ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my project guide Dr. N. A. Patil and coordinator Prof. S. P. Patil for their invaluable guidance, support, and expertise throughout the development of their patience, encouragement, and valuable insights have been instrumental in shaping the app and making it a success. I am truly thankful for their mentorship and the time they dedicated to helping me navigate through the challenges and learn from the experience.

I would also like to extend my thanks to the Head of the Department Dr. U. M. Patil, for their continuous support and belief in my abilities. Their encouragement and provision of necessary resources created an environment conducive to innovation and growth. I am grateful for their leadership and for fostering a positive learning atmosphere that has contributed to my development.

Furthermore, I am deeply grateful to the Director, Dr. J. B. Patil, for their visionary leadership and unwavering support. Their guidance and confidence in my project gave me the motivation to strive for excellence. I appreciate their belief in my potential and their efforts to create an environment that encourages students to explore their creativity and pursue their ideas.

Project Team:

1. **Mihir Chandrakant Tathe(TY AIML-23)**
2. **Lokesh Nandalal Patil(TY AIML-51)**
3. **Yash Jagadish Marathe(TY AIML-59)**
4. **Kuldip Kishor Mahale(TY AIML-60)**

TY AIML Semester Project-III

Index

A.Y: 2025-26

Chapter No.	Name of Chapter	Page Number
1	Introduction 1.1 Project background and motivation 1.2 Problem statement 1.3 Objectives 1.4 Scope & limitations	
2	Literature Survey 2.1 Review of related work 2.2 Existing methods / models 2.3 Gaps in literature (Include minimum 3-5 standard research papers/ websites. Include their citations)	
3	Methodology 3.1 Data Description & Preprocessing 3.1.1 Data sources (include citation) 3.1.2 Data attributes / features 3.1.3 Data cleaning (missing values, outliers) 3.1.4 Data Visualization 3.2 Proposed approach / architecture 3.3 Algorithms / models used 3.4 Workflow / pipeline design	
4	Implementation Details 4.1 Tools, libraries, frameworks used 4.2 Modules / components description 4.3 Code snippets / pseudocode	
5	Experiments & Evaluation 5.1 Experimental setup 5.2 Training / validation / test split 5.3 Evaluation metrics 5.4 Results & analysis 5.5 Comparison & discussion	
6	Conclusion & Future Work	
7	References (use IEEE format)	

CHAPTER 1 : INTRODUCTION

1.1 Abstract

With the growing digitalization of academic, financial, and governmental processes, the need for secure, accurate, and automated document verification has become more critical than ever. Traditional manual verification methods are slow, error-prone, and ineffective against modern forgery techniques involving AI-assisted editing, deepfake manipulation, and high-quality digital tampering. This project presents **AuthenTech – An AI-Powered Document Verification System** designed to address these challenges using an integrated approach of **Computer Vision, Optical Character Recognition (OCR), and Natural Language Processing (NLP)**.The system employs the **YOLOv8 deep learning model** to detect micro-level tampering, forged signatures, altered photographs, or inconsistencies within certificates and identity documents. For textual extraction, the system leverages **Gemini OCR**, which provides high-accuracy recognition even in noisy, low-quality, or multi-format documents. Extracted text is further validated using **NLP-based consistency rules**, ensuring correctness in names, roll numbers, grades, and institutional details. A scalable **FastAPI backend** handles processing, while a clean, user-friendly interface enables real-time verification. AuthenTech overcomes limitations of existing systems such as template dependency, poor tampering detection, and low OCR accuracy. The solution is practical for **universities, recruiters, banks, and government agencies**, offering a fast, secure, and reliable method for authenticating sensitive documents in the digital era

1.2 Introduction to AI-Powered Document Verification

AI-powered document verification uses machine learning, computer vision, OCR, and deep learning to automatically detect whether a document is real or forged. It examines both:

A. Visual Integrity

- Detects tampered regions
- Identifies cut-paste modifications

- Finds mismatched fonts or alignment
- Detects manipulated images or photos
- Identifies inconsistencies in seals, signatures, and logos

B. Textual Integrity

- Extracts text using OCR
- Checks spelling/semantic correctness
- Compares extracted text with expected format
- Detects unexpected changes in roll numbers, grades, names, dates, etc.

The AuthenTech system uses:

- **YOLOv8** for deep image analysis and tampering detection
- **Gemini OCR API** for high-accuracy text extraction
- **NLP-based text verification** for detecting inconsistencies
- **FastAPI backend** for efficient inference
- **Modern frontend dashboard** to provide simple document upload and results

This system replaces manual checking with a highly accurate AI pipeline that can verify any document in just a few seconds, providing both authenticity output and tampering analysis.

1.3 Problem Statement

Organizations across industries face several problems with manual document verification. These include:

1. Increasing fraud and identity theft
   Attackers use AI tools to generate fake or modified certificates and identity proofs.

2. Difficulty detecting advanced forgeries
   Modern editing tools allow micro-level tampering that the human eye often cannot detect.
3. Slow, time-consuming verification
   Reviewing documents manually delays processes like admissions, onboarding, and KYC.
4. High dependency on humans
   Accuracy depends on the skill and experience of the verification officer.
5. Operational inefficiency for large-scale organizations
   Universities, banks, and corporates receive thousands of documents daily.
6. Lack of standardization
   Different officers give different results; there is no unified method.

