Decoding Deception:Error Level Analysis for Image Forgery Detection

[1] Bhagyashri R. Hanji, [2]Charan G N, [3]Hemanth Kumar V, [4]J S Naga Vishnu Sai, [5]Jeevan S
[1]*Professor, Department of Computer Science and Engineering*
[2,3,4,5]*UG Students, Department of Computer Science and Engineering*
[1,2,3,4,5]*Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka India*

Abstract— Detecting digital image forgery is crucial to safeguard image integrity, especially in an era where manipulation is effortless. Error Level Analysis serves as a valuable tool by decreasing image quality and comparing error levels to identify modifications. This study employs Convolutional Neural Network, a deep learning method to enhance image forgery detection. By introducing Error Level Analysis extraction, the validation accuracy improves by approximately 2.7%, leading to enhanced test accuracy. However, this enhancement comes at the cost of a 5.6% increase in processing time. The research underscores the trade-offs involved in leveraging ELA within a deep learning framework for more effective image authenticity verification.

Keywords— Image Forgery Detecting, ELA, CNN, Digital Content Verification, Tampered Images, Flask framework, Image Preprocessing.

I. INTRODUCTION

Image data can be easily manipulated in the ever-changing digital environment. Photo editing software is now widely available not only for desktop computers and laptops, but also for handheld mobile devices. Deep models are often used in to create super-realistic face-altering images and videos. People often use this on social media, in business, and even in crimes. The use of images for criminal purposes should raise concern because it will cause serious problems for society, government and business. Therefore, the validity of images on the internet must be verified. Therefore, it is important to ensure the integrity of digital images. In this case, a fake image detection system can be used to ensure the validity of the image. Digital Imaging Forensics (DIF) is a field that defines the accuracy of digital images in terms of both the integrity of the image content and its location. Active and force majeure correction detection methods are two algorithms for detecting fake images in DIF. Force majeure fake discovery systems do not require prior knowledge of the image content. Good fashion requires placing watermarks and digital signatures on images and proving their authenticity. Therefore, any modification to the image can destroy the embedded watermark and digital text, thus helping to find the use of the image. Copying (cloning) modification of the system is irresistible to fake images, which have the greatest impact on the original image.

Owing to the quick advancement of digital image processing technologies and the rising acceptance of digital recording devices, even a novice user can now perform digital image processing quite easily. With today's digital image processing software, anyone can create alterations made to digital photos so that it will be nearly hard to tell a fake from the real thing visually. The media has been using distorted digital images more frequently in recent decades, and this has led to ongoing discussions concerning the veracity of the information being presented. Artificial changes, distortions or attacks refer to the deliberate alteration of image content with the aim of hiding or distorting its content.

The rest of the paper is organized as follows. Section 2 details the literature survey. The proposed method is described in section 3. The outcome and application is discussed in section 4. Conclusion and future scope are summarized in section 5.

II. LITERATURE SURVEY

The vast amount of publications devoted to creating defenses against such attacks shows that the presented embedding distortion methods are currently the most widely used. The majority of techniques currently in use in the literature involve the extraction of explicit features like statistical, geometrical, wavelet, block, key

point, transformation, texture, and so forth. In [1], the authors work with Digital Image Forgery Detection Using Deep Learning Approach. The goal was to classify the image patches as either original or forged. During the training stage, patches were carefully selected from original image regions and the borders of embedded splicing. These patches served as input for the network, which then produced classification results. In the testing stage, the same methodology used for training is applied to extract patches, and the final decision on image classification was made by majority voting among the patches belonging to either the first or second class. Impressively, the experiment results showed a high classification accuracy. The fine-tuned model achieved 97.8% accuracy, while the zero-stage trained model achieved 96.4% accuracy. These results were obtained by evaluating set of images containing artificial distortions, and they outperformed existing solutions. The CASIA dataset was used for the experimental research.

Paper [2] discusses about the Image Forgery Detection Using a Convolutional Neural Network (CNN) Model Trained on a Pre-trained AlexNet Model. This method was designed to detect and pinpoint forged components in modified photographs. The deep features of a CNN based on the pre-trained AlexNet model was used and, these deep characteristics proved to be efficient and successful which was tested using the publicly accessible benchmark dataset MICC- F220.

