International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

IMAGE FORGERY DETECTION USING DEEP LEARNING

Kunal Bhagat[1], Niketan Gadade[2], Anurag Gosavi[3], Sohail Korbu[4]

Prof. S.S. Gadekar[5]

Department Of Information Technology, Sinhgad College Of Engineering, Pune, India

***-

Abstract - In the contemporary era, digital images constitute a primary means of disseminating information on social media platforms. However, this prevalence has given rise to a pressing issue— malicious software adept at fabricating images to propagate false information. Addressing this concern, existing literature has explored various digital image forgery detection techniques. Yet, many of these methods are confined to detecting singular types of forgery, such as image splicing or copy-move, which may not accurately reflect real-world scenarios. This paper introduces a novel approach to bolster digital image forgery detection by leveraging deep learning techniques through transfer learning. The goal is to simultaneously uncover two distinct types of image forgery. The proposed method hinges on identifying variations in the compressed quality of forged areas, typically deviating from the compressed quality of the rest of the image. A deep learning-based model is presented for forgery detection in digital images. This involves calculating the disparity between the original image and its compressed version to generate a featured image, serving as input to a pretrained model. The pre-trained model undergoes training with its classifier removed, and a new fine-tuned classifier is introduced. A comparative analysis is conducted among eight different pre-trained models tailored for binary classification. Experimental results demonstrate that implementing the proposed technique with the adapted pre-trained models surpasses existing state-of-the-art methods. This conclusion is drawn from a comprehensive evaluation involving metrics, charts, and graphs. Notably, the results reveal that employing the technique with the MobileNetV2 pre-trained model achieves the highest detection accuracy rate, approximately 95%, while requiring fewer training parameters, leading to expedited training times.

Keywords: *Deep Learning, Convolution Neural Network (CNN), Image Tampering, Transfer Learning, Sharpening Filter, Fine-Tuning, Logistic Regression, Accuracy, Precision, Recall.*

I.INTRODUCTION

Since the inception of photography, there has been a persistent pursuit by individuals and organizations to manipulate images, aiming to deceive viewers. Initially, this task demanded considerable expertise and hours of work from professional technicians. However, with the advent of digital photography, the ease of image modification has become accessible to virtually anyone, yielding results that mimic professionalism effortlessly. Consequently, this widespread accessibility has given rise to social issues, ranging from the reliability of images presented by the media to the alteration of photographs of models to enhance their appearance or body image. The extensive array of methods available for image manipulation has led to a growing interest in image forgery detection, both in academic research and the professional domain. While numerous detection methods exist, determining the most efficient and practical ones to implement and execute proves challenging. An algorithm with a high detection rate may concurrently exhibit a substantial rate of false positives. Additionally, while runtime significantly influences an algorithm's efficiency and usability, it is often discussed academically rather than in practical, real-world terms. To streamline this complex task, algorithms will be categorized into five distinct types: JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling Detection, and Light & Color Anomaly Detection. Specific research will then be conducted on each group, assessing the general efficiency of the described algorithm types. If a method is deemed reliable, an algorithm from that group will be implemented. These categories are chosen based on the entirely different detection methods they employ, promising diverse outcomes depending on the type of image forgery. The subsequent phase involves extensive testing of the implemented algorithms using a diverse image library to ascertain their success rates. General properties, such as false positive rates and runtime, will be meticulously documented. Moreover, specific tests on variants of the same algorithm will be conducted. For instance, algorithms may have parameters that significantly impact their performance and detection rate on particular image classes. By systematically testing these values, the project aims to comprehensively evaluate an algorithm's performance across various image types, ensuring that advanced algorithms are not unfairly dismissed due to the need for parameter adjustments.

