

# DAYANANDA SAGAR UNIVERSITY

Devarakaggalahalli, Harohalli  
Kanakapura Road, Ramanagara-562112, Karnataka, India



**SCHOOL OF  
ENGINEERING**

**Bachelor of Technology  
in  
COMPUTER SCIENCE AND ENGINEERING**

## **Major Project Phase-II Report**

**IMAGE FORGERY DETECTION USING DEEP LEARNING**

**Batch: 57**

By

**Ekta Agarwal – ENG20CS0096**

**Gauthami CS – ENG20CS0104**

**K Jahnavi – ENG20CS0137**

**Under the supervision of  
Prof. Veena M  
Assistant Professor, Dept. Of CSE**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,  
SCHOOL OF ENGINEERING  
DAYANANDA SAGAR UNIVERSITY,  
BANGALORE**

**(2023-2024)**



# DAYANANDA SAGAR UNIVERSITY



**SCHOOL OF  
ENGINEERING**

## **Department of Computer Science & Engineering**

Devarakaggalahalli, Harohalli, Kanakapura Road,  
Ramanagar – 562112, Karnataka, India

## **CERTIFICATE**

This is to certify that the Major Project Stage-II work titled “**IMAGE FORGERY DETECTION USING DEEP LEARNING**” is carried out by **Ekta Agarwal (ENG20CS0096), Gauthami C S (ENG20CS0104), K Jahnavi (ENG20CS0137)**, bonafide students of eighth semester of Bachelor of Technology in Computer Science and Engineering at the School of Engineering, Dayananda Sagar University, Bangalore in partial fulfillment for the award of degree in Bachelor of Technology in Computer Science and Engineering, during the year **2023-2024**.

<b>Prof. Veena M</b> Assistant Professor Dept. of CSE, School of Engineering Dayananda Sagar University  Date:	<b>Dr. Girisha GS</b> Chairman CSE School of Engineering Dayananda Sagar University  Date:	<b>Dr. Udaya Kumar Reddy KR</b> Dean School of Engineering Dayananda Sagar University  Date:
--	---	---

**Name of the Examiner**

**Signature of Examiner**

- 1.
- 2.

# DECLARATION

We, **Ekta Agarwal (ENG20CS0096), Gauthami C S (ENG20CS0104), K Jahnavi (ENG20CS0137)**, are students of eighth semester B. Tech in **Computer Science and Engineering**, at School of Engineering, **Dayananda Sagar University**, hereby declare that the Major Project Stage-II titled “**Image forgery detection using Deep Learning**” has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Computer Science and Engineering** during the academic year **2023-2024**.

**Student**

**Signature**

**Ekta Agarwal:**

**ENG20CS0096:**

**Gauthami C S:**

**ENG20CS0104:**

**K Jahnavi:**

**ENG20CS0137:**

**Place: Bangalore**

**Date:**

## ACKNOWLEDGEMENT

*It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for the successful completion of this project work.*

*First, we take this opportunity to express our sincere gratitude to School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor's degree in this institution.*

*We would like to thank **Dr. Udaya Kumar Reddy K R, Dean, School of Engineering & Technology, Dayananda Sagar University** for his constant encouragement and expert advice.*

*It is a matter of immense pleasure to express our sincere thanks to **Dr. Girisha G S, Department Chairman, Computer Science and Engineering, Dayananda Sagar University**, for providing right academic guidance that made our task possible.*

*We would like to thank our guide **Veena M Assistant Professor, Dept. of Computer Science and Engineering, Dayananda Sagar University**, for sparing her valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.*

*We would like to thank our **Project Coordinator Dr. Meenakshi Malhotra and Prof. Mohammed Khurram J** as well as all the staff members of Computer Science and Engineering for their support.*

*We are also grateful to our family and friends who provided us with every requirement throughout the course.*

*We would like to thank one and all who directly or indirectly helped us in the Project work.*

# TABLE OF CONTENTS

	Pages
LIST OF ABBREVIATIONS.....	V
LIST OF FIGURES.....	VI
ABSTRACT.....	VII
CHAPTER 1 INTRODUCTION.....	1
1.1. OBJECTIVES.....	2
1.2. DEEP LEARNING .....	3
1.2.1. SIGNIFICANCE IN DETECTING IMAGE FORGER.....	3
1.2.2. CHALLENGES IN DETECTING IMAGE FORGERY.....	4
1.3. SCOPE.....	5
1.3.1 SOCIAL IMPACT .....	6
1.3.2 ENVIRONMENTAL IMPACT .....	6
CHAPTER 2 PROBLEM DEFINITION.....	7
CHAPTER 3 LITERATURE SURVEY.....	8
CHAPTER 4 PROJECT DESCRIPTION.....	11
4.1. PROPOSED DESIGN.....	11
4.2. DATASET DESCRIPTION.....	12
4.3. ASSUMPTIONS AND DEPENDENCIES.....	14
CHAPTER 5 REQUIREMENTS.....	15
5.1. FUNCTIONAL REQUIREMENTS.....	15
5.2. NON-FUNCTIONAL REQUIREMENTS.....	16
5.3. SOFTWARE REQUIREMENTS.....	17
5.4. HARDWARE REQUIREMENTS.....	17
CHAPTER 6 METHODOLOGY.....	18
CHAPTER 7 EXPERIMENTATION.....	21
7.1 TEST CASES.....	26
CHAPTER 8 RESULT AND DISCUSSION.....	28
8.1 RESULTS OF GUI.....	29
CHAPTER 9 CONCLUSION AND FUTURE SCOPE.....	32
REFERENCES.....	33

## LIST OF ABBREVIATIONS

CNN	Convolution Neural Network
YOLO	You Only Look Once
DL	Deep Learning

## LIST OF FIGURES

<b>FIGURES</b>	<b>PAGE</b>
FIG 4.1.1 Flowchart	12
FIG 4.2.1 Documents	13
FIG 4.2.2 Real or Fake Human Faces	13
FIG 7.8.1 Output of Documents	23
FIG 7.8.2 Output of Human Faces	23
TAB 8.1 Accuracy of the Model	28
FIG 8.1.1 Initial Page	29
FIG 8.1.2 Signup Option	29
FIG 8.1.3 Login Option	30
FIG 8.1.4 Home Page	30
FIG 8.1.5 Selecting the model option	31
FIG 8.1.6 Inserting the image	31



## **ABSTRACT**

In an era characterised by the widespread manipulation of digital images, ensuring the integrity and authenticity of visual content has become paramount. This project addresses the challenge of image forgery detection using deep learning techniques, specifically focusing on the YOLOv8 model. The proposed system targets three primary categories of images prone to forgery: official documents (like Aadhar cards, PAN cards, driving licenses), human faces and brand logos.

To train the forgery detection model, a diverse dataset comprising authentic and manipulated images across these categories is utilized. Leveraging the YOLOv8 architecture, the model is trained to identify and localize forged regions within images accurately. The resulting model is integrated into a user-friendly graphical interface developed using the Streamlit framework.

The graphical interface offers a seamless user experience, featuring authentication functionalities such as sign-in and sign-up options to ensure secure access. Upon accessing the system, users are presented with a range of forgery detection options, including face forgery, logo forgery and document forgery. They can upload images for analysis, and the system provides visual feedback by highlighting suspected forgery regions with bounding boxes.

