

**Title: DETECTION OF FAKE CURRENCY USING LOGISTIC
REGRESSION**



A

ADM Course Project Report

in partial fulfilment of the degree

Bachelor of Technology
in
Computer Science & Engineering

By

N.NITHISH 2303A51066

J.SATHWIK 2303A51055

CH.VEDHAN 2303A510G8

G.PREETHAM 2303A51054

Under the guidance of

Bediga Sharan
Assistant Professor

Submitted to School of Computer Science and Artificial Intelligence

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the **Application of Data Mining – Course Project** Report entitled “**“detection of fake currency ”**” is a record of bonafide work carried out by the student(s) **“N.nithish,j.sathwik,ch.vedhan,g.preetham”**, bearing Hall ticket, No(s) **2303A51066,1055,10G8,1054,1** **during** the academic year 2024-25 in partial fulfillment of the award of the degree of *Bachelor of Technology* in **Computer Science & Engineering** by the SR University, Warangal.

Supervisor

(Mr. Bediga Sharan)

Assistant Professor

Head of the Department

(Dr. M. Sheshikala)

Professor

TABLE OF CONTENT

S.NO	TITLE	PAGE-NO
1	EVALUATION & SELECTION OF SPECIFICATIONS / FEATURES	3-4
2	Features of Currency	4-8
3	Analysis of Features and Finalization on Subject to Constraints:	8-10
4	Design Selection	10-11
5	Flowchart	12
6	Block Diagram	13

LIST OF FIGURES

FIG.NO	FIGURE NAME	PAGE-NO
Fig 3.1	All security features of Indian currency 2000 Portrait	5
Fig 3.2	Portrait of Mahatma Gandhi	6
Fig 3.3	Security Thread	6
Fig 3.4	Ashoka Pillar	6
Fig 3.6	Identification Mark	7
Fig 3.7	Guarantee Clause	7
Fig 3.8	Currency Numeral with the Rupees Symbol	7
Fig 3.9	Bleed Lines	8
Fig 3.10	Latent Image of Denomina on Numeral	8
Fig 3.11	Micro Leering	8
Fig 3.12	Government of India	9

3.1. EVALUATION & SELECTION OF SPECIFICATIONS / FEATURES

1. Accuracy:

- Explanation: Accuracy refers to the ability of the fake currency detection system to correctly classify genuine and counterfeit currency notes. A high accuracy ensures reliable detection and minimizes false positives or false negatives, which are crucial in sensitive domains like finance.

2. Robustness:

- Explanation: Robustness indicates the system's resilience to variations and challenges, such as changes in lighting conditions, image quality, or counterfeit techniques. A robust system can effectively detect counterfeit features under diverse scenarios, enhancing its reliability in real-world applications.

3. Generalization:

- Explanation: Generalization refers to the system's ability to perform well on unseen data or currency notes not included in the training dataset. A model with good generalization can detect counterfeit features across different currencies, denominations, and regions, making it versatile and adaptable to various counterfeit threats.

4. Speed:

- Explanation: Speed relates to the efficiency of the detection process, particularly in scenarios where currency notes need to be processed quickly, such as in banking or retail environments. A fast detection system enables swift verification of currency authenticity, improving operational efficiency and customer satisfaction.

5. Versatility:

- Explanation: Versatility denotes the system's flexibility to handle input from diverse sources and formats, including images captured from different devices or under varying conditions. A versatile system accommodates various input types and ensures consistent performance across different environments, enhancing its usability and applicability.

6. Feature Extraction:

- Explanation: Feature extraction involves identifying relevant patterns or characteristics from currency images that distinguish between genuine and counterfeit notes. Effective feature extraction methods capture subtle counterfeit features while minimizing noise, enabling accurate detection by the machine learning model.

7. Model Interpretability:

- Explanation: Model interpretability refers to the ability to understand and explain the decisions made by the fake currency detection model. Interpretable models provide insights

into the features influencing classification results, fostering trust and transparency in the system's operation.

Open CV:

OpenCV is a sizable open-source library for image processing, machine learning, and computer vision. It now plays a significant part in real-time operation, which is crucial in modern systems. With it, one may analyze pictures and movies to find faces, objects, and even human handwriting. To install OpenCV run the command - `pip install opencv-python`. Python is able to handle the OpenCV array structure for analysis when it is integrated with different libraries, such as NumPy. We use vector space and apply mathematical operations to these features to identify visual patterns and their various features. [42] NumPy:

Many mathematical operations can be carried out on arrays with NumPy. It provides a vast library of high-level mathematical functions that work on these arrays and matrices, as well as strong data structures that ensure efficient calculations with arrays and matrices. To install NumPy run the command - `pip install numpy`. [43] VS Code:

Debugging, task execution, and version control are supported by the simplified code editor Visual Studio Code. It tries to give developers only the tools they require for a short cycle of codebuilddebugging and leaves more sophisticated processes to IDEs with more features, like Visual Studio

IDE. [44]

3.2 Features of Currency

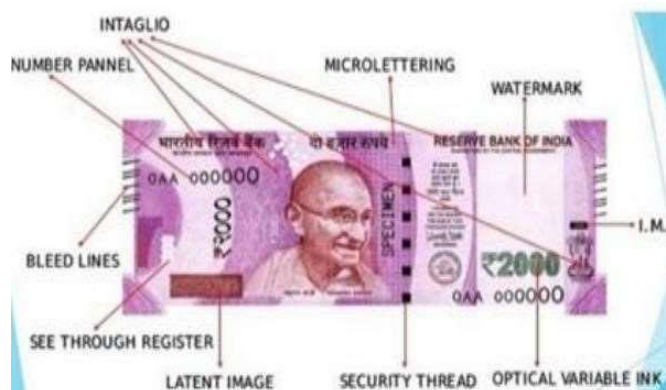


Fig 3.1: All security features of Indian currency 2000[3] Portrait

All features of Indian currency 2000 showing in fig of Mahatma Gandhi at the Center:

The intaglio printing of portrait of Mahatma Gandhi at the center of the currency.



Fig 3.2: Portrait of Mahatma Gandhi [1]

Security Thread:

When held up to the light, the security thread, which has "RBI" and "Bharat" inscribed on it continually, can be seen at the left side of the watermark. The photo of the Mahatma has a security thread on one side.



Fig 3.3: Security Thread [1]

See through Register:

The denomination numeral is displayed in the see-through register. Both sides of this register are printed. One side of the two sides is hollow, and the other side is filled with material. The micro lettering has been written horizontally along this register. The note has a latent image on the left side. Moreover, this register is shown above the latent image. When viewed in contrast to the light, this register appears as a single design.



: Ashoka Pillar:

On the right side of the coin there is a picture of the Ashoka pillar.



Fig 3.5: Ashoka Pillar[1]

Identification Mark:

Just over the Ashoka's pillar symbol, there is an identification mark.



Fig 3.6: Identification Mark[1]

Guarantee Clause:

Located to the right of Mahatma Gandhi's image, the guarantee clause is signed by the governor and includes a promise clause that is printed in intaglio.

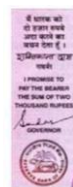


Fig 3.7: Guarantee Clause[1]

Currency Numeral with the Rupees Symbol:

Fluorescent ink will be used for printing. When viewed from different perspectives, the numerals change.



Fig 3.8: Currency Numeral with the Rupees Symbol[1]

Bleed Lines:

The oblique lines that protrude from the sides of banknotes are known as bleed lines.

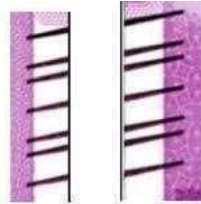


Fig 3.9: Bleed Lines [1]

Latent Image of Denomina on Numeral:

The right side of Mahatma Gandhi's portrait is bordered by a vertical band on the opposite side of the denomination. A latent image of the corresponding denominational value is present in it. Its denominational value is represented by a numerical value. The latent picture can be seen when the coin is held horizontally, and it should also be held at eye level. While using counterfeit money, it is not noticeable.



Fig 3.10: Latent Image of Denomina on Numeral [1]

Micro Lettering:

Between the vertical band and the image of Mahatma Gandhi, micro lettering is visible. The term "RBI" and the denominational value are written in tiny letters. The micro letters on counterfeit money are incorrectly printed.

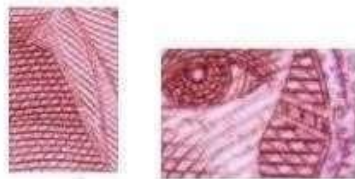


Fig 3.11. Micro Lettering [1]

Government of India:

The words "Government of India" are printed at the top of the one rupee note, directly over the Devanagari-scripted number one. The smallest currency note now in use in India is 1 rupee, and it is the only one that was produced by the Government of India rather than the Reserve Bank of India like the others. Because of this, it is the only one with the Finance Secretary's signature rather than the RBI Governor's.



Fig 3.12. Government of India[1]

Required Algorithm:

Image acquisition:

The act of obtaining an image from sources is known as image acquisition. Hardware systems like cameras, encoders, sensors, etc. can be used to do this. It is without a doubt the most important phase in the MV (Machine Vision) workflow because a bad image would make the workflow ineffective as a whole. As machine vision systems don't study the acquired digital image of the object and not the object itself, acquiring an image with the proper clarity and contrast is crucial. A set of photo-sensitive sensors turn an object's incoming light wave into an electrical signal during the image acquisition step. These little components provide the function of accurately describing the object to your machine vision algorithms. It's a frequent fallacy that with an MV system, choosing the correct colours is crucial. However, it's not always the case. Colours frequently increase noise and make detection more challenging. The main objective of an image acquisition system is to increase contrast for the important features. The ideal image is one in which the camera can clearly see the object of interest.