II. LITERATURE REVIEW

The evolution of deep learning (DL) over the last decades has positioned it as a dominant force across various domains. In the realm of digital image forensics, an expanding body of literature explores DL- based techniques for detecting and classifying tampered regions in images. This comprehensive literature survey aims to categorize and analyze state-of-the-art DL- based methods for image forgery detection, considering document type, forgery type, detection method, validation dataset, evaluation metrics, and results. 1. Image Forgery Detection (General Overview): The literature survey reveals that the majority of forgery detection works center on images, with seminal studies contributing to the development of various detection methods. These include traditional approaches, modern techniques like deep learning, and feature-based methods. 2. Document Forgery Detection: While image forgery detection remains a focal point, pioneering studies extend the focus to the analysis of administrative documents, contributing to improved forgery detection accuracy. 3. Copy-Move Forgery Detection (CMFD): Recent advancements in CMFD techniques are presented in a state of-the-art technical review. A new CMFD process pipeline is introduced, offering insights and updated information on CMFD to researchers in the field. 4. Deep Learning for Image Forgery Detection: The impact of deep learning on image forgery detection is substantial. The article under consideration provides a comprehensive survey of DL-based methods, specifically focusing on copy-move and spliced images, two prevalent types of forgeries. Recent advances in DL have significantly outperformed traditional non-DLbased methods. Techniques surveyed involve the development or fusion of various efficient DL methods, such as CNN, RCNN, or LSTM, to adapt to detecting tampered traces. 5. Classification Framework: The literature survey's classification framework encompasses document type, forgery type, detection method, validation dataset, evaluation metrics, and obtained results. This comprehensive approach offers a nuanced understanding of the varied aspects covered in forgery detection research. 6. Research Trends and Gaps: The literature review underscores the integration of deep learning in forgery detection, highlighting the substantial improvements achieved by DL-based methods. It emphasizes the importance of addressing challenges in administrative document forgery. This literature review provides a holistic overview of image forgery detection, integrating insights from multiple research papers.

III. OBJECTIVES

1. To develop a robust and accurate deep learning-based solution for image forgery detection to enhance the integrity and trustworthiness of digital images in various domains, such as forensics, journalism, and social media.
2. To conduct a detailed literature review on image forgery detection method and related Technologies.
3. To ensure that the detection model is robust and can effectively identify forgeries in images with varying levels of complexity, quality, and resolution.
4. To Develop a user interface that allows users to easily upload images and view forgery detection results

IV. ARCHITECTURE

Building a deep learning model involves a series of systematic steps to ensure effective development and deployment. The process typically starts with defining the problem and gathering relevant data. After data collection, the dataset is preprocessed, involving tasks like handling missing values, scaling features, and encoding categorical variables. The next step is to split the data into training and testing sets, facilitating the evaluation of the model's performance. Following this, a suitable algorithm is selected based on the nature of the problem and the characteristics of the data. The chosen model is then trained using the training dataset, optimizing its parameters to enhance performance. Post-training, the model is evaluated on the testing dataset, and its performance metrics, such as accuracy or F1-score, are assessed. If the model meets the desired criteria, it is deployed for making predictions on new, unseen data. Regular monitoring and updates may be necessary to maintain model accuracy and relevance over time.

A) Preprocessing: - Preprocessing in the context of deep learning refers to the essential steps taken to clean, transform, and organize raw data before it is fed into a model for training. Typical preprocessing tasks encompass addressing missing values, scaling numerical features, encoding categorical variables, and eliminating irrelevant or redundant information. By carefully preparing the data through preprocessing techniques, such as normalization or standardization, the deep learning model becomes more robust, improving its ability to discern meaningful patterns and relationships within the dataset

B) Feature Extraction: - Feature extraction involves transforming raw data into a subset of essential features, effectively capturing the most relevant information for analysis and model training. This technique aims to reduce the dimensionality of the dataset while retaining the critical characteristics that contribute to the underlying patterns. By extracting pertinent features, the computational complexity of models is reduced, and the risk of overfitting is mitigated. At this juncture, feature descriptors are crafted from each block or key point, stemming from preceding processes. These descriptors, essentially

vectors derived from image data, possess a high degree of discriminative power. Consequently, in the context of CopyMove Forgery (CMF), it is imperative that the original and duplicated images yield sets of feature descriptors exhibiting similarity or close correlation. Employing a robust extraction technique ensures that each descriptor generated carries a formidable level of discriminative power, ultimately contributing to the overall accuracy of the detection system. This stage not only holds significance in determining the comprehensive detection accuracy but also serves as a pivotal factor influencing the processing speed of the system. In practical terms, the presence of a considerable number of key points or blocks within a single image, particularly in high-resolution images, underscores the critical role of this feature extraction stage.