Hence, an automated, AI-driven document verification system is needed to ensure:

- Faster processing
- Higher accuracy
- Scalability
- Fraud detection
- Standardized analysis

This forms the core motivation behind the AuthenTech system.

1.4 Existing System

Document verification has traditionally been performed through manual inspection, where officers visually examine certificates, identity cards, mark sheets, or government documents to determine their authenticity. While this method has been widely used for decades, it suffers from major drawbacks in terms of accuracy, reliability, and efficiency. To overcome these issues, several digital verification systems and commercial solutions have been

developed in recent years. However, each comes with limitations that make them insufficient for today's advanced forgery techniques.

The existing systems can be broadly classified into:

1. Traditional Manual Verification Systems
2. OCR-Based Automated Systems
3. Commercial AI Verification Platforms

1. Traditional Manual Verification Systems

Manual verification is still used in universities, banks, government offices, and corporate HR departments. Verification officers check:

- Names, roll numbers, grades, and signatures
- Official stamps and seals
- Layout and format of the document
- Matching with physical records

Limitations:

- Time-consuming and slow
- Highly prone to human error
- Vulnerable to advanced forgeries
- Cannot detect pixel-level edits
- Difficult to scale for thousands of documents
- High dependency on trained staff

This traditional system fails to meet the speed and accuracy requirements of modern digital workflows.

2. OCR-Based Automated Systems

Some organizations use Tesseract OCR, EasyOCR, or basic text extraction tools to read document content automatically. These systems convert documents into text for easier verification.

Advantages:

- Faster than manual checking
- Helps digitize old records
- Useful for extracting structured fields

Limitations:

- Poor performance on noisy, blurred, or handwritten documents
- Fails with multi-language or complex fonts
- Cannot detect tampered images or forged regions
- Only extracts text—does not verify authenticity
- Struggles with documents containing stamps, seals, or watermarks

OCR-only systems cannot identify visual manipulations, making them insufficient for fraud detection.

3. Commercial AI Verification Platforms

Several advanced commercial solutions attempt to automate verification using AI. As referenced in your Week-2 file, some notable systems include:

A. DocVerify – Automated Document Verification System

DocVerify uses template-based matching and OCR to validate documents.

Strengths:

- Good for structured documents
- Works for standard ID formats

Limitations:

- Template-dependent
- Cannot detect micro-forgeries
- Fails on non-standard certificates
- Limited capability for image analysis

B. Mitek Systems – AI-Based Verification

Mitek focuses on identity documents such as passports and licenses.

Strengths:

- Industry-grade verification
- Good image quality analysis

Limitations:

Not suitable for academic certificates

Does not perform deep forgery detection

Limited customization

CHAPTER 2 : LITEATURE SURVEY

2.1 Related Concept

The proposed AI-Powered Document Verification System is based on several modern technologies and scientific principles. The major related concepts are:

1. Computer Vision

Computer vision enables machines to interpret and understand images. In this project, computer vision is used for analyzing document structure, detecting tampered regions, identifying anomalies, and evaluating the visual integrity of certificates.

2. Deep Learning

Deep learning models learn patterns from large datasets. The YOLOv8 model used in this project identifies forged areas, manipulated text, edited seals, and cut-paste forgeries. It detects pixel-level irregularities that are invisible to the human eye.

3. Optical Character Recognition (OCR)

OCR technology extracts textual information from scanned documents and images. The project uses **Gemini OCR**, which provides high-accuracy text recognition even on low-quality or multi-language documents.

4. Natural Language Processing (NLP)

NLP checks the semantic correctness of extracted text. It validates name formats, roll numbers, CGPA ranges, date formats, and content consistency.

5. Image Forensics

Image forensics techniques help identify fake, manipulated, or tampered images by analyzing noise, compression artifacts, and inconsistent image patterns.

6. FastAPI Framework

FastAPI is used to build the backend and manage communication between the AI models and the frontend. It provides high-performance API handling and real-time processing.

7. Web Technologies

Frontend uses HTML, CSS (Tailwind), and JavaScript for creating an interactive and user-friendly interface for document upload and result display.

2.1 Objective

The main objectives of the AI-Powered Document Verification System are:

1. Automate Document Verification

To reduce manual verification time and effort by creating a fully automated AI-driven verification system.

2. Detect Forgery and Tampering

Use YOLOv8 deep learning models to identify forged regions, edited seals, manipulated signatures, photo replacements, and text-level modifications.

3. Extract and Validate Textual Information

Apply Gemini OCR to extract text and use NLP techniques to check the accuracy, structure, and consistency of fields like name, roll number, grades, and dates.

4. Improve Verification Accuracy

Achieve higher accuracy than manual inspection or traditional OCR systems by combining multiple AI technologies.

5. Provide Real-Time Verification

Enable instant document verification through FastAPI, suitable for high-volume environments such as universities, banks, and government portals.

6. Ensure Scalability and Ease of Integration

Design a system that can integrate with online portals (admissions, KYC, HR onboarding) via APIs.