extra Time Consumption and Expensiveness: The development and training of deep learning models can be time-consuming and costly.

3.9.Future Scope

1. Uncovering Deepfakes and AI-Generated Content: With the rise of deepfake technology and AI-generated content, there is a growing need to develop specialized models capable of distinguishing between authentic and manipulated media, including videos, audio, and images.
2. Privacy Protection: Integrating forgery detection mechanisms that respect and preserve individual's privacy by ensuring sensitive information is not exposed during the analysis of images.
3. Deployment in Various Industries: Expanding the adoption of forgery detection systems in industries beyond traditional media, such as healthcare (medical imaging authenticity), banking (fraud detection), and e-commerce (product authentication).

Conclusion

In conclusion, deep learning has shown remarkable promise in detecting image forgeries, including DeepFake content, by learning complex patterns from large datasets. Image forgery detection using deep learning has advanced significantly, improving the integrity of visual content. Our project, combining Error Level Analysis (ELA) with CNN and VGG16 models, has surpassed previous results. The base paper [25] achieved 71.6% accuracy and 75.69% precision. In contrast, our CNN model achieved 88.16% accuracy and 85.94% precision, while the VGG16 model reached 97.14% accuracy and 97.50% precision. This robust system effectively identifies, calculate the percentage of forged area and highlights the forged region, demonstrating superior performance metrics for both copy-move and splicing forgery.

Acknowledgements

We would like to express our sincere gratitude to our Principal Prof. Dr. P.V. Jadhav for their constant support and guidance, our project guides, Prof. D. D. Pukale and Prof. V. D. Kulkarni, for their invaluable support and guidance throughout the development of our Image Forgery Detection using Deep Learning project. Their expertise and encouragement have been instrumental in our progress. We also thank the faculty of Bharati Vidyapeeth's College of Engineering for Women, Pune for providing the necessary resources and a supportive environment. Special thanks to our peers for their constructive feedback. Thank you all for your contributions, which have been crucial to the success of our project.

References

[1]. J. Ouyang, Y. Liu, and M. Liao, "Copy-move forgery detection based on deep learning," in Proc. 2017 10th Int. Congr. Image Signal Process., BioMedical Eng. Informatics (CISP-BMEI), 2017, pp. 1–5.

[2]. N. H. Rajini, "Image forgery identification using convolution neural network," Int. J. Recent Technol. Eng., vol. 8, 2019.

[3]. A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, 2004.

[4]. Y. Abdalla, T. Iqbal, and M. Shehata, "Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network," Information, vol. 10, no. 09, p. 286, 2019.

[5]. Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in Proc. IEEE Int. Workshop Information Forensics Security (WIFS), 2016.

[6]. CASIA Tampered Image Detection Evaluation Database, 2010.

[7]. Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered jpeg image detection via DCT coefficient analysis," Pattern Recognition, vol. 42, pp. 2492-2501, 2009.

[8]. 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.

[9]. Y. Wu, W. Abd Almageed, and P. Natarajan, "ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features," in Proc. 2019 IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Long Beach, CA, USA, 15–20 June 2019, pp. 9535–9544.

[10]. K. B. Meena and V. Tyagi, "Image Forgery Detection: Survey and Future Directions," in Data, Engineering and Applications: Volume 2, R. K. Shukla, J. Agrawal, S. Sharma, and G. Singh Tomer, Eds., Springer, Singapore, 2019, pp. 163–194.

[11]. A. A. K. Jaiswal and R. Srivastava, "Image Splicing Detection using Deep Residual Network," in Proc. 2nd Int. Conf. Adv. Comput. Softw. Eng. (ICACSE), San Francisco, CA, USA, 13–15 Oct. 2019.

[12]. R. Salloum, Y. Ren, and C.-C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (mfcn)," J. Vis. Commun. Image Represent., vol. 51, pp. 201–209, 2018.

[13]. P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Learning rich features for image manipulation detection," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), June 2018.

[14]. J. Bunk, J. H. Bappy, T. M. Mohammed, L. Nataraj, A. Flenner, B. S. Manjunath, S. Chandrasekaran, A. K. Roy-Chowdhury, and L. Peterson, "Detection and localization of image forgeries using resampling features and deep learning," in Proc. CVPR Workshops, IEEE Comput. Soc., 2017, pp. 1881–1889.

[15]. L. Jian, L. Xiaolong, Y. Bin, et al., "Segmentation-based image copy-move forgery detection scheme," IEEE Trans. Inf. Forensics Sec., vol. 10, no. 3, pp. 507–518, 2015.

[16]. 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, 2022.

[17]. L. Bondi, S. Lameri, D. Güera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering detection and localization through clustering of camera-based CNN features," in Proc. 2017 IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), 2017, pp. 1855–1864.

[18]. B. Chaitra and P. B. Reddy, "A study on digital image forgery techniques and its detection," in Proc. 2019 Int. Conf. Contemporary Comput. Informatics (IC3I), 2019, pp. 127–130.

[19]. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 6, pp. 1841–1854, 2012.

[20]. S. Easow and D. L. C. Manikandan, "A study on image forgery detection techniques," Int. J. Comput. (IJC), vol. 33, no. 1, pp. 84–81, 2019.

[21]. A. Kuznetsov, "Digital image forgery detection using deep learning approach," J. Phys.: Conf. Ser., vol. 1368, no. 3, p. 032028, 2019.

[22]. P. Pierluigi, "Photo Forensics: detect photoshop manipulation with error level analysis," 2023.

[23]. A. Raja, "Active and passive detection of image forgery: A review analysis," IJERT-Proc, vol. 9, no. 5, pp. 418–424, 2021.

[24]. P. Sharma, M. Kumar, and H. Sharma, "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation," Multimedia Tools Appl.

[25]. Devjani Mallick, Mantasha Shaikh, Anuja Gulhane and Tabassum Maktum, "Copy Move and Splicing Image Forgery Detection using CNN": ITM Web Conf., 44 (2022) 0305.