Users have the flexibility to adjust the confidence threshold for the forgery detection allowing them to tailor the sensitivity of the system according to their preferences. Through this project, we aim to provide a practical solution for detecting image forgery across various contexts, empowering users to maintain the integrity and trustworthiness of digital visual content.

## CHAPTER 1: INTRODUCTION

In an era dominated by digital media, the ease of manipulating images has led to a surge in image forgery, necessitating the development of sophisticated detection techniques to maintain the integrity and trustworthiness of visual content. Image forgery detection is a vital field within digital image processing, dedicated to identifying alterations made to digital images with the intent to deceive or mislead viewers. Image forgery can take various forms, ranging from simple alterations such as cropping or resizing to more complex techniques like copy-pasting, retouching, and object insertion. These manipulations can have significant implications across diverse domains, including journalism, forensics, and digital marketing, where the authenticity and reliability of visual content are paramount.

One prevalent type of image forgery is the manipulation of photographs for deceptive purposes. For example, in the realm of journalism, forged images can be used to fabricate news stories or misrepresent events, leading to misinformation and public distrust. Consider the infamous case of the “Shark on the Streets” image circulated during Hurricane Harvey in 2017, where a digitally altered photograph purported to show a shark swimming through flooded streets. The image, although compelling, was later debunked as a forgery created using photo editing software.

In addition to journalistic contexts, image forgery detection is crucial in forensic investigations, where the authenticity of digital evidence is paramount. For instance, in criminal investigations, forged images can be used to tamper with surveillance footage or alter crime scene photos, potentially obstructing justice and impeding legal proceedings. Moreover, image forgery extends beyond photographs to encompass other types of visual content, such as digital documents and artwork. In the context of digital documents, forged signatures or altered text can have legal ramifications, leading to disputes over contracts or agreements. Similarly, in the art world, forged paintings or sculptures can deceive collectors and undermine the value of genuine artworks.

To combat the proliferation of image forgery, researchers and practitioners have developed a myriad of forgery detection technique, ranging from traditional methods to advanced deep learning algorithms. Traditional techniques typically rely on analyzing image metadata, detecting inconsistencies in pixel values, or examining geometric distortions to identify potential forgeries. However, these methods often struggle to detect sophisticated forgeries that mimic genuine images convincingly. In recent years, the advent of deep learning, particularly convolution neural networks (CNN), has revolutionized the field of image forgery detection. Deep learning-based approaches leverage the power of neural networks to automatically learn discriminative features from large datasets of authentic and manipulated images, enabling more accurate and robust forgery detection. These methods excel in detecting subtle alterations that may evade detection by traditional techniques, thereby enhancing the reliability and effectiveness of forgery detection systems.

## 1.1 OBJECTIVES:

This project aims to achieve these objectives:

- i. **Develop a deep learning-based forgery detection model:** Design and implement a You Only Look Once (YOLO) model trained to detect forged regions within digital images accurately.
- ii. **Evaluate Model Performances:** Assess the effectiveness and reliability of the forgery detection model through rigorous experimentation and evaluation using benchmark datasets and real-world image collections.
- iii. **Optimize System efficiency:** Optimize the computational efficiency and speed of the forgery detection system to ensure fast and scalable detection of the forged content while minimizing resource requirements.
- iv. **Create an Intuitive User Interface:** Develop a user-friendly graphical interface (GUI) that enables seamless interface with the forgery detection system, facilitating accessibility for end-users such as forensic analysts and multimedia professionals.

## **1.2 DEEP LEARNING:**

### **1.2.1 SIGNIFICANCE IN IMAGE FORGERY DETECTION**

The significance of deep learning in image forgery detection lies in its ability to automatically learn and extract complex patterns and features directly from image data, enabling more accurate and robust detection of forged content. Unlike traditional forgery detection methods, which often rely on handcrafted features or heuristics, deep learning algorithms, particularly convolution neural networks (CNNs), have the capacity to learn intricate representations of both authentic and manipulated images.

One of the key advantages of deep learning in image forgery detection is its adaptability and scalability. Deep learning models can be trained on large datasets of diverse images, encompassing various types of forgeries and alterations. By learning from a comprehensive dataset, deep learning algorithms can generalize well to unseen data and effectively detect forged content, even in the presence of complex manipulations.

Furthermore, deep learning-based approaches offer superior performance in detecting subtle alterations and artifacts that may be imperceptible to the human eye or traditional forgery detection methods. CNNs can automatically identify intricate patterns and anomalies indicative of image manipulation, thereby enhancing the accuracy and reliability of forgery detection systems.

Moreover, deep learning enables end-to-end learning, where the entire forgery detection pipeline, from feature extraction to classification, is learned directly from the data. This holistic approach eliminates the need for manual feature engineering and heuristic design, leading to more efficient and effective forgery detection systems.

Additionally, deep learning models can be fine-tuned and optimized for specific forgery detection tasks, allowing for flexibility and customization based on the requirements of the application. Whether detecting copy-move forgeries, splicing, retouching, or other types of manipulations, deep learning algorithms can be tailored to address the unique challenges posed by each scenario.

## 1.2.2 CHALLENGES IN IMAGE FORGERY DETECTION

### *Model complexity and training time:*

Implementing the YOLOv8 model for image forgery detection entails dealing with the complexity of the model architecture and the computational resources required for training. The YOLOv8 model comprises numerous layers and parameters, making it computationally intensive to train. As a result, optimizing the training pipeline to reduce training time while maintaining model performance becomes crucial. Balancing model complexity with training time and resource constraints poses a significant challenge in the development phase of the project.

### *Natural Variability:*

Variations in lighting conditions, camera angles, and image settings introduce natural variability in the dataset, making it challenging to accurately distinguish between genuine and manipulated images. For instance, variations in lighting can affect the appearance of forged regions, while changes in camera angles can alter the perspective of objects within the image. Addressing natural variability requires robust feature extraction techniques and model training strategies that generalize well across diverse environmental conditions and imaging scenarios.

### *Data collection, availability, and quality:*

Acquiring a comprehensive dataset of authentic and forged images across the three categories of documents, human faces, and brand logos poses a significant challenge. Ensuring the availability and quality of the dataset involves sourcing images from various sources while adhering to data privacy and copyright regulations. Additionally, accurately labeling the dataset to distinguish between authentic and forged instances is crucial but can be time-consuming and error-prone. Overcoming these challenges requires meticulous data collection strategies and rigorous quality assurance measures to ensure the reliability and representativeness of the dataset.

*Variety of Documents:*

Detecting forged documents, such as Aadhar cards, PAN cards, and driver's licenses, presents a unique challenge due to the wide variety of document types and their associated security features. Each document type may exhibit distinct forgery characteristics, requiring specialized detection algorithms tailored to the specific features of each document category. For instance, detecting forged signatures or altered text within documents requires robust document analysis techniques capable of identifying subtle alterations and anomalies. Adapting the YOLOv8 model to effectively detect forged documents across diverse document types poses a significant challenge in the project.

Addressing these challenges involves a combination of algorithmic innovations, dataset curation strategies, and optimization techniques tailored to the specific requirements of image forgery detection using YOLO in machine learning. By overcoming these challenges, the project aims to develop a robust and reliable forgery detection system capable of detecting image manipulations across various document types, human faces, and brand logos.