The authors in [3] suggested a lightweight and efficient model for picture forgery detection in their work. The main contribution was the creation of deep learning-based system for detecting picture forgeries, especially in the setting of double image compression. The suggested model was trained to detect the presence of forgeries. The experimental findings were impressive, with an overall validation accuracy of 92%. Image splicing and copy-move image forgeries were successfully identified using the suggested approach. In [4], the authors brief a methodology for improving the robustness of picture forgery detection. The Compressed Image Robust Forgery Detection Using CNN Surveillance. Images accessible on internet sharing platforms are frequently modified, including global alterations such as compression, resizing, or filtering. Detecting these frauds can be difficult. The fundamental feature of the framework is that it takes into account the image quality particular to the application at hand. A Camera Identification model based on convolutional neural networks (CNNs) is used to do this. This CNN model is trained using a combination of compressed and uncompressed pictures of varying quality.

Image Forgery Detection with the use Error Level Analysis and Deep Learning is presented in [5]. Determination of whether an image has been manipulated, forensic analysis can be conducted using techniques such as Error Level Analysis (ELA) to calculate the compression ratio between original and fake image. Metadata provides insights of the document. It is crucial to remember that metadata might also be changed. Deep Learning is used to recognize image manipulations. Dataset consisting of both fake and original images is used, applying Error Level Analysis to each of the images and analyzing supporting parameters for error rate analysis aiming to accurately detect forged images. Papers [6] and [7] introduces a novel approach to detect copy move and splicing image forgery. The method utilizes CNN with three different models namely ELA, VGG19, and a pre-processing technique. The images are pre-processed at a specific compression rate and then used to train the model. The trained model classifies the images as either authentic or forged. To preprocess and analyze images at a particular compression rate, the authors [7] suggest utilizing ELA using the VGG19 model. The preprocessed photos are then utilized to train the CNN model, which determines if the images are genuine or faked. The proposed network [8] consists of five convolutional layers, two fully-connected layers, and a Softmax classifier. To train the model, the researchers utilize CASIA v1.0, a public image set that contains authentic and manipulated images. The experiment involves various types of image tampering, including splicing, retouching, and re-compressing.

Article [9] provide a learning-based system for detecting various forms of image deceptions based on an CNN architecture. Both copy-move forgeries and inpainting-based forgeries are considered. The authors emphasize the interpretability of forgery detection in addition to classification, ensuring that the CNN model distinguishes the artificial regions that contribute to

classification. In accurately classified scenarios, created regions are assessed using the Grad-CAM Heat map.

Research in [10] presents a deep learning-based approach for identifying digital picture counterfeiting. The model employs a YOLO-CNN using ResNet50v2 architecture. CASIA_v1 and CASIA_v2 benchmark datasets are used for training and testing. Further the findings show that the recommended method beats the competition and achieves excellent accuracy when using the CASIA_v2 dataset. Authors in [11] present a two-phase approach to detect altered images using machine learning techniques pointing out the challenges in differentiating between genuine and manipulated images, given the availability of sophisticated manipulation software. Paper [12] depicts that Deep learning algorithms like CNNs offer promising results in detecting image forgeries by extracting relevant features. CNNs have proven to be highly effective in handling image forgery detection tasks. What sets them apart is their ability to extract residual noise-based features. By analyzing these features, CNNs can differentiate between unaltered and manipulated images, even in the presence of sophisticated forgery techniques.

