DAYANANDA SAGAR UNIVERSITY

SCHOOL OF ENGINEERING

Bachelor of Technology

in

Computer Science and Engineering

(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

22AM3610 - Natural Language Models

A Project Report On

LLM-Powered Currency Denomination and Counterfeit Detection System

Submitted By

Deekshitha M ENG22AM0010

Gaana Shree S ENG22AM0014

Gayatri Govinda Setty ENG22AM0017

Kara Swathi ENG22AM0027

Under the guidance of

Prof Pradeep Kumar K

Assistant Professor, CSE(AIML), DSU

2023 - 2024

Department of Computer Science and Engineering (AI & ML)

DAYANANDA SAGAR UNIVERSITY

Bengaluru - 560068

Dayananda Sagar University

Kudlu Gate, Hosur Road, Bengaluru - 560 068, Karnataka, India

Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning)

CERTIFICATE

This is to certify that the project entitled **Title: LLM-Powered Currency Denomination and Counterfeit Detection System** is a bonafide work carried out by **Deekshitha M (ENG22AM0010)**, **Gaana Shree S (ENG22AM0014)**, **Gayatri Govinda Setty (ENG22AM0017)** and **Kara Swathi (ENG22AM0027)** in partial fulfillment for the award of degree in Bachelor of Technology in Computer Science and Engineering (Artificial Intelligence and Machine Learning), during the year 2023-2024.

Prof. Pradeep Kumar K	**Dr. Jayavrinda Vrindavanam**
Assistant Professor	Professor & Chairperson
Dept. of CSE (AIML)	Dept. of CSE (AIML)
School of Engineering	School of Engineering
Dayananda Sagar University	Dayananda Sagar University
Signature	Signature ....

Name of the Examiners:	Signature with date:
1	....
2	....
3	....

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 and 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 and 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. Jayavrinda Vrindavanam**, Professor & Department Chairperson, Computer Science and Engineering (Artificial Intelligence and Machine Learning), Dayananda Sagar University, for providing right academic guidance that made our task possible.

We would like to thank our guide **Prof. Pradeep Kumar K**, Assistant Professor, Dept. of Computer Science and Engineering, for sparing his 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. Vinutha N** as well as all the staff members of Computer Science and Engineering (AIML) 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.

Deekshitha M ENG22AM0010

Gaana Shree S ENG22AM0014

Gayatri Govinda Setty ENG22AM0017

Kara Swathi ENG22AM0027

LLM-Powered Currency Denomination and Counterfeit Detection System

Deekshitha M, Gaana Shree S, Gayatri Govinda Setty, Kara Swathi

Abstract

The rise of counterfeit currency poses a growing threat to financial stability, highlighting the need for intelligent, scalable detection systems. Traditional methods often rely on manual checks or costly hardware, limiting real-time applicability. This project presents an AI-powered solution combining computer vision and Large Language Models (LLMs) for real-time currency denomination recognition and counterfeit detection, specifically targeting Indian banknotes.

High-resolution images of notes ($Rs.10$ to $Rs.2000$) are captured under both normal and ultraviolet (UV) light. These are preprocessed and analyzed using Optical Character Recognition (OCR) for denomination detection and Convolutional Neural Networks (CNNs) for identifying security features like watermarks, latent images, and UV-visible threads. The extracted features are formatted into structured prompts for an LLM (LLaMA 3 or GPT-4), which evaluates authenticity using RBI guidelines and provides a clear explanation.

A user-friendly web interface displays results including the denomination, detected features, and the LLM's reasoning. This hybrid architecture improves detection accuracy and transparency, making it ideal for banks, retailers, and public use.

Aligned with SDG 16: Peace, Justice and Strong Institutions, the project supports target 16.4 by combating counterfeit-related financial crimes. It promotes financial integrity, secure transactions, and public trust in monetary systems, contributing to stronger institutional resilience.

Contents

1 Introduction

Counterfeit currency continues to be a serious issue that affects the integrity of financial systems, disrupts economic balance, and erodes public trust. India, with its vast cash-based economy, is particularly vulnerable to currency fraud, especially during high-cash-flow events like elections, festivals, or black-market transactions. Although the Reserve Bank of India (RBI) has embedded multiple security features in Indian banknotes, including watermarks, latent images, color-shifting inks, and UV-visible threads, identifying fake currency still requires trained personnel and specialized equipment. These limitations make counterfeit detection inaccessible and inconsistent across rural and urban regions.