**1.3 SCOPE:**

The scope of our project involves developing an image forgery detection system using the YOLOv8 model and integrating it with the Streamlit framework to create a user-friendly GUI. Our goal is to deliver a robust system capable of accurately identifying forged images within documents, human faces, and brand logos. This system will benefit individuals and organizations involved in digital content verification, forensic investigations, and security applications by providing a reliable tool for detecting image forgeries with high precision and efficiency. Additionally, the project aims to contribute to the advancement of image forgery detection technology, thereby enhancing trust and integrity in digital media.

### **1.3.1 SOCIAL IMPACT:**

- **Trust and Security:** Enhances trust and security by verifying the authenticity of visual content, reducing the risk of fraud.
- **Combatting Misinformation:** Helps combat misinformation by identifying forged images, promoting factual accuracy online.
- **Legal and Forensic Applications:** Aids legal and forensic investigations by ensuring the integrity of digital evidence presented in courts.
- **Empowering Users:** Empowers users to make informed decisions about digital content, enhancing digital literacy and critical thinking skills.

### **1.3.2 ENVIRONMENTAL IMPACT:**

- **Energy Consumption:** Deep learning model training and deployment consume significant computational resources, leading to energy consumption.
- **Data Storage and Transmission:** Large-scale datasets require storage space and bandwidth for transmission, contributing to environmental footprint.
- **Sustainability Considerations:** Incorporating into system design and development can mitigate environmental impact.
- **Long-term Sustainability:** Ongoing maintenance and updates require efficient software development practices to minimize resource consumption.

## **CHAPTER 2: PROBLEM DEFINITION**

### **PROBLEM STATEMENT**

The widespread availability of advanced image editing tools had fueled a rise in digital image forgery, presenting considerable obstacles of preserving the authenticity and integrity of visual content. Traditional forgery detection methods often struggle to accurately identify and localize forged regions within images, particularly in the presence of complex manipulations. Additionally, the lack of user-friendly forgery detection tools exacerbates the problem, hindering individuals and organizations from effectively verifying the authenticity of digital images. To address these challenges, this project aims to develop an advanced image forgery detection system using the YOLOv8 model in deep learning. Integrated with a user-friendly graphical interface, the system will empower users to detect and localize forged regions within images accurately, enhancing trust, combating misinformation, and facilitating reliable verification of digital content across various domains.



## CHAPTER 3: LITERATURE REVIEW

This research investigates the difficulty faced by image modification software in distinguishing genuine photographs from altered ones in various media sources. It emphasizes the limit of standard forgery detection algorithms that rely on specific attributes and proposes deep learning techniques for extracting complex data for greater accuracy. The study's findings highlight the shortcomings of traditional approaches in detecting various tampering methods while highlighting deep learning's ability to autonomously learn intricate features critical for identifying tampered regions across multiple manipulation techniques [1].

In the digital age, widespread image manipulation via tools like Adobe Photoshop posed challenges for manual detection of forged images. This prompted a surge in digital image forensics research, particularly exploring deep learning for copy-move image forgery detection. The paper extensively reviewed conventional and deep learning-based methods, highlighting their methodologies and significance. While deep learning showed promise, challenges arose from limited databases and restricted application in copy-move forgery detection compared to other domains. Overcoming challenges in real-world image detection and handling various tampering types remains a focus for improved performance in forgery detection methodologies [2].

This paper explores image forgery detection technique crucial for preserving trust in visual media. It discusses diverse forgery types, blind detection methods, and comparative analyses of detection techniques and datasets. Despite advancements, existing methods often require human intervention and struggle to differentiate between malicious tampering and innocent editing. The need for a unified, robust detection method capable of identifying any forgery type within images is emphasized. There's potential to extend detection techniques to audio and video tampering, but improvements in deep learning-based approaches are necessary for more effective digital image forensics [3].

This article introduces an efficient deep learning-based technique for detecting copy-move forged images. The proposed algorithm initiates with the tampered image as input,

employing segmentation, feature extraction, dense depth reconstruction, and identification of tampered areas. Notably, this system enhances computational efficiency and accuracy in detecting duplicated regions. The escalating prevalence of image forgeries, particularly through copy-move methods, poses challenges in detection due to accompanying transformation attacks aiming to evade detection systems. The authors' approach, utilizing deep learning-based feature extraction, employs Simple Linear Iterative Clustering (SLIC) for segmentation, VGGNet for multi-scale feature extraction, and Adaptive Patch Matching (ADM) to achieve matched regions. The proposed method surpasses existing techniques, demonstrating effectiveness in detecting tampering despite various attacks, effectively revealing real forged regions while removing unforged areas [4].

This paper explores image forgery detection using a Convolutional Neural Network (CNN)-based pre-trained AlexNet model to extract deep features, enhancing efficiency without extensive training. Utilizing Support Vector Machine (SVM) as a classifier, the proposed approach achieves a high accuracy of 93.94% on the MICC-F220 dataset, consisting of 220 forged and non-forged images. The experiment showcases the effectiveness of deep features extracted from the pretrained model, even amidst rotational and geometrical transformations. Comparisons with existing state-of-the-art approaches demonstrate the method's robustness. Future endeavors include working on diverse benchmark forgery datasets to further evaluate and compare performance against existing techniques [5].

This study explores the escalating worries about image forgery brought on by the pervasive usage of tools for image enhancement that are also used to transmit false information. It presents a string deep learning-based method designed to detect image forgeries in situations involving double image compression. The model, which uses Convolutional Neural Network (CNN) architecture, is trained using differences between the original and recompressed images. This approach is lightweight and effective at the same time. With a validation accuracy of 92.23%, the system effectively identifies several forms of image forgeries, including copy-move and splicing techniques. Future plans call for refining the forgery localization process, managing smaller image resolutions and

image spoofing, and combining it with other localization methods for increased accuracy. Furthermore, efforts will concentrate on creating a comprehensive database of forgeries for training deep learning networks, augmenting capabilities in image forgery detection and localization [6].

This paper presents a study and classification of the most important works on image and document forgery detection, focusing on document type, forgery type, detection method, validation dataset, evaluation metrics, and obtained results. The paper highlights the increasing prevalence of digital documents use in administrations, which had made it easier for fraudsters to fabricate and use forged documents. The paper also discusses the challenges of this research field and compares proposed methods and discusses their advantages and limits [7].

The increasing prevalence of digital tools and techniques has made it challenging to detect crimes like forgery or duplication of official documents. Forgery detection is particularly difficult when the source image is unavailable, and the problem becomes more complex when detected directly with compresses digital images and fail to detect forgery within the compresses image. This research paper aims to demonstrate two unsupervised algorithms for forgery detection copy-move and copy-paste based forged scenarios directly in the JPEG compressed domain. The paper proposes a forgery detection technique for forged documents in JPEG compressed form, as many official documents are compressed and made available online. The paper also discusses the importance of developing counter technology for automatic detection of digital forgeries. The paper also discusses the challenges of detecting forgery in digital images, such as identity documents, degree certificates, university transcripts, photographs, official letters, and asset documents [8].

## CHAPTER 4: PROJECT DESCRIPTION

Our project focuses on leveraging deep learning algorithms to address two crucial tasks: image forgery detection and document verification. In the first part, we aim to detect forged images by comparing them with authentic ones, utilizing the YOLO (You Only Look Once) algorithm. We employ datasets containing images of various official documents such as Aadhar cards, PAN cards, etc., along with datasets of real or fake human faces. Through the YOLO algorithm, we aim to accurately detect and classify objects within these documents, ensuring authenticity and identifying potential forgeries. By combining these approaches, our project aims to contribute to the development of robust and reliable solutions for detecting image forgeries and verifying the authenticity of official documents, thereby enhancing security and trust in digital transactions and identity verification processes.