III.PROPOSED SYSTEM

The proposed system uses deep Learning technology like CNN, VGG-16 for the development of the model. The collected datasets are pre-processed and trained using deep learning algorithms. The Web Application is also developed where the user can upload image and the application will classify the result. VGG-16, a deep convolutional neural network, excels in feature extraction, capturing intricate patterns in images. When integrated with ELA, which highlights compression artifacts and inconsistencies, the combination enhances the system's ability to detect subtle manipulations or forgeries in images. This synergy leverages both ELA's strengths in identifying inconsistencies and VGG16's capacity for high-level feature recognition, resulting in a more robust and accurate forgery detection system. The system architecture comprises a Flask web application that serves as the user interface for image forgery detection as depicted in Figure 1. The application preprocesses user-uploaded images before sending them to a Convolutional Neural Network model built with TensorFlow and Keras. The CNN extracts features through convolutional and pooling layers, followed by fully connected layers for classification. To enhance interpretability, ELA is integrated, revealing regions susceptible to manipulation. The trained model classifies the uploaded image as Authenticated/Original or Tampered, accompanied by a confidence score. The entire process is orchestrated within the Flask framework, ensuring seamless communication between the user interface and the deep learning components. This architecture facilitates real-time image analysis through an intuitive web interface, making it accessible and practical for users seeking to identify instances of image forgery.

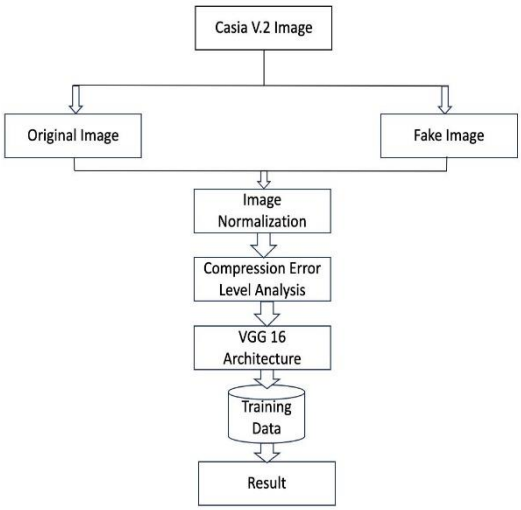

Figure. 1 System Architecture

The sequence diagram, figure 2 below details the sequence of steps that are encountered during the execution of proposed method. User collects the data, applies the algorithm, train and tests the data. After this giving an input image to get the required output

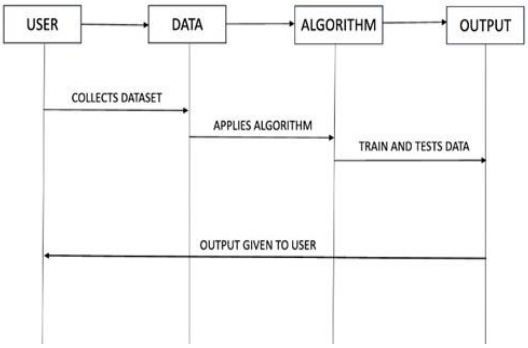

Figure 2. Sequence Diagram

Firstly, the datasets are collected for the prediction. The data sets consist of Image Forgery detection Classes. The image preprocessing technique is applied on the selected data, image resize, splitting data into Train and Test. The splitted train data are passed as input to the CNN algorithm, which helps in training. The trained skin image data is evaluated by passing test data to the algorithm, accuracy is calculated with VGG16. Once the data is trained the model is used to test data with better accuracy.

A. Methodology

In the realm of digital imagery, the need for reliable tools to identify image forgery has become increasingly crucial. To address this challenge, a novel approach has been developed—an image forgery detection system that combines cutting-edge deep learning techniques with error analysis. The proposed work will delve into the methodology behind this innovative system, highlighting its key components and explaining how it contributes to the ongoing advancements in forgery detection. At the heart of this system lies a powerful Convolutional Neural Network, seamlessly integrated into a user-friendly Flask web application. The objective is to empower users to effortlessly upload their images through the intuitive web interface, initiating a multi-step process that unravels the truth and authenticity behind the visuals. Once an image is uploaded, the system commences its investigation. The initial step involves preprocessing the image, preparing it for further analysis. Subsequently, the pre-trained CNN model comes into play, leveraging the renowned TensorFlow and Keras frameworks. This model showcases its prowess by employing convolutional and pooling layers, skillfully extracting relevant features from the image. To ensure accurate classification, fully connected layers are carefully crafted within the CNN model. To enhance the interpretability of the results, error level analysis has been incorporated into the system. Acting as a detective's magnifying glass, ELA deftly highlights regions within the image that are susceptible to manipulation. By shedding light on these areas, it provides a clearer understanding of potential tampering. The real magic happens when the trained model steps up to distinguish between authenticated/original images and those that have undergone tampering. With a confident stride, it classifies the images and accompanies the results with a handy confidence score. This score serves as a measure of certainty, offering users a deeper insight into the system's assessment. To ensure the system's accuracy and effectiveness, a meticulously curated dataset is at the core of its training and evaluation process. Performance metrics, such as accuracy and confidence scores, are meticulously analyzed to showcase the system's true potential. Through this rigorous evaluation, the system's ability to reliably detect image forgery is enhanced.

