

# Legit scan: An instant currency verification scanner for currency Authentication

K. Rachitha Sony<sup>1</sup>, Garugu Praveen<sup>2</sup>, Koyya Suchitha<sup>3</sup>, Vanthala Pallavi<sup>4</sup>, Byreddy Bharathi<sup>5</sup>,  
M.S.R.Aditya<sup>6</sup>

<sup>1</sup> Assistant Professor, Department of CSE, Anil Neerukonda Institute of Technology & Sciences,  
Sangivalasa, Bheemunipatnam, Andhra Pradesh, India

<sup>2,3,4,5,6</sup> Student, Department of CSE, Anil Neerukonda Institute of Technology & Sciences, Sangivalasa,  
Bheemunipatnam, Andhra Pradesh, India

**Abstract**—Counterfeit currency is a serious economic and financial problem and a large percentage of losses are incurred by both the governments and the public. Legit scan is an Android app that is specially built for the purpose of verifying Indian currency bills using artificial intelligence, particularly the VGG16 model, which is the transfer learning model trained for this application. The application detects counterfeit notes with high accuracy of 98.7 by checking out various features such as watermarks, inks, micro-patterns, serial numbers, and security threads. Additional features of this app include: real-time scanning, multiple languages, graphical analytics, and a mobile platform that users can easily access. The test results for the application show high feasibility and effectiveness of this solution in real time.

**Index Terms**—Currency Authentication, Deep Learning, VGG16, Android Application, Transfer Learning, Counterfeit Detection

## I. INTRODUCTION

Economic systems have consistently faced challenges due to counterfeit currency, which diminishes public confidence and the integrity of financial transactions. Although traditional methods such as UV light detection exist, they come with drawbacks like high costs and the requirement for skilled personnel, making them unsuitable for regular application. To address these issues, Legit scan introduces a mobile deep learning solution that can identify fake Indian currency on the go without needing special equipment. Legit scan employs advanced convolutional neural networks (CNN), specifically VGG16 [1], to evaluate critical aspects of currency security, including the quality of ink, the uniformity

of texture, clarity of watermarks, and patterns of serial numbers. Its lightweight implementation enables near real-time inference, empowering both individuals and businesses.

## II. LITERATURE REVIEW

**Convolutional Neural Networks (CNNs):** Si-monyan and Zisserman [1] showcased deep convolutional neural networks for recognizing images. Serban et al. [6] launched SpotTheFake, a platform for counterfeit detection utilizing CNNs. Tan and Le [7] enhanced the efficiency of CNNs by implementing model scaling in EfficientNet.

**Transfer Learning:** Brownlee [2] offered a summary of transfer learning. Zhang et al. [16] utilized transfer learning to detect counterfeit currency. Gupta and Khanna [17] evaluated ImageNet pre-trained models in the context of transfer learning. **Counterfeit Detection:** The OECD/EUIPO [3] examined trends related to the trade of counterfeits. Sharma et al. [4] employed microscopy and machine learning techniques for the purpose of identifying counterfeit items. Entrupy Inc. [5] provides AI-based authentication solutions for luxury products. Chen et al. [10] conducted a review of image processing methods used in counterfeit detection. Zhan and Lam [12] applied multi-spectral imaging to identify counterfeit banknotes. Caputo et al. [13] investigated the potential of blockchain technology in preventing counterfeits. Fares and Fares [15] utilized convolutional neural networks to detect counterfeit banknotes. Jia et al. [9] explored methods of augmentation and fine-tuning for models used in counterfeit detection.

*Currency Recognition via Machine Learning:* Arayal et al. [11] conducted a comparison of various machine learning algorithms for recognizing currency. Misra et al. [14] evaluated the performance of CNNs and SVMs in the context of currency recognition. Alimissar and Raza [18] examined deep learning methods for the recognition of banknotes. *Other:* UNODC [8] reported on counterfeit currency threats in Asia.