### 4.1 PROPOSED DESIGN

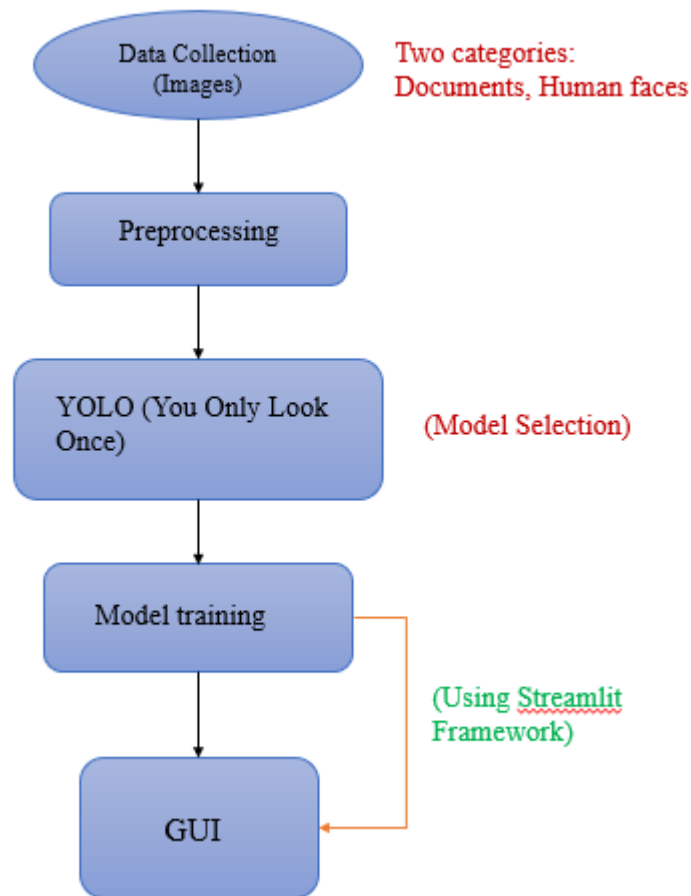
The image forgery detection process begins with the collection of a diverse dataset comprising original and tampered images across three categories: documents (e.g., PAN cards, Aadhar, DL), human faces. Preprocessing techniques are applied to clean and remove noise from the dataset. The YOLO model is then employed for identifying tampered regions within the images, trained specifically on the three datasets to enhance accuracy and robustness.

Model training entails optimizing the YOLO architecture and parameters to effectively detect forged regions while minimizing false positives. The trained YOLO model serves as the cornerstone of the forgery detection system, leveraging its real-time object detection capabilities to accurately pinpoint tampered areas within uploaded images.

Integration of the YOLO model into a user-friendly website streamlines the forgery detection process, allowing users to specify the type of image they wish to analyze (documents, faces, or logos). Upon uploading an image, the system utilizes the trained

YOLO model to detect and visualize tampered regions, providing users with actionable insights into potential image manipulations.

This streamlined approach emphasizes the efficacy of the YOLO model in detecting image forgeries across diverse categories, enhancing system adaptability and accessibility for users seeking to authenticate digital content.



**Fig 4.1.1 Flowchart**

## 4.2 DATASET DESCRIPTION

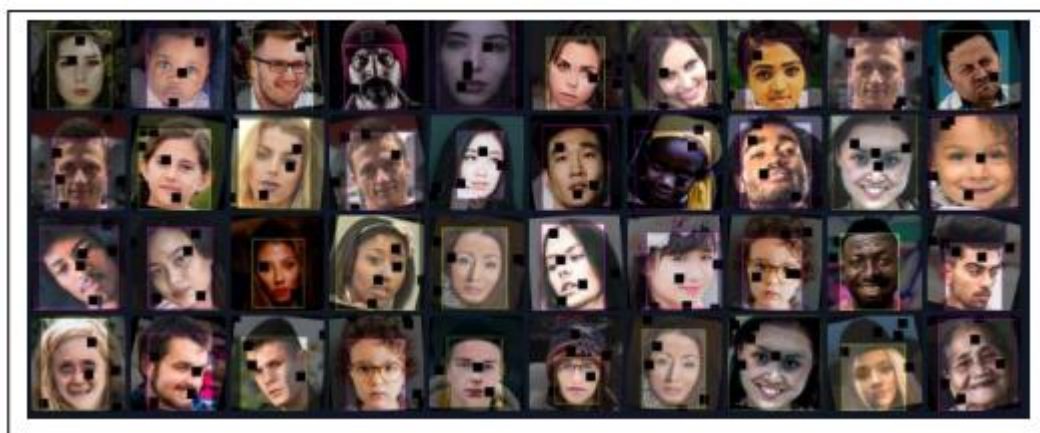
Our dataset comprises a diverse collection of images used for training YOLO deep learning model. It is trained with two distinct datasets:

**Documents Datasets:** This dataset contains images of documents, including PAN cards, Aadhar cards, PAN card and driver's licenses. The dataset consists of a total of 7,257 images formatted for YOLOv8. It is divided into training data (70%), validation data (20%), and testing data (10%).

**Real or Fake Human Faces Dataset:** With a total of 297 images formatted for YOLOv8, this dataset is designed to distinguish between real or fake human faces. The dataset distribution includes 89% for training, 11% for validation, and 0% for testing.



**Fig 4.2.1 Documents: Driving License, Aadhar, PAN Cards**



**Fig 4.2.2 Real or Fake Human face**

### **4.3 ASSUMPTIONS AND DEPENDENCIES:**

Our image forgery detection project operates under several key assumptions and dependencies to ensure its successful execution. Firstly, we assume that the datasets used for training the YOLO model contain accurately labeled images, with clear distinctions between authentic and forged samples across different categories such as human faces, logos, and documents. Additionally, we depend on the availability of sufficient computational resources, including high-performance GPUs and memory, to facilitate the training and evaluation of the YOLO model.

Moreover, we rely on the robustness and efficiency of the YOLO framework for object detection, which is essential for accurately identifying tampered regions within images. Furthermore, our project assumes access to reliable internet connectivity and cloud storage services for data management, model deployment, and website hosting. We also depend on the cooperation and participation of users for providing feedback on the system's performance, which is crucial for iterative improvements and fine-tuning of the YOLO model's detection capabilities.

## CHAPTER 5: REQUIREMENTS

### 5.1 FUNCTIONAL REQUIREMENTS:

Functional requirements outline the specific functionalities and features that a system, software, or project must possess to meet the needs and expectations of its users. These requirements serve as the foundation for design, development, and testing activities.

- a. Image Upload: Users should be able to upload images containing potential forgeries, including documents, human faces through the graphical user interface (GUI).
- b. Category Selection: The GUI should provide users with options to select the category of forgery detection they wish to perform, such as face forgery, document forgery.
- c. Forgery Detection: The system should accurately detect and localize forged regions within uploaded images, employing the YOLO (You Only Look Once) algorithm for object detection.
- d. Threshold Configuration: Users should have the ability to configure confidence threshold for forgery detection, allowing them to adjust the sensitivity of the detection algorithm based on their requirements.
- e. Visual output: The GUI will display the uploaded images with overlaid bounding boxes highlighting detected forged regions or identified objects, providing users with visual feedback on the analysis results.