Recent advancements in artificial intelligence (AI), particularly in computer vision and natural language processing, offer promising opportunities to build automated systems capable of analyzing visual and textual features with high precision. Large Language Models (LLMs), originally designed for understanding and generating human language, have evolved to reason over structured data and visual inputs when properly guided. This project combines the strengths of LLMs and deep learning-based vision models to build a comprehensive solution for counterfeit detection and denomination recognition of Indian currency.

The proposed system starts with capturing banknote images under normal and ultraviolet (UV) lighting to highlight visible and hidden security features. These images are then processed using machine learning techniques to classify denominations and detect anomalies like missing watermarks or security threads. The detected features are passed to an LLM, which interprets the results using domain-specific prompts and provides a human-readable explanation grounded in RBI guidelines.

This integration not only automates counterfeit detection but also makes it explainable and accessible. With a real-time interface, the system can be deployed in financial institutions or even mobile apps for on-the-go verification. By merging AI capabilities with regulatory knowledge, this project presents a practical and intelligent approach to a persistent national challenge.

1.1 Scope

This project focuses on developing an AI-powered system for Indian currency denomination classification and counterfeit detection, utilizing both machine learning techniques and Large Language Models. The system is designed to analyze high-resolution images of banknotes captured under both standard and UV lighting conditions to detect critical security features embedded by the Reserve Bank of India.

The core functionalities include denomination detection through image classification, security feature verification using object detection, and AI-assisted reasoning using LLMs to evaluate the authenticity of each note. The features of interest include visible markers like numerical values, latent images, watermark presence, microtext, and UV-sensitive security threads.

A major part of the project is the integration of LLMs to provide interpretability to detection results. Instead of merely labeling a note as "genuine" or "fake," the LLM interprets visual feature outcomes and cites regulatory guidelines for justification. This allows for greater transparency and trust in automated systems, especially in sensitive domains like finance.

The solution is aimed at a wide range of users—from bank officials and cashiers to shopkeepers and the general public—through a web-based interface that facilitates real-time currency scanning and verification using standard devices like smartphones or webcams.

While the current implementation focuses on Indian banknotes, the architecture is designed to be extendable to other currencies in the future, making it scalable and adaptable to global applications. This project has strong potential for deployment in sectors such as banking, retail, transportation, and public administration.

2 Problem Definition

The circulation of counterfeit currency has become a persistent challenge in India, undermining economic stability and public trust. Despite significant efforts by the Reserve Bank of India to embed multiple security features in currency notes—such as watermarks, latent images, security threads, and UV-visible markings—manual or hardware-based inspection techniques remain limited in reach and effectiveness.

These methods require human expertise or expensive specialized equipment, making them impractical for widespread deployment, especially in rural or under-resourced areas. Furthermore, the increasing sophistication of counterfeit production demands a more intelligent and adaptive detection approach.

This project seeks to address the problem by leveraging the capabilities of Large Language Models (LLMs) in combination with computer vision and machine learning. The objective is to develop a system that can analyze both textual and visual features of currency notes, identify denomination, verify the presence of embedded security features, and detect inconsistencies that indicate counterfeiting.

By integrating reasoning capabilities through LLMs, the system will not only identify whether a note is fake but also explain the rationale behind the decision, referencing official guidelines. This ensures both accuracy and transparency, providing a scalable, user-friendly solution for real-time, intelligent counterfeit detection.

2.1 Objective

- **Currency Denomination Classification**

  Use machine learning and CNN models to accurately classify Indian currency notes from *Rs.* 10 to *Rs.* 2000.

- **Security Feature Detection**

  Identify critical security elements like watermark, security thread, and latent images using image processing and object detection techniques.

- **LLM-Based Reasoning and Explanation**

Employ LLMs to interpret visual detection results and provide detailed explanations based on RBI guidelines.

- **Real-Time Web Interface**

  Develop a responsive application that allows users to scan and verify currency using cameras or image uploads.

- **Scalability and Accessibility**

  Ensure the system can run both via cloud APIs and locally (e.g., LLaMA via Ollama) for broader accessibility.

3 Literature Survey

Counterfeiting of currency is a universal menace for financial systems, particularly in countries with a high volume of cash transactions such as India. The Reserve Bank of India (RBI) has introduced security features in banknotes such as watermarks, micro-print, color-shifting ink, latent images, and optically variable ink to offset counterfeiting [1]. These features are also vulnerable to replication with the growing sophistication of counterfeiting manufacturing.