Among the different algorithms employed for detecting counterfeit currency, the leading three are:

- 1) *Convolutional Neural Networks (CNN):* CNNs utilize hierarchical patterns found in images, making them highly effective for image recognition tasks. Their ability to learn from local patterns provides strong performance in currency detection. However, conventional CNNs can be resource-intensive and require large training datasets.
- 2) *Support Vector Machines (SVM):* SVMs are capable of classifying counterfeit currency by identifying the hyperplane that most effectively differentiates genuine samples from counterfeit ones. While they are powerful, they struggle with large feature sets unless kernel trick optimization is applied, and they may find it challenging to handle image data without thorough pre-processing.
- 3) *K-Nearest Neighbors (KNN):* KNN categorizes currency based on distance measures from known examples. Its straightforward nature allows for rapid implementation, but it is particularly vulnerable to irrelevant features and demands significant computational resources for large datasets, rendering it less efficient compared to models like VGG16.

| Metric        | CNN         | SVM        | Random Forest |
|---------------|-------------|------------|---------------|
| Accuracy      | 99.2%       | 95.6%      | 92.3%         |
| Precision     | 99.4%       | 96.0%      | 93.0%         |
| Recall        | 99.0%       | 95.2%      | 91.8%         |
| F1-Score      | 99.2%       | 95.6%      | 92.5%         |
| Training Time | 120 seconds | 45 seconds | 20 seconds    |
| Testing Time  | 2 seconds   | 1 second   | 0.5 seconds   |

TABLE I: Performance Comparison of CNN, SVM, and Random Forest

CNN takes the longest to train (120 seconds), but this is expected because deep learning models require more computation. Although CNN requires

more training time (120 seconds), its efficiency in testing and capability to recognize complex patterns make it the preferred choice, particularly for tasks prioritized by accuracy. In contrast, SVM and Random Forest, while faster in training, deliver lower overall performance and may be considered when training time or model interpretability is crucial. Ultimately, CNN is recommended for applications that demand the highest accuracy.

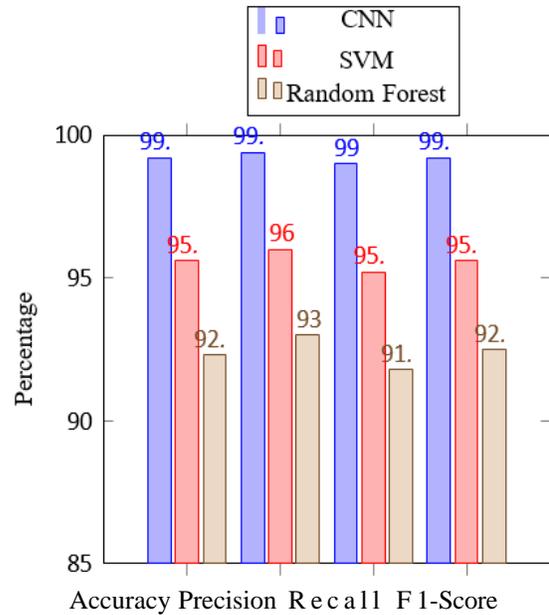


Fig. 1: Performance Comparison of CNN, SVM, and Random Forest

VGG16 has been selected for this study because of its proven architecture that facilitates fine-tuning via transfer learning. Its deep structure enables VGG16 to identify intricate features in currency images that simpler models may miss. Additionally, it offers the benefit of easy implementation and can attain high accuracy even with a smaller amount of training data through transfer learning.

### III. METHODOLOGY

#### A. Dataset Preparation

We obtained our dataset from the DataMendely platform, specifically the Indian Currency Dataset. This dataset comprises ten thousand images featuring various denominations (10, 20, 50, 100, 500, 2000) with authentic samples. To enhance feature generalization, we applied data augmentation meth-

ods including cropping, brightness modification, and rotation adjustments.

**B. Model Architecture**

VGG16 (Visual Geometry Group 16), a 16-layer CNN, is used to detect unrecognizable features that are not obvious to the naked eye. VGG16 uses transfer learning with ImageNet weights applied, followed by additional training on currency-specific features such as watermark detection and serial number verification.

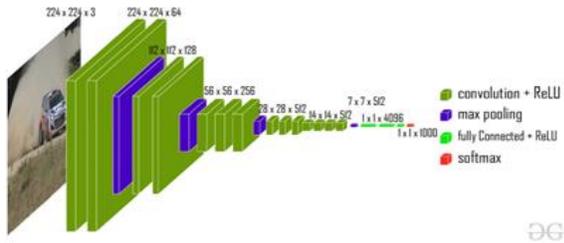


Fig. 2: VGG 16 Architecture

It consists of 16 layers, including 13 convolutional layers and 3 fully connected layers, organized into blocks. Each block features multiple convolutional layers followed by max-pooling layers for downsampling. The input dimensions are set to (224, 224, 3), and the architecture includes various layers with increasing filter counts (64, 128, 256, and 512 filters). The output is flattened into a vector and processed through fully connected layers, culminating in a softmax layer that outputs probabilities for 1000 classification categories. The simplicity and uniformity of the VGG-16 design