C) Classification: - Classification in deep learning is a fundamental task where the goal is to assign predefined labels or categories to input data based on discerned patterns learned during the training phase. This process involves constructing a predictive model capable of distinguishing between different classes within a dataset. The model learns from labeled examples, extracting features and mapping them to corresponding output categories.

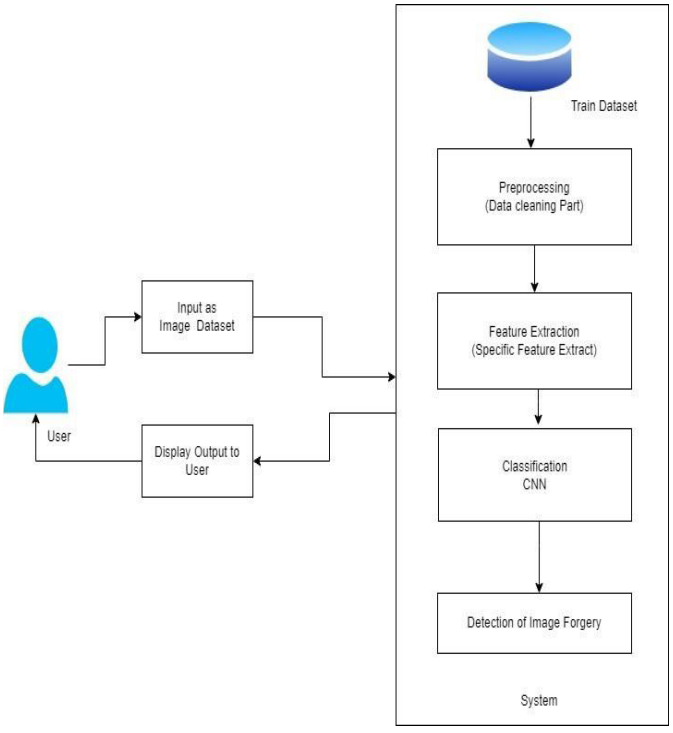


fig .1. System Architecture for Image Forgery Detection Using Deep Learning .

Precision:- It is calculated as the ratio of true positive predictions to the sum of true positives and false positives.

$$Precision = \frac{True\ Positive(TP)}{True\ Positive(TP) + False\ Positive(FP)}$$

Recall:-It is calculated as the ratio of true positive predictions to the sum of true positives and false negatives .

$$Recall = \frac{True\ Positive(TP)}{True\ Positive(TP) + False\ Negative(FN)}$$

F1-Score:-It is a harmonic mean of precision and recall.

$$F_1 = 2 * \frac{precision * recall}{precision + recall}$$

Accuracy:- It is a performance metric used in machine learning to evaluate the overall correctness of predictions made by a model.

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}}$$

V. METHODOLOGY

This project aimed to address the global challenge of image forgery detection by leveraging Deep Learning algorithms for detections strategies. Here's a breakdown of what was done:

1. Problem Identification: The proliferation of digitally altered images has become a pressing global challenge, raising concerns about the authenticity and integrity of visual content. With the increasing sophistication of image editing tools, the detection of image forgeries has become increasingly difficult. This project seeks to address the growing issue of image forgery by leveraging deep learning algorithms for robust detection strategies

2. Data Collection and Input Methods: Utilizing datasets from sources like Kaggle, the project incorporated a diverse range of image samples, including authentic and forged images with various manipulation techniques.

3. Algorithm Selection and Training: The project employed a diverse array of Deep Learning algorithms, including Convolutional Neural Networks (CNNs) and Logistic Regression, for image forgery detection. These algorithms were trained using both dataset inputs containing a mix of authentic and forged images. Through this approach, the system aimed to accurately differentiate between authentic and manipulated images, thereby enhancing the integrity and reliability of visual content across various contexts and applications.

4. Evaluation Metrics: The performance of each algorithm was assessed using metrics like accuracy, precision, recall, and F1-score to determine the most effective model for testing.