3.3 Analysis of Features and Finalization on Subject to Constraints:

Constraint 1: Data Availability:

- Analysis: Limited availability of diverse counterfeit currency images may restrict the model's ability to generalize across various currencies and denominations.
- Action: Augment the dataset with synthetic data generation techniques or explore transfer learning approaches to leverage pre-trained models on similar tasks.

Constraint 2: Computational Resources:

- Analysis: Limited computational resources may restrict the complexity of the model architecture and training process.
- Action: Optimize feature extraction techniques and model architectures to balance performance and computational efficiency. Consider deploying the model on cloud-based platforms for scalability.

Constraint 3: Regulatory Compliance:

- Analysis: Regulatory constraints regarding the use of sensitive currency images and data privacy may impact the development and deployment process.
- Action: Implement robust data anonymization and encryption techniques to ensure compliance with data protection regulations. Collaborate with legal experts to address regulatory concerns and obtain necessary approvals.

Constraint 4: Real-time Processing:

- Analysis: Real-time processing requirements for currency authentication applications may impose constraints on model inference speed and latency.
- Action: Optimize model inference algorithms and deploy lightweight models suitable for real-time processing. Explore hardware acceleration techniques like GPU acceleration for faster inference.

Constraint 5: Interpretability and Explainability:

- Analysis: The need for model interpretability and explainability to gain user trust and regulatory approval.
- Action: Incorporate explainable AI techniques such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations) to provide insights into model predictions and feature importance.

Constraint 6: Scalability and Adaptability:

- Analysis: Scalability requirements to handle increasing volumes of currency data and adaptability to evolving counterfeit techniques.
- Action: Design modular and scalable architectures that allow easy integration of new features and adapt to emerging counterfeit threats. Implement continuous monitoring and update mechanisms to ensure the model remains effective over time.

Constraint 7: User Interface and Accessibility:

- Analysis: User interface design constraints to ensure ease of use and accessibility for diverse user groups.
- Action: Collaborate with UX/UI designers to develop intuitive and accessible interfaces for currency authentication applications. Conduct usability testing to gather feedback and iterate on interface design.

3.4 Design Selection

Data Collection:

- Explanation: Gather a comprehensive dataset of currency images, including genuine and counterfeit notes, covering various denominations, currencies, and regions. A diverse dataset ensures the model learns to detect counterfeit features across different scenarios.

Preprocessing:

- Explanation: Preprocess currency images by standardizing resolution, brightness, and orientation. Apply noise reduction and image enhancement techniques to improve image quality, ensuring consistent feature extraction and model performance.

Feature Extraction:

- Explanation: Employ feature extraction methods like Histogram of Oriented Gradients (HOG), Local Binary Patterns (LBP), or Convolutional Neural Networks (CNNs) to capture distinctive features from currency images. Select features robust to variations and discriminative between genuine and counterfeit notes.

Model Selection:

- Explanation: Evaluate various machine learning algorithms such as Support Vector Machines (SVM), Random Forest, or Convolutional Neural Networks (CNNs) for classification. Choose a model demonstrating high accuracy, robustness, and generalization capabilities on the dataset.

Model Training:

- Explanation: Split the dataset into training, validation, and test sets. Train the selected model, fine-tuning hyperparameters to optimize accuracy and minimize overfitting. Validate the model's performance through cross-validation and testing on unseen data.

Evaluation Metrics:

- Explaination: Define evaluation metrics like precision, recall, F1-score, and accuracy to assess model performance. Validate accuracy and robustness through cross-validation and testing, ensuring the model meets desired performance criteria.

Deployment:

- Explaination: Develop an application interface or API for seamless integration of the fake currency detection model into banking or retail systems. Ensure compatibility with different platforms and environments, facilitating easy deployment and usage.

Security Measures:

- Explaination: Implement encryption and access control mechanisms to protect sensitive data, such as currency images and detection results. Conduct security audits and penetration testing to identify and address potential vulnerabilities in the system.

Continuous Improvement:

- Explaination: Establish feedback mechanisms to collect user feedback and detection results for model retraining. Monitor model performance over time and update it periodically to adapt to new counterfeit threats or changes in currency designs.

Regulatory Compliance:

- Explaination: Ensure compliance with data protection regulations and industry standards like GDPR, HIPAA, or ISO/IEC 27001 to maintain user privacy and data security, adhering to legal requirements.

3.5 Flowchart