B. System Requirements

At least 8 GB of RAM is recommended to ensure smooth execution of the Flask web application and the image processing tasks performed by the CNN. Adequate storage space is necessary for the application, its dependencies, and the stored images. A minimum of 50 GB of available storage is recommended. The application heavily relies on Python for scripting and executing code. The Flask web framework is used to run the web application.

TensorFlow and Keras - these deep learning libraries play a important role in implementing and executing the CNN model. The OpenCV library is vital for performing various image processing tasks. Matplotlib, NumPy, Pandas: These libraries are used for data visualization and manipulation purposes.

C. VGG Architecture

In the VGG16 architecture as shown in figure 3, the convolutional layers (Conv blocks 1-5) progressively extract hierarchical features from input images, beginning with Conv1's detection of low-level features such as edges, colors, and textures using 64 filters with a 3x3 receptive field and ReLU activation. Subsequent layers, including Conv2 to Conv5, build upon these features, capturing more complex patterns and refining representations. The Max Pooling Layers (MaxPool blocks 1-5), represented by MaxPool1-5, contribute to spatial downsampling, enhancing computational efficiency. Fully Connected (FC) Layers, specifically FC6 and FC7, transition from spatial features to class scores through 4096 neurons with ReLU activation, while FC8 generates final class probabilities based on the number of classes.

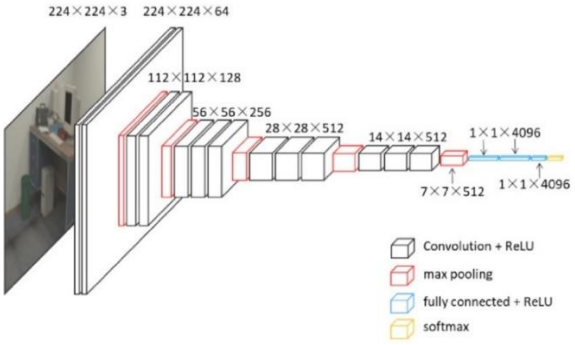

Figure 3. VGG Architecture

IV.OUTCOMES AND APPLICATIONS

Forgery detection accuracy, sensitivity and specificity, false positive and false negative rates, and visualization of detected forgeries are among the results of the work.

Forgery Detection Accuracy: Evaluate the overall accuracy of your forgery detection system using Error Level Analysis. Measure how effectively the combination of ELA and VGG16 can identify manipulated or forged regions within images.

Sensitivity and Specificity: Analyze the sensitivity and specificity of your system. Sensitivity measures the ability to correctly identify manipulated regions, while specificity assesses the system's accuracy in recognizing authentic areas.

False Positive and False Negative Rates: Examine the rates of false positives and false negatives. Determine the instances where the system incorrectly identifies authentic regions as forgeries (false positives) or fails to detect manipulated regions (false negatives).

Visualization of Detected Forgeries: Provide visualizations of detected forgeries, highlighting the manipulated regions in the images. This can help in understanding how the system identifies and marks suspicious areas.

Following are few applications to mention for image forgery detection.

Forensic Investigations: Image forgery detecting is paramount in forensic investigations, aiding experts in uncovering manipulated images to ensure the reliability of digital evidence, thereby enhancing the accuracy and integrity of criminal investigations and legal proceedings.

Digital Content Verification: Crucial for maintaining the trustworthiness of digital content, image forgery detection verifies the authenticity of images, playing a vital role in preventing the dissemination of misleading or doctored visual information across various online platforms.

Media and Journalism: Image forgery detection is a critical tool for media and journalism professionals to validate the authenticity of visual content, ensuring that published images are free from manipulation and upholding the credibility of news reporting and storytelling.