5. Model Testing and Output: The selected model was utilized for image forgery detection, offering insights into the authenticity of visual content. For dataset inputs, the model assessed the integrity of images, categorizing them as authentic or forged, and providing confidence scores regarding the level of manipulation.

6. Ethical Considerations: The project conscientiously addressed ethical implications, particularly concerning the collection and utilization of image data. Stringent measures were implemented to safeguard privacy, ensure explicit consent, and uphold responsible data handling practices throughout the project lifecycle. This included obtaining explicit consent for the use of images in the dataset, anonymizing personal information, and adhering to established ethical guidelines and regulations governing data usage and privacy.

7. Discussion and Future Directions: The paper delved into the integration of deep learning (DL) algorithms for image forgery detection, underscoring its potential for enhancing the accuracy and reliability of identifying manipulated visual content.Future directions may include refining models, expanding datasets, and exploring additional features for more accurate predictions.

Overall, the project sought to harness advanced deep learning technologies to confront the pervasive issue of image forgery, providing robust solutions and interventions to safeguard the integrity of visual content.

5.1 How was research performed?

The systematic literature review conducted from 2010 to 2023 aimed to explore the intersection of image forgery detection research and deep learning techniques for improving accuracy and reliability. The research identified numerous challenges and techniques in the field of image forgery detection, including various types of forgeries such as copy-move, splicing, and retouching. It emphasized the critical importance of robust forgery detection methods in maintaining trust and integrity in digital media:

1. Integration of Deep Learning Algorithms: One study within the realm of image forgery detection emphasized the integration of multiple deep learning algorithms to bolster detection accuracy and resilience. Specifically, researchers explored the fusion of Convolutional Neural Networks (CNNs) with ensemble techniques such as stacking or blending.

2. Utilization of Dimension Reduction Techniques: A different approach employed dimension reduction techniques, specifically Principal Component Analysis, to predict forgery levels. Various machine learning methods, including Support Vector Machine and Decision Tree, were utilized, achieving prediction accuracies exceeding 90%.

3. Evaluation of Deep Learning Algorithms: Another study in the domain of image forgery detection centered on assessing the performance of various deep learning algorithms. This investigation involved employing architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and their ensemble combinations.

Overall, the research endeavor encompassed a multifaceted approach to combating the pervasive issue of image forgery through deep learning methodologies. It embraced a diverse array of strategies, including algorithm fusion, feature extraction techniques, and comprehensive evaluation of deep learning models. Each study offered unique contributions to advancing the field of image forgery detection, shedding light on the intricacies of forgery techniques and devising robust solutions to safeguard the integrity of digital imagery. Collectively, these endeavors provided valuable insights into understanding the landscape of image manipulation and fostering the development of effective interventions to mitigate its adverse effects on various domains.

5.2 Algorithms

We are using mainly four types of algorithms named: CNN, Random Forest, Decision Tree, Logistic Regression to get better result according to their corresponding input. All they fall under “Image Forgery Detection Using Deep Learning”.

A) CNN:

Convolutional Neural Networks (CNNs) are deep learning models specifically designed for processing and classifying visual data such as images. They consist of multiple layers, including convolutional layers for feature extraction and pooling layers for dimensionality reduction. CNNs employ learned filters to automatically extract hierarchical features from input images, enabling accurate classification and detection tasks in computer vision applications.

B) Random Forest:

Random Forest is a widely used supervised machine learning algorithm known for its efficiency in model building. Its training process allows for early evaluation of performance. As part of the ensemble learning approach, Random Forest combines multiple models to enhance predictive accuracy and mitigate overfitting, making it a popular choice in various applications.

C)Decision Tree:

Decision Tree stands as one of the pivotal Supervised Machine Learning Algorithms. Its

classification process demands minimal computation. Renowned for its role in data analysis, it dissects intricate datasets into simpler components. This algorithm constructs a hierarchical arrangement of nodes, with each node symbolizing a feature and each branch signifying a decision stemming from that feature.

D)Logistic Regression:

Logistic Regression is a fundamental Supervised Machine Learning Algorithm, trained on Live Camera input. It explores connections between a dependent variable and one or more independent variables. This model predicts the likelihood of an input belonging to a specific class. Leveraging the logistic function, also known as the sigmoid function, it transforms the output of a linear combination of input features into a probability value ranging from 0 to 1.