## 5.2 NON-FUNCTIONAL REQUIREMENTS

- a. Performance: The system should exhibit high performance, with fast response times for image processing and forgery detection tasks, ensuring a seamless user experience even with large datasets.
- b. Scalability: The system architecture should be scalable, capable of handling increasing numbers of concurrent users and larger datasets without sacrificing performance or reliability.
- c. Reliability: The system should be reliable, with minimal downtime and robust error handling mechanisms to ensure uninterrupted operation and data integrity.
- d. Usability: The graphical user interface (GUI) should be intuitive and user-friendly, with clear navigation and informative feedback to guide users through the forgery detection process.
- e. Maintainability: The system should be easy to maintain and update, with well-organized codebase, clear documentation, and modular design to facilitate future enhancements and modifications.
- f. Compliance: The system should comply with relevant regulatory requirements and industry standards for data privacy, security and accessibility, ensuring adherence to legal and ethical guidelines.
- g. Performance Efficiency: The system should optimize resource utilization, minimizing memory and CPU usage during image processing tasks to maximize efficiency and minimize operational costs.
- h. Data Integrity: The system should ensure data integrity throughout the forgery detection process, preventing data corruption or loss and maintaining the accuracy and reliability of analysis results.
- i. User Experience: The system should prioritize user experience, providing responsive and interactive features, clear concise feedback, and customization options to enhance user satisfaction and engagement.

## 5.3 SOFTWARE REQUIREMENTS:

The software requirements are descriptions of features and functionalities of the target system. Requirements convey the expectations of users of the software product. The requirements can be obvious or hidden, known or unknown, expected or unexpected from client's point of view. It defines how the intended software will interact with hardware, external interfaces, speed of operation, response time of system, portability of software across various platforms, maintainability, speed of recovery after crashing, limitations, etc.

- Jupyter Notebook
- Google colab
- Tenserflow
- Dataset
- Operating system

## 5.4 HARDWARE REQUIREMENTS:

There are hardware requirements, also known as system requirements, for every OS we are going to use. These requirements include the minimum processor speed, memory, and disk space require to install Windows. In almost all cases, you will want to make sure that your hardware exceeds these requirements to provide adequate performance for the services and applications running on the server. Here are the minimum hardware requirements to execute this project.

- 4 GB RAM
- 8 GB HARDRIVE
- Processor: Any 3Gen + Intel processor
- IO devices: Keyboard, Mouse, Monitor
- Hard disk

## CHAPTER 6: METHODOLOGY

The proposed methodology for image forgery detection using deep learning involves collecting and annotating a diverse dataset containing government documents, face images. You Only Look Once (YOLO) V8 is employed as the primary algorithm for object detection and forgery identification. The deep learning model is trained and fine-tuned using the dataset, with techniques like transfer learning and ensemble learning utilized to optimize performance. Evaluation metrics such as accuracy, precision, recall, and F1-score are employed for validation, ensuring robustness and generalization. Finally, the trained YOLO model is deployed into a user-friendly interface for real-time forgery detection, facilitating authentication and fraud prevention in various domains.

### YOLO (YOU ONLY LOOK ONCE):

You Only Look Once (YOLO) is a revolutionary object detection algorithm that has gained significant popularity in the field of computer vision. Yolo offers a unique approach to object detection by providing real-time detection capabilities with impressive accuracy.

Traditionally, object detection algorithms involve dividing the image into multiple regions and performing classification and localization tasks separately for each region. However, YOLO takes a different approach by treating object detection as a single regression problem, predicting bounding boxes and class probabilities directly from the entire image in a single pass.

#### **The key characteristics and features of YOLO include:**

1. **Single Shot Detection:** YOLO operates on the principle of single-shot detection, which mean it predicts bounding boxes and class probabilities for objects directly from the entire image in a single forward pass of the neural network. This approach significantly improves speed and efficiency compared to traditional detection algorithms.

2. **Unified Architecture:** YOLO employs a unified architecture that combines object detection and classification tasks into a single neural network. This architecture allows YOLO to consider global context information when making predictions, leading to more accurate localization and classification of objects.
3. **Grid-based Prediction:** YOLO divides the input image into a grid of cells and predicts bounding boxes and class probabilities for objects within each cell. Each grid cell is responsible for detecting objects whose center lies within that cell, enabling YOLO to handle overlapping objects and object instances of different sizes effectively.
4. **Non-Maximum Suppression:** After predicting bounding boxes and class probabilities, YOLO applies a post-processing technique called non-maximum suppression (NMS) to filter out redundant or overlapping detections and retain only the most confident predictions. This ensures that each object is detected only once, improving the overall accuracy of the algorithm.
5. **Model Variants:** Over the years, several variants of YOLO have been developed, each with improvements in speed, accuracy and model architecture. These variants include YOLOv1, YOLOv2, YOLOv3 and the latest iteration, YOLOv4, YOLOv8, each pushing the boundaries of real-time object detection capabilities.

In summary, You Only Look Once (YOLO) represents a significant advancement in object detection technology, offering real-time performance, accuracy, and efficiency in detecting objects within images or video frames. Its unified architecture, grid-based prediction, and single-shot detection approach make it a popular choice for a wide range of computer vision applications, revolutionizing the way objects are detected and localized in visual data.

## STREAMLIT FRAMEWORK

In our Image forgery detection project, Streamlit serves as the framework for building the graphical user interface (GUI) that facilitates user interface with the forgery detection system. Here's how Streamlit is utilized in the project:

1. **User Authentication Pages:** Streamlit is utilized to design and implement the sign-in and sign-up pages, allowing users to authenticate themselves to access the forgery detection system. Streamlit's user-friendly components enable the capture of user input, such as usernames and passwords, and provide seamless navigation between authentication stages.
2. **Image Upload page:** Streamlit enables the creation of an image upload page where users can insert an image to be analyzed for forgery detection. Leveraging Streamlit's file uploader component, users can conveniently select and upload images from their local devices directly within the GUI interface.
3. **Interactive Components:** Streamlit empowers developers to integrate interactive components like buttons and sliders to enhance user experience and system functionality. Through these components, users can perform various actions such as submitting authentication requests, navigating between different GUI pages, and initiating forgery detection algorithms.

Overall, Streamlit serves as a versatile and effort for building the GUI components of the image forgery detection system, providing a seamless user experience and facilitating user interaction with the underlying forgery detection algorithms.



## CHAPTER 7: EXPERIMENTATION

In this chapter, we detailed the experimental procedures undertaken to investigate the image forgery. The aim of this experimentation was to detect whether the given image is forged or non-forged. In the following section, we provide a comprehensive method, data collection procedures and analytical techniques employed in this project.

The experimentation is done on two different datasets. The first dataset contains id proofs such as PAN card, Aadhar card and driving licence. The second dataset contains the real or fake faces of human.

YOLOv8 model is trained on both the datasets to make accurate predictions. The experimentation process includes all the steps starting from the data collection, training the model till building an user friendly GUI using streamlit framework.

1. Data Collection – Documents dataset containing PAN cards, Aadhar card and driving license taken from [universe.roboflow.com](https://universe.roboflow.com)
2. Data Collection – Real or Fake human faces dataset is also taken from [universe.roboflow.com](https://universe.roboflow.com)
3. Installing necessary modules

 `!pip install roboflow` `!pip install ultralytics`

Python pip command is used for installing modules like roboflow and ultralytics. Ultralytics is used for creating accurate model including training and deploying ML models with a np-code interface and deep learning framework support.