Historical Image Analysis: Image forgery detection aids historical researchers by preserving the accuracy of historical records, identifying and mitigating alterations to images, and ensuring the reliability of visual artifacts in the study and interpretation of the past.

Copyright Protection: Image forgery detection serves as a powerful tool for protecting intellectual property rights, helping to identify unauthorized alterations to images and ensuring that creators copyrights are upheld, particularly in the digital landscape where content can be easily manipulated.

V.CONCLUSION

The study explores forgery detection using CNN in a Flask web application. The combined use of deep learning and error analysis effectively distinguishes authentic from forged images. The user-friendly interface allows real-time analysis, presenting promising results. Ongoing challenges include improving model robustness and dataset diversity. The work emphasizes on the ongoing need for innovative forgery detection methods to uphold trust in evolving digital landscapes. The output is measured using the 'confidence' of the forged or original image metric for the model's performance in image forgery detection. The confidence metric is used to evaluate how well the model is able to classify images into the specified classes during training and evaluation. Continued research and development in optimizing the proposed system for real-time performance, potentially through hardware acceleration or model quantization, would expand its applicability in time-sensitive scenarios. Considering the integration of human-in-the-loop approaches, where expert feedback is incorporated into the model training and validation process, could improve the system's interpretability and decision-making.

These are a few of the work's limitations, including the

need for different methodologies, limited use of static images, and computational resources. The use of deep learning models may require significant computational resources, limiting the accessibility of the proposed system in resource constrained environments. The developed approach focuses on image forgery detection and may not seamlessly extend to video and audio formats. Video and audio manipulation present unique challenges, requiring tailored methodologies beyond the current scope of the project.

REFERENCE

[1] A Kuznetsov, "Digital image forgery detection using deep learning approach", Journal of Physics: Conference Series, 2019

[2] Amit Doegar, Maitreyee Dutta, Gaurav Kumar, "CNN based Image Forgery Detection using pre-trained AlexNet Model", Proceedings of International Conference on Computational

[3] Syed Sadaf Ali, Iyyakutti Iyappan Ganapathi, Ngoc-Son Vu, Syed Danish Ali, Neetesh Saxena and Naoufel Werghi, "Image Forgery Detection Using Deep Learning by Recompressing Images", Electronics 2022, 11, 403.

[4] Boubacar Diallo, Thierry Urruty, Pascal Bourdon, Christine Fernandez-Maloigne, "Robust forgery detection for compressed images using CNN supervision", Forensic Science International: 2020, 100112.

[5] Ida Bagus Kresna Sudiatmik, Fathur Rahman, Trisno, Suyoto, "Image forgery detection using error level analysis and deep learning", TELKOMNIKA, Vol.17, No.2, April 2019, pp.653659

[6] Devjani Mallick, Mantasha Shaikh, Anuja Gulhane and Tabassum Maktum, "Copy Move and Splicing Image Forgery Detection using CNN", ICACC-2022

[7] Wina Permana Sari, Hisyam Fahmi, "The effect of error level analysis on the image forgery detection using deep learning", Kinetik: Game Technology, Information System, Computer

[8] Network, Computing, Electronics, and Control Journal, Vol. 4, No. 3, August 2019.Na Huang, Jingsha He, Nafei Zhu, "A Novel Method Detecting Image Forgery Based on Convolutional Neural Network", IEEE, 2018

[9] Ankit Katiyar and Dr. Arnav Bhavsar, "Image Forgery Detection with Interpretability", Indian Institute of Technology Mandi, HP, INDIA, 2022

[10] Emad Ul Haq Qazi, Tanveer Zia and Abdulrazaq Almorjan, "Deep Learning-Based Digital Image Forgery Detection System", applied Sciences, 2022

[11] J.Malathi, B.Narasimha Swamy and Ramgopal Musunuri "Image Forgery Detection by using Machine Learning", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue- 6S4, April 2019

[12] Sankalp Patekar, Sumaiya Khan, Diksha Bhusare, Manish Bhujbal and Prof.Gayatri Hegde PCE New Panvel, Navi Mumbai, April 2023