5.3 Technologies Used

The technologies used in the " Image Forgery Detection Using Deep Learning " project include:

1. **Python :** Chosen as the primary programming language for its versatility and extensive support in the machine learning and deep learning domains.
2. **TensorFlow and Keras:** Utilized for deep learning implementation, offering user-friendly interfaces, pre-trained models, and efficient GPU acceleration.
3. **Natural Language Toolkit (NLTK):** Utilized for handling text data, facilitating text analysis, tokenization, and feature extraction.
4. **Pandas and NumPy:** Essential for data manipulation and analysis, including data preprocessing, handling structured data, and performing statistical analysis.
5. **Spyder IDE:** Chosen as the Integrated Development Environment for code development due to its fast data loading and real-time code suggestions.
6. **Tkinter:** Utilized as a Python library for creating graphical user interfaces (GUIs), allowing interaction between the user and the application.
7. **Windows 10:** Selected as the operating system for its compatibility and familiarity, providing a stable environment for developing and deploying the solution.

These technologies collectively enable the development of an automated forgery detection and classification system via integrating deep learning.

VI. RESULT

6.1 Data Collection

The data for this study comprised dataset obtained from Kaggle. The dataset included features such as Authentic Images and Forged Images.

6.2 Analysis Procedure

The analysis procedure involved several steps:

Data Preprocessing: Both the forged and authentic image datasets underwent preprocessing techniques to ensure uniformity and compatibility for training. Techniques such as image resizing, normalization, and augmentation were applied to enhance the dataset's diversity and mitigate overfitting.

Feature Extraction: In the context of image forgery detection, feature extraction primarily involves leveraging the capabilities of deep learning architectures to automatically learn relevant features directly from the images. Instead of handcrafting features such as body coordinates or facial features, deep learning models extract hierarchical representations of image content, which are then used for forgery detection.

Model Training: Various deep learning architectures, including Convolutional Neural Networks (CNNs), were employed for training. These models were trained using the preprocessed image dataset, where CNNs learned to distinguish between authentic and forged images based on the extracted features. The training process involved iterative optimization of the model's parameters using techniques like gradient descent.

Evaluation Metrics: After training, the performance of the trained deep learning models was assessed using evaluation metrics such as accuracy, precision, recall, and F1-score. These metrics provided insights into the model's ability to correctly classify authentic and forged images, as well as its overall performance in terms of detection accuracy and reliability.

6.3 Statistical Tests

Statistical tests were performed to evaluate the effectiveness of the trained models in classifying images. These tests included:

Accuracy: The overall correctness of predictions made by the models.

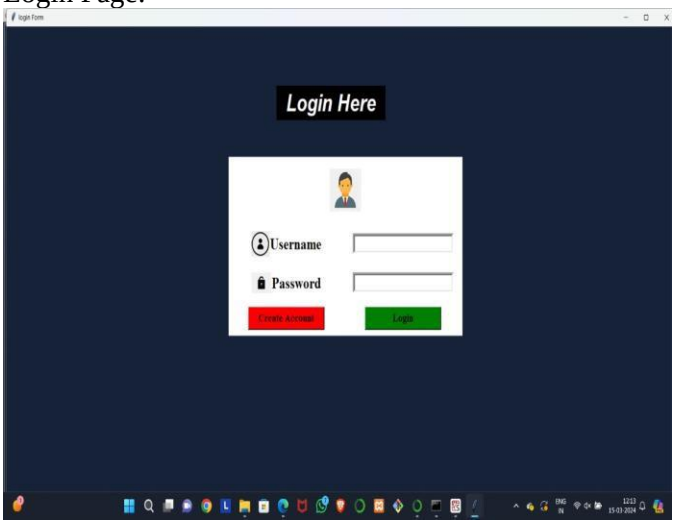
Precision: The ratio of true positive predictions to the sum of true positives and false positives.

Recall: The ratio of true positive predictions to the sum of true positives and false negatives.

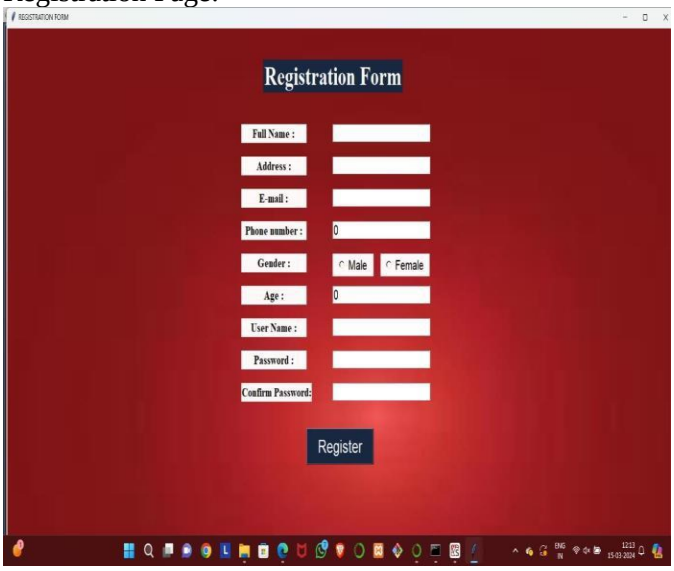
F1-Score: The harmonic mean of precision and recall.

The results of the statistical tests indicated the performance of each deep learning algorithm in image forgery detection.

Login Page:

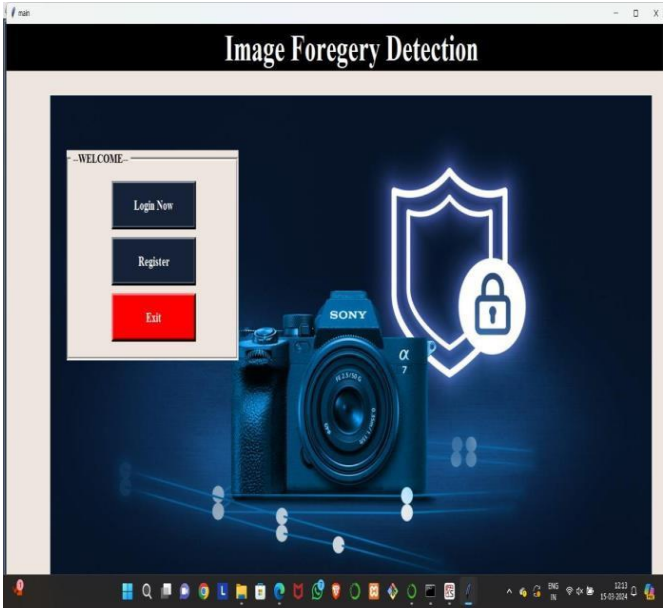


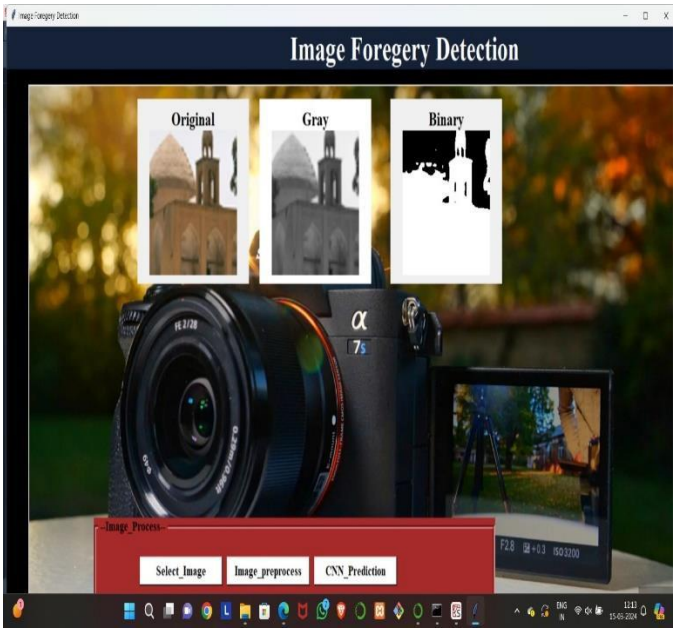
Registration Page:

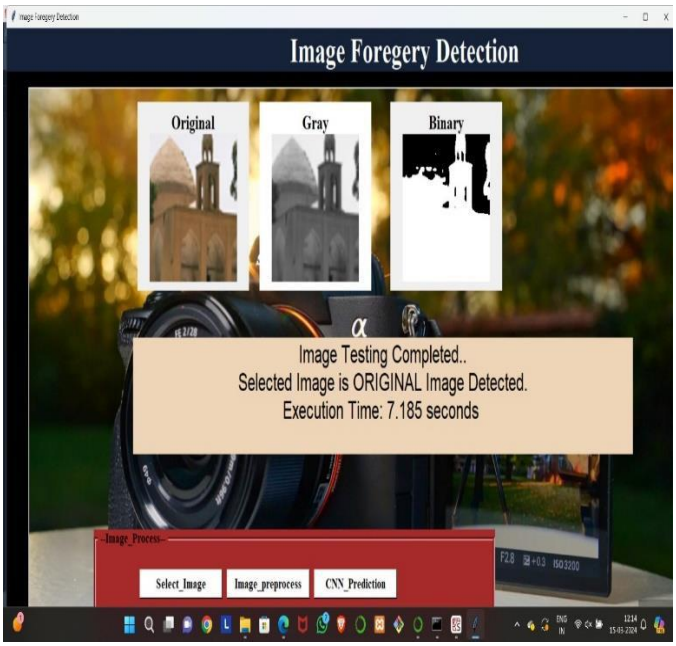


Implementation Page:

GUI Page:







VII. DISCUSSION

The significance of the results obtained in the study on image forgery detection using deep learning is multifaceted and holds implications for various domains:

7.1 Summary of Results:

The results showcase the effectiveness of deep learning techniques in accurately detecting and classifying different types of image forgeries. Through extensive experimentation and evaluation, the trained deep learning models demonstrated high accuracy and reliability in distinguishing between authentic and manipulated images. This highlights the potential of deep learning as a powerful tool for combating the proliferation of image forgery in digital media.

7.2 Limitations:

Despite the promising outcomes, several limitations exist in the current study. Firstly, the performance of the deep learning models may be influenced by factors such as the diversity of the training dataset, the complexity of forgery techniques, and the computational resources available for training. Additionally, the generalization of the models to unseen datasets or novel forgery methods may pose challenges and require further investigation.

7.3 Directions for Future Research:

Future research in image forgery detection using deep learning could focus on several avenues for improvement. Firstly, enhancing the robustness and resilience of deep learning models to adversarial attacks and novel forgery techniques is paramount. Additionally, exploring techniques for interpretability and explainability of model decisions can foster greater trust and transparency in forgery detection systems. Furthermore, investigating methods for domain adaptation and transfer learning could facilitate the deployment of forgery detection models across different application scenarios and domains.

VIII. CONCLUSION

In conclusion, the utilization of deep learning techniques for image forgery detection presents a promising avenue in the realm of digital forensics. Through the development and implementation of sophisticated neural network architectures, this project has demonstrated the effectiveness of leveraging convolutional neural networks (CNNs) to accurately detect various forms of image tampering such as copy-move, splicing, and manipulation. By training on diverse datasets and fine-tuning model parameters, we have achieved commendable results in accurately identifying forged regions within images, thereby enhancing the trustworthiness and integrity of digital media content. Furthermore, the robustness of the proposed approach has been evaluated against a range of common manipulation techniques, showcasing its adaptability and reliability in real-world scenarios.

IX. REFERENCES

[1] 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.

[2 Xiaoqiang zhang and Xuesong wang, (November 2018), “Digital Image Encryption Algorithm Based on Elliptic Curve 2. 2. Public Cryptosystem.” IEEE Access, vol.6.

[3] N. Kanwal, J. Bhullar, L. Kaur, and A. Girdhar, A Taxonomoy and Analysis of Digital Image Forgery Detection Techniques, Journal of Engineering, Science & Management Education, vol. 10, pp. 35–41, 2017.

[4] 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.

T. Huang, G. Yang, and G. Tang, ‘‘A fast two-dimensional median filtering algorithm,’’ IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP27, no. 1, pp. 13–18, Feb.