#### 4. Importing roboflow for managing dataset

```
!pip install roboflow

from roboflow import Roboflow
rf = Roboflow(api_key="V02Gzx4K7i3Tl1lYM0Lp")
project = rf.workspace("pavan-kumar").project("forge-eq4rh")
version = project.version(1)
dataset = version.download("yolov8")
```

#### 5. Creating a new YOLO model and loading the pretrained YOLO model for the training step.

```
# Create a new YOLO model from scratch
model = YOLO('yolov8n.yaml')

# Load a pretrained YOLO model (recommended for training)
model = YOLO('yolov8n.pt')
```

#### 6. Training the model using the document and face dataset for 20 epochs.

```
# Train the model using the dataset for 11 epochs
results = model.train(data='/content/forge-1/data.yaml', epochs=20)
```

```
# Train the model using the dataset for 11 epochs
results = model.train(data='/content/Faces-8/data.yaml', epochs=20)
```

#### 7. Evaluating the model's performance on the validation set.

```
# Evaluate the model's performance on the validation set
results = model.val()
```

## 8. Detection of forge or non-forge.



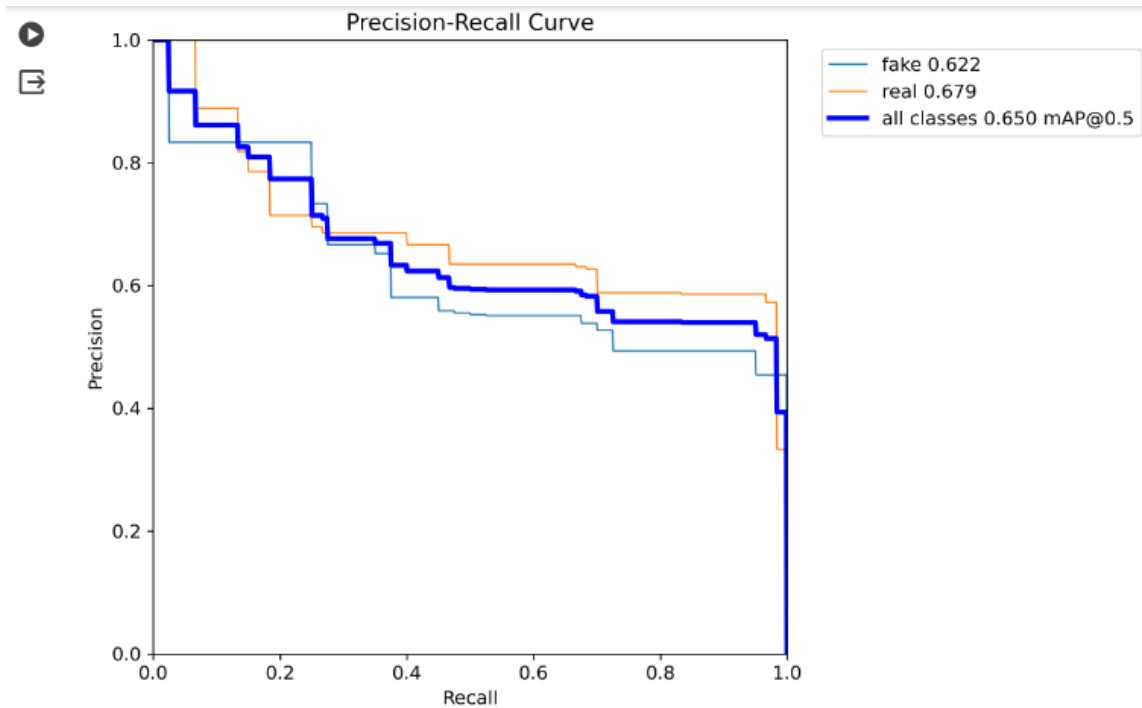
Fig 7.8.1 Output of Documents



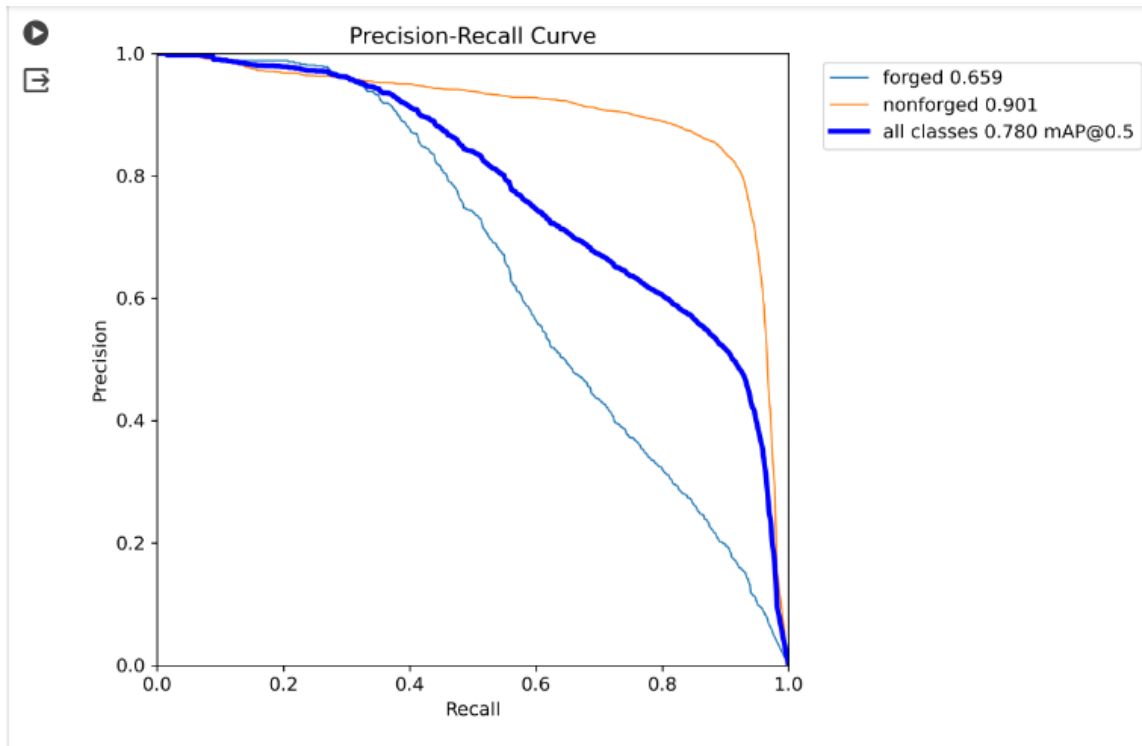


**Fig 7.8.2 Output of human faces**

9. Precision recall curve of YOLOv8 model for human face dataset.



10. Precision recall curve of YOLOv8 model for documents dataset.



As the model is giving accurate results, we have built a attractive user interface using streamlit framework.

### 11. Building a Sign-up page for the web app

```
# Function for signup page
def signup():
    st.title("Sign Up")
    new_username = st.text_input("New Username")
    new_password = st.text_input("New Password", type="password")
    if st.button("Sign Up"):
        if check_username(new_username):
            st.error("Username already exists.")
        else:
            store_credentials(new_username, new_password)
            st.success("You have successfully signed up as {}".format(new_username))
```

### 12. Building a Login page for the GUI

```
# Function for login page
def login():
    st.title("Login")
    username = st.text_input("Username")
    password = st.text_input("Password", type="password")
    if st.button("Login"):
        if authenticate(username, password):
            st.success("You are now logged in as {}".format(username))
            st.session_state.logged_in = True
        else:
            st.error("Invalid username or password.")
```

### 13. Function for Model selection

```
# Sidebar for YOLO configuration
conf = st.sidebar.slider("Confidence Threshold", min_value=0.0, max_value=1.0, value=0.5, step=0.05)

if selected_model == "Face Detection":
    model_path = 'Real_Fake.pt'
elif selected_model == "Forgery Detection":
    model_path = 'best (8).pt'
```

To run the streamlit, the command “->> streamlit run your\_script.py”.

## 7.1 TEST CASES:

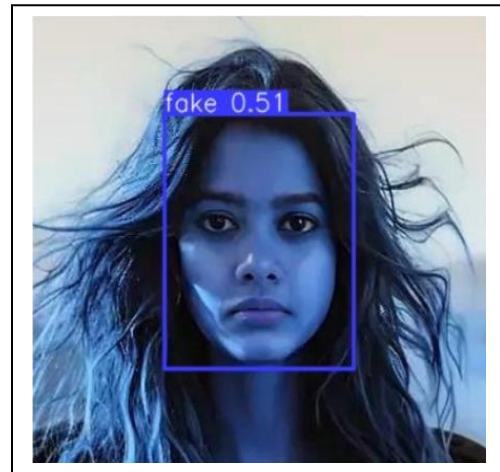
### a. Non forged documents (PAN card):



### b. Non forged face:



c. Forged image of a human face:



d. Forged documents (Aadhar card):



e. Non forged documents (Driving License):



## CHAPTER 8: TESTING AND RESULTS

**TAB 8.1 Accuracy of the model**

MODEL	DATASET(Types)	ACCURACY	RECALL	PRECISION
YOLO (You Only Look Once)	Documents	78.5%(mAP)	0.72	0.76
	Human Faces	38.5%(mAP)	0.99	0.5

From the above table (Tab 8.1), YOLO (You Only Look Once) model demonstrates varying performance across different datasets. In the documents dataset, it achieves an accuracy of 78.5% (mAP), indicating its effectiveness in identifying tampered regions within documents. The model maintains a balanced trade-off between recall (0.72) and precision (0.76), suggesting its capability to accurately detect instances of forgery while minimizing false positives. Conversely, in the human faces dataset, the YOLO model achieves a high accuracy of 38.5% (mAP) with an excellent recall score (0.99), capturing nearly all instances of forgery. However, the precision score (0.5) is comparatively lower, indicating a higher likelihood of false positives. Overall, the YOLO model's effectiveness is influenced by the specific characteristics and complexities of each dataset.

## 8.1 RESULT OF GRAPHICAL USER INTERFACE (GUI)

### Forgery Detection App



**Fig 8.1.1 Initial Page**

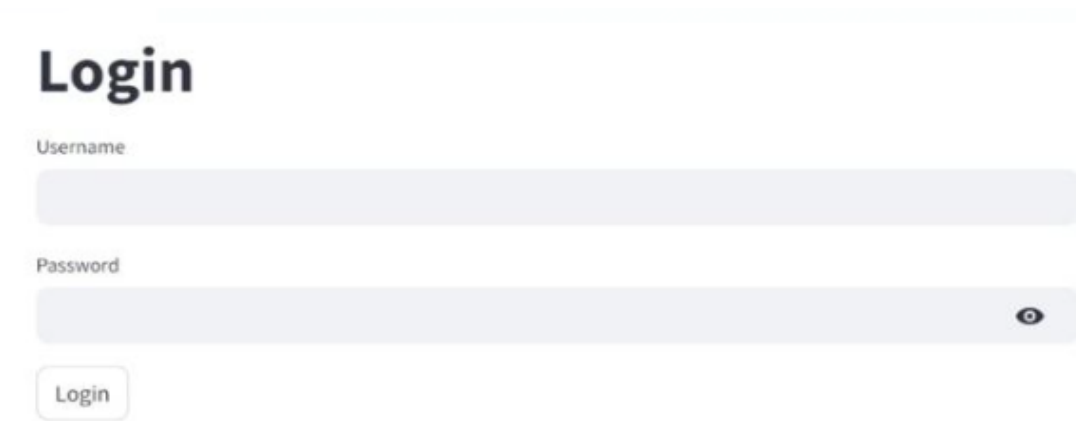
### Sign Up

New Username

New Password

Sign Up

**Fig 8.1.2 Sign Up Option**



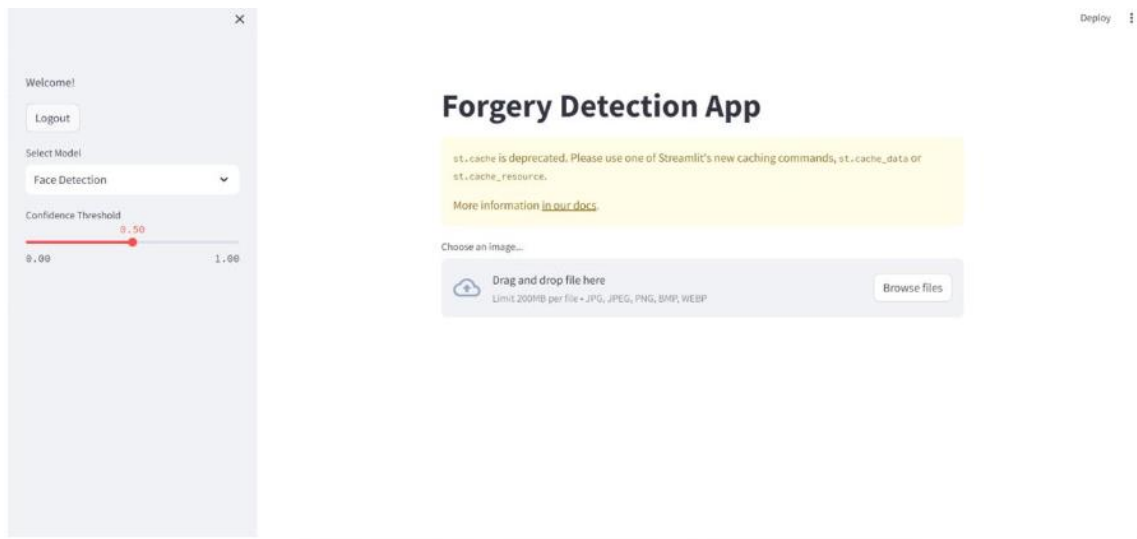
**Login**

Username

Password

Login

**Fig 8.1.3 Login Option**



Welcome!

Logout

Select Model

Face Detection

Confidence Threshold

0.50

0.00 1.00

**Forgery Detection App**

st.cache is deprecated. Please use one of Streamlit's new caching commands, st.cache\_data or st.cache\_resource.

More information [in our docs](#).

Choose an image...

Drag and drop file here

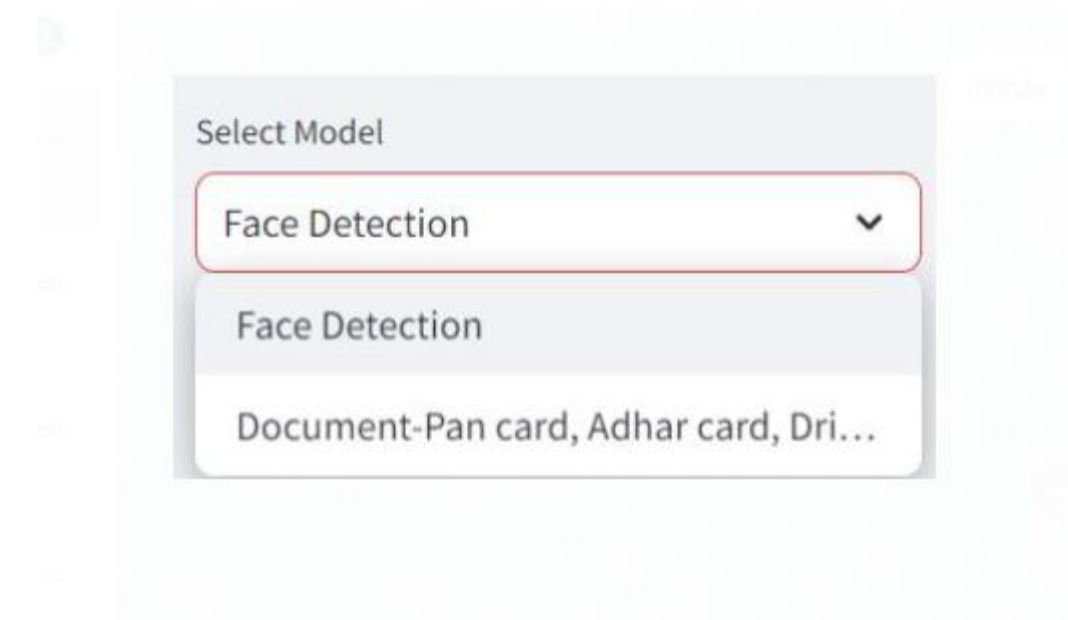
Limit 200MB per file • JPG, JPEG, PNG, BMP, WEBP

Browse files

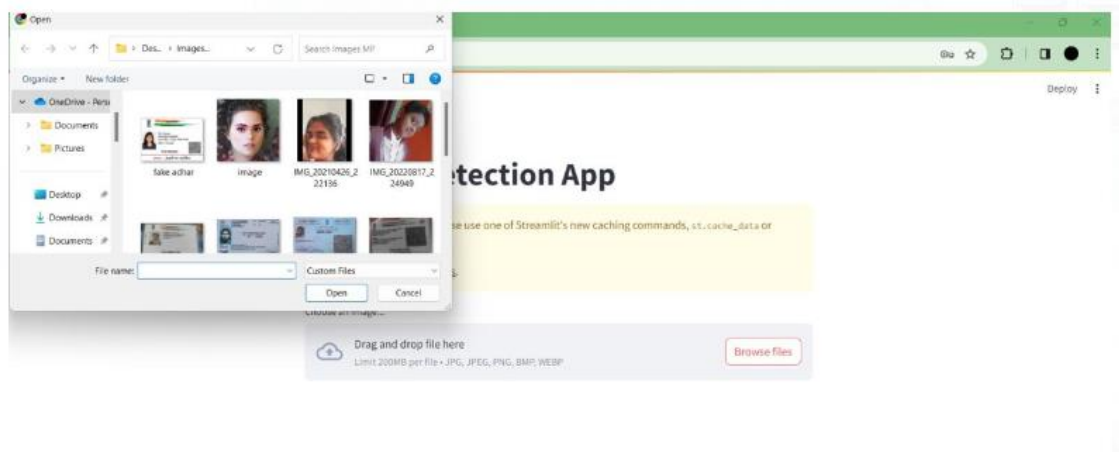
Deploy

**Fig 8.1.4 Home Page**





**Fig 8.1.5 Selecting the Model Option**



**Fig 8.1.6 Inserting the Image**



## CHAPTER 9: CONCLUSION

In conclusion, the development and implementation of our image forgery detection project using the YOLOv8 model and Streamlit framework mark a significant step forward in digital content verification technology. By leveraging deep learning algorithms and user-friendly interface design, we have created a powerful tool capable of accurately identifying forged images across various categories such as documents, human faces, and brand logos. This project holds immense potential to address the growing challenges of image forgery in diverse domains, including forensic investigations, multimedia content verification, and security applications. Moving forward, continuous refinement and optimization of the system will be essential to further enhance its effectiveness and usability, ultimately contributing to a safer and more trustworthy digital environment.

### FUTURE SCOPE

The future scope of this project is promising, with several avenues for expansion and improvement. One potential direction is to enhance the accuracy and efficiency of the image forgery detection system by integrating advanced machine learning techniques and refining the YOLOv8 model. Additionally, incorporating additional datasets and categories of forged images could broaden the system's applicability and effectiveness in detecting a wider range of forgeries. Furthermore, there is potential to develop complementary features such as automatic image authentication, real-time forgery detection, and integration with other digital forensic tools. This could extend the utility of the system across various domains including law enforcement, digital media analysis, and online content moderation. Moreover, exploring partnerships with industry stakeholders, academic institutions, and law enforcement agencies could facilitate collaboration and knowledge exchange, leading to the development of more robust and comprehensive solutions for combating image forgery.

Overall, the future scope of this project includes ongoing research, development, and collaboration efforts aimed at advancing the state-of-the-art in image forgery detection and contributing to the broader goal of ensuring trust and integrity in digital media.

## REFERENCES

- [1] Zankhana J. Barad and Mukesh M. Goswami, "Image Forgery Detection using Deep Learning: A Survey", IEEE, 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS).
- [2] Arfa Binti Zainal Abidin, Azurah Binti A Samah, Hairudin Bin Abdul Majid, and Haslina Binti Hashim, "Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review", 2019, IEEE.
- [3] Navdeep Kanwal, "An analysis of Image Forgery Detection Techniques", May 2019, Statistics Optimization & Information Computing.
- [4] Ritu Agarwal and Om Prakash Verma, "An efficient copy-move forgery detection using deep learning feature extraction and matching algorithm", 23rd DEC 2019, Multimedia Tools and Applications.
- [5] Amit Doegar, Maitreyee Dutta and Gaurav Kumar, "CNN based Image Forgery Detection using pre-trained AlexNet Model", 2018, Proceedings of International Conference on Computational Intelligence & IoT (ICCIoT), ELSEVIER.
- [6] 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", 2022, MDPI.
- [7] Mehdi Ghorbani, Mohammad Firouzmad, "DWT-DCT based Copy-Move image forgery detection", 2011.
- [8] Guohui Li, Qiong Wu, Dan Tu, and ShaoJie Sun, "A sorted neighbourhood approach for detecting duplicate reason based on DWT and SVD", 2007, IEEE.
- [9] Li Kang, Xiao-Ping Cheng, "Copy-Move forgery detection in digital image", 2010, IEEE.

- [10] Alin C. Popescu Hany Farid, “Exposing digital forgeries by detecting duplicated image regions”, 2004.
- [11] J Zhang, Z Feng, Y Su, “A new approach for detecting copy-move forgery detection in digital image”, 2008, IEEE Singapore.
- [12] Mohd Dilshad Ansari, S.P. Ghrera and Vipin Tyagi, “Pixel-Based Forgery Detection”2014