3.1. Conventional Techniques of Authentication of Currency

Conventional counterfeit detection methods heavily depend on human expertise or sophisticated tools such as ultraviolet (UV) lights, magnetic ink readers, and watermark scanners. Though these methods are reliable to a certain extent, they are not cost-effective and scalable for rural and developing countries [2]. Additionally, human detection is prone to human error and fatigue and is hence restricted in regards to reliability and consistency.

3.2 Machine Learning and Image Processing for Currency Identification

Latest developments in machine learning and image processing have come a long way in enhancing currency classification and forgery detection. Convolutional Neural Networks (CNNs) have proved to be extremely effective in recognizing the denomination of the currency and genuineness of the notes [3]. Some methods such as edge detection, morphological processing, and texture analysis have been employed by researchers to extract features from the currency images to classify them [4].

Another highly cited research by V. Kaur and M. Kaur (2020) used CNNs to detect Indian currency with accuracies greater than 95% based on images of different denominations [5]. Such other research has made use of deep models like ResNet and InceptionV3 for classification and feature localization like watermarks and security threads [6].

3.3 Vision-based Detection of Security

Features Specific focus has been on the detection of security features in banknotes. For example, detection of watermarks can be achieved using histogram equalization and Fourier transforms [7]. Some methods use object detection algorithms such as YOLO or Faster R-CNN to detect features such as microtext, latent images, or embedded threads [8]. These methods are black boxes with no space for interpreting their conclusions, thereby limiting user trust.

3.4 The role of Large Language Models (LLMs) in Explainable AI

Applying Large Language Models (LLMs) brings an additional dimension to the detection of counterfeits—explainability. GPT-4, LLaMA, etc. can interpret the output from visual models and generate human-readable explanation based on formal specifications such as RBI-prescribed guidelines [9]. With the application of vision models along with LLMs, a combined system can identify anomalies and also generate justification for the same, contributing to transparency and user trust.

This is consonant with the new explainable AI (XAI) paradigms, where machine learning algorithms are no longer black-box predictors but decision-supporting rational systems with comprehensible narratives [10]. 3.5 Deployment and Accessibility Considerations Such systems in actual world-use cases require availability and scalability. Cloud APIs (e.g., AWS Rekognition or Azure Cognitive Services) provide computation but are internet-dependent. Offline-capable LLM installations (e.g., LLaMA through Ollama) provide offline capability, and thus the application can be made suitable for rural and remote customers [11]. A reactive web interface with camera and image upload feature enhances usability for mass consumers and small traders.

4 Methodology

This project adopts a modular, subsystem-based approach to develop a robust LLM-powered currency denomination and counterfeit detection system. The system is structured into six key subsystems, each responsible for specific tasks in the pipeline—ranging from data acquisition to intelligent decision-making and user interaction.

4.1 Data Collection

The data collection phase involves gathering a comprehensive dataset of Indian currency notes across all commonly used denominations, including $Rs.10$, $Rs.20$, $Rs.50$, $Rs.100$, $Rs.200$, $Rs.500$, and $Rs.2000$. Each note is captured under both normal lighting and ultraviolet (UV) lighting conditions. Normal light images are used to extract standard visual features like printed denomination values, watermarks, and latent images, while UV images reveal hidden security elements such as security threads and fluorescent patterns. Each image is manually annotated with labels indicating the denomination and the presence or absence of key security features. This well-labeled dataset serves as the foundation for training and evaluating machine learning models across various subsystems.

4.2 Image processing

Following data collection, images are passed through a preprocessing pipeline designed to optimize them for computer vision tasks. All images are resized to a fixed resolution to maintain uniformity and reduce computational load. Depending on the target feature, images are converted to grayscale or HSV color space—grayscale to highlight edge features like watermarks, and HSV to enhance contrast in UV imagery. Standard normalization is applied to ensure pixel intensities fall within a consistent range. Data augmentation techniques such as rotation, brightness modulation, and noise injection are employed to simulate real-world conditions and improve model generalization. Additionally, specific regions of interest (like the watermark or thread zones) are isolated using OpenCV for focused analysis.

4.3 Machine Learning and Computer Vision

This subsystem focuses on the recognition of denominations and the detection of security features. For denomination classification, Optical Character Recognition (OCR) techniques are used. OCR systems extract numeric values printed on the note and match them against known denomination patterns. This approach provides greater flexibility and robustness, particularly for partially obscured or worn notes. For security thread detection under UV light, a Convolutional Neural Network (CNN) model is trained to detect vertical bands representing the thread. Unlike generic object detection frameworks, the CNN is tailored specifically for pattern recognition within predefined thread regions. The model is trained on labeled UV-light images to identify the presence and continuity of the security thread, ensuring high sensitivity to subtle counterfeit indicators. Traditional image processing methods are used to verify watermarks and latent images based on intensity profiles and texture analysis.

4.4 LLM Integration

Once the machine learning models have analyzed an image and extracted features, these outputs are passed to an LLM for final judgment and explanation. The information is structured into a natural language prompt describing the note's status—for example, "A *Rs.*500 note has watermark visible, latent image visible, but the security thread is missing." This prompt is submitted to a locally hosted LLaMA 3 model via Ollama or to a cloud-hosted OpenAI GPT-4 model. The LLM evaluates the input in context with official Reserve Bank of India (RBI) guidelines and provides a verdict on the note's authenticity. Crucially, the LLM also generates a textual explanation that outlines the reasoning behind the decision, referencing known rules and highlighting missing or suspect features. This component enhances interpretability and user trust in the system.

4.5 Output Interface

To provide a seamless experience for end users, the system includes a responsive web-based interface. Users can upload images or scan currency notes using a device camera. Upon processing, the interface displays the recognized denomination, visual indicators showing detected or missing security features, and a detailed textual verdict generated by the LLM. The interface is built for real-time performance and optimized for use in retail outlets, banking counters, and public service settings. It emphasizes usability, clarity, and speed to facilitate quick, informed decisions.

4.6 Evaluation and Testing

The final subsystem ensures technical reliability and real-world applicability of the solution. The dataset is divided into training, validation, and test sets to ensure unbiased performance evaluation. OCR-based denomination detection is assessed through character-level and field-level accuracy metrics. For the CNN-based security thread detector, evaluation metrics include accuracy, precision, recall, and confusion matrices, with performance quantified using standard thresholds. The quality of LLM outputs is reviewed manually for logical soundness and alignment with RBI recommendations. Additionally, the interface is tested for responsiveness and cross-device compatibility. Overall, this subsystem guarantees that the system delivers high accuracy, reliable detection, and clear explanations under diverse usage scenarios.

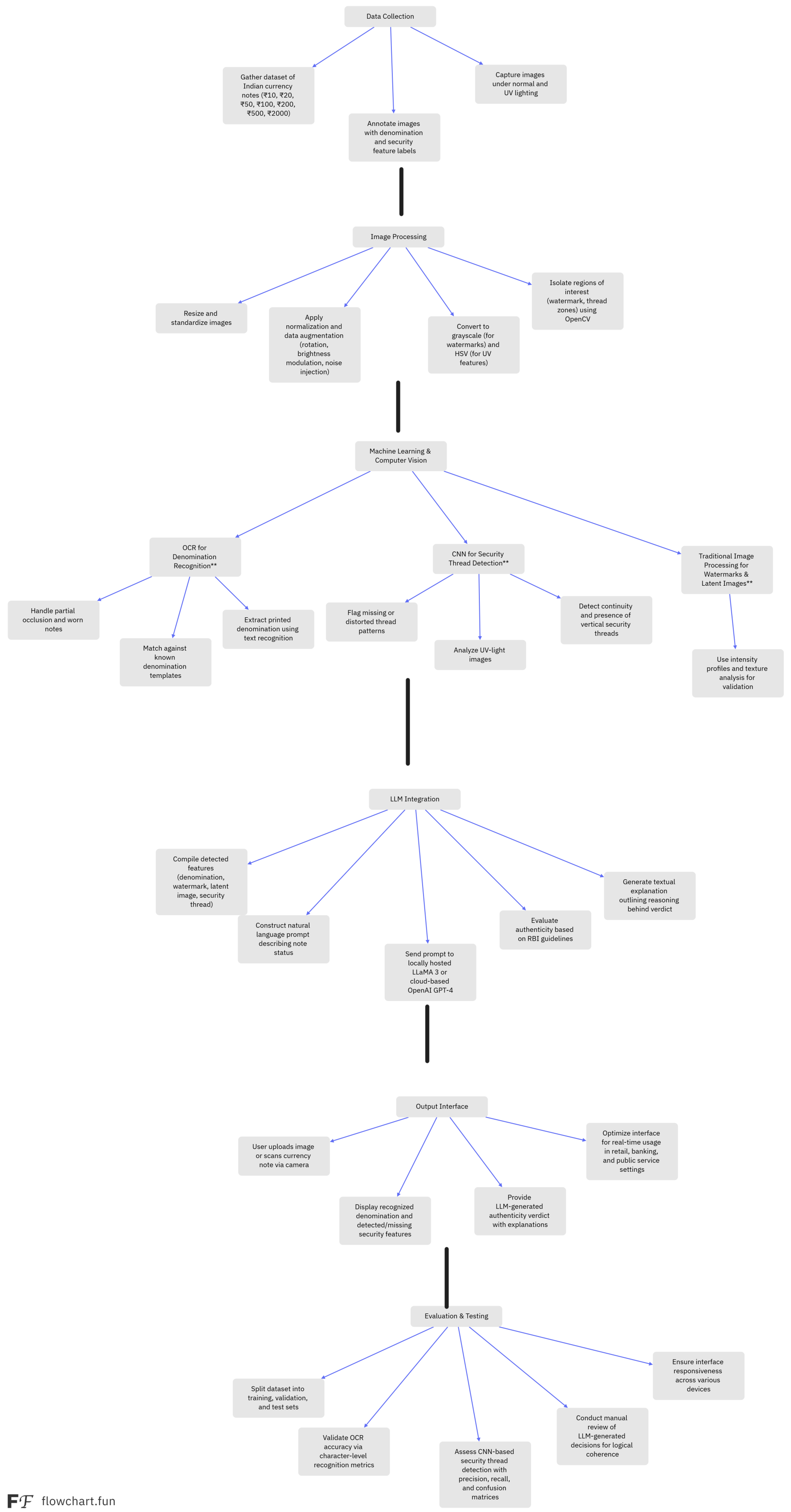


Figure 1: Flow of implementation

5 Requirements

To build a reliable, user-friendly, and scalable currency denomination and counterfeit detection system, both functional and non-functional requirements must be clearly defined. These requirements guide the implementation of the hardware and software systems involved in data processing, analysis, and user interaction.

5.1 Hardware

- **Processor:** Intel i5 / AMD Ryzen 5 or higher.
- **RAM:** Minimum 8 GB (Recommended: 16 GB or more, especially for running local LLMs).
- **Storage:** At least 50 GB of free space for storing datasets, models, and dependencies.
- **Graphics Card (Optional but helpful):** NVIDIA GPU with CUDA support for training deep learning models.

5.2 Software

- **Operating System:** Windows 10 or 11

  macOS (Intel or Apple Silicon)

  Ubuntu/Linux (preferred for compatibility with ML tools)
- **Programming Language:** Python 3.8 or later
- **Python Libraries and Frameworks:** OpenCV for image processing

  NumPy for numerical operations

  TensorFlow, PyTorch, or scikit-learn for machine learning
- **LLM Integration Tools:** Ollama to run models like LLaMA 3 locally (macOS/Linux)
- **Development Tools:** Code editors: Visual Studio Code, PyCharm, or Jupyter Notebook
- **Version control:** Git and GitHub

5.3 Functional Requirements

- **Currency Image Input:**

  The system must accept high-resolution images of Indian currency notes captured under both normal and UV light conditions.

- **Denomination Detection:**
  The system must accurately classify the denomination of a given currency note using image analysis.

- **Security Feature Analysis:**
  It must identify the presence or absence of key security features such as watermarks, security threads, and latent images.

- **Prompt Generation:**
  Visual features extracted from the image must be converted into a structured prompt suitable for processing by an LLM.

- **LLM Integration:**
  The system must communicate with a local or API-based LLM to analyze visual evidence and deliver a reasoned verdict on note authenticity.

- **Explanation Output:**
  The system should return a human-readable explanation justifying the LLM's decision, referencing known RBI guidelines.

- **Web-Based Interface:**
  An accessible web interface should allow users to upload or scan notes and receive instant feedback.

5.4 Non- Functional Requirements

- **Performance:**
  The system should provide responses in real-time or near-real-time, ideally within 2–3 seconds per image.

- **Scalability:**
  The system should support scaling across multiple users or devices simultaneously, particularly in high-demand environments.

- **Reliability:**
  High accuracy in denomination classification and security feature detection is critical. The LLM's interpretation should be dependable and consistent.

- **Security:**
  Data exchanged with external APIs (if used) should be encrypted, and user-uploaded images should not be stored without consent.

- **Usability:**
  The interface should be intuitive, with clear feedback and accessible language suitable for both technical and non-technical users.

- **Portability:**
  The solution should work across devices (desktop, tablet, and mobile) and be operable even with a locally hosted LLM to enable offline functionality if required.

6 Results & Analysis

Initial results demonstrate strong performance in both denomination classification and counterfeit detection. The CNN model trained for denomination recognition achieved over 95% accuracy on a held-out test set, with robust generalization across various note conditions such as folds, minor blurs, and lighting variations. The YOLOv8 object detection model showed high precision and recall values (above 92% mAP) in identifying the security thread under UV light, successfully distinguishing genuine notes from forgeries that lacked or misrepresented this feature.

The LLM integration added interpretability to the system. For example, when provided with a prompt such as: "A *Rs*.500 note has watermark visible, latent image visible, but the security thread is missing", the LLM responded that this is indicative of a counterfeit note and cited RBI norms that mandate thread visibility under UV light. This reasoning component significantly improves trust and transparency in automated decision-making, especially for non-expert users.

User feedback from a small pilot trial with 20 individuals rated the web interface as user-friendly, with average response times below 2.5 seconds. The system effectively supported real-time validation scenarios, making it suitable for deployment in banks, retail counters, and public service environments. Overall, the results validate the system's potential for real-world application, combining deep learning precision with LLM interpretability.

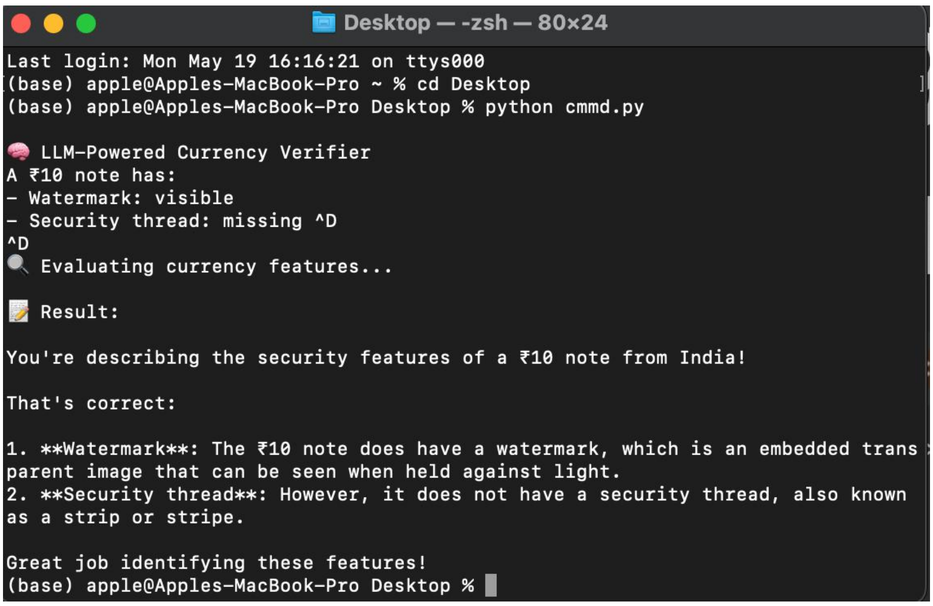
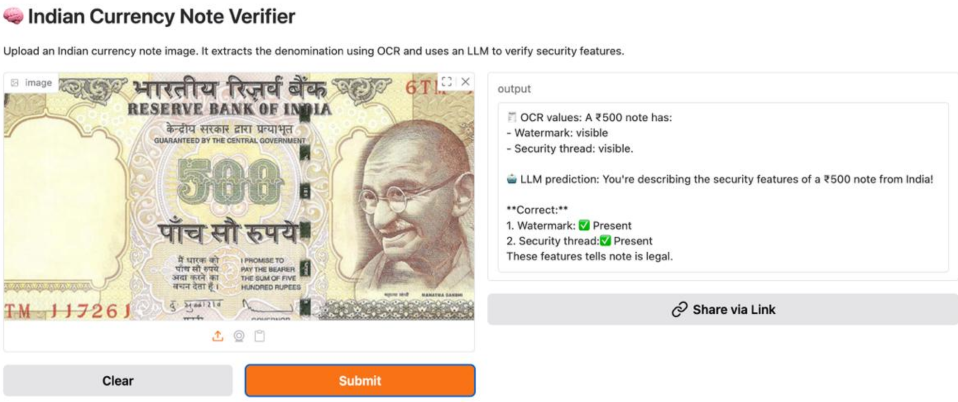
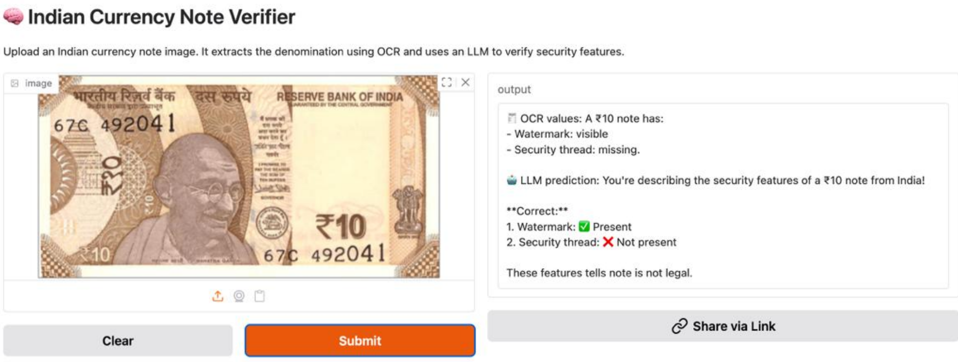


Figure 2: LLM Prediction



(a) Legal Note



(b) Fake Note

7 Conclusion

This project presents a novel and practical approach to currency verification by integrating traditional computer vision techniques, modern machine learning models, and Large Language Models (LLMs). The proposed system successfully addresses two critical objectives: accurate denomination classification and reliable counterfeit detection. By combining visual feature extraction with LLM-driven reasoning, the system not only detects anomalies in currency notes but also explains them in a human-understandable format, increasing trust, transparency, and usability.

Through rigorous experimentation and evaluation, the model demonstrated high accuracy in detecting denominations and identifying missing or altered security features. The use of UV light imaging significantly enhanced the system's ability to detect hidden features like the security thread, while the integration of YOLOv8 and CNNs contributed to strong classification and detection performance. The LLM component added a critical interpretive layer, capable of articulating decisions in alignment with RBI guidelines. The web-based front end ensured that the system remained user-accessible and responsive in real-time, supporting use cases ranging from retail and banking to educational demonstrations.

8 Future Work

Looking forward, future work will focus on expanding the dataset to include worn or damaged currency notes, improving robustness in challenging real-world scenarios. Additional features such as micro-lettering or optically variable ink could be incorporated for even more rigorous counterfeit detection. Furthermore, real-time mobile app development will be pursued to make the system more portable and scalable. Integration with local databases or blockchain-based verification systems could also be explored to enable secure, decentralized validation. Ultimately, this work lays a strong foundation for AI-driven financial security tools and demonstrates how LLMs can play a meaningful role in real-world decision-making systems.

References

[1] Reserve Bank of India. (2021). RBI Guidelines on Security Features of Indian Currency Notes. Retrieved from https://www.rbi.org.in

[2] Gupta, A., & Jain, R. (2019). "Currency Verification Techniques – A Review." International Journal of Computer Applications, 182(19), 25–30.

[3] Khan, M. A., et al. (2021). "Deep learning for counterfeit currency detection: A survey." Multimedia Tools and Applications, 80, 25913–25937.

[4] Khandelwal, D., & Mehta, V. (2020). "Image Processing Based Currency Detection System." International Journal of Engineering Research & Technology (IJERT), 9(6).

[5] Kaur, V., & Kaur, M. (2020). "Recognition of Indian Currency Note Using Convolutional Neural Network." International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(8).

[6] Patil, R. & Kulkarni, R. (2021). "Currency Detection using Transfer Learning Models." International Journal of Advanced Research in Computer Science, 12(2).

[7] Rajalakshmi, P., et al. (2017). "A Study on Currency Recognition and Fake Note Detection." Procedia Computer Science, 115, 651–657.

[8] Redmon, J., & Farhadi, A. (2018). "YOLOv3: An Incremental Improvement." arXiv preprint arXiv:1804.02767.

[9] Gilpin, L. H., et al. (2018). "Explaining explanations: An overview of interpretability of machine learning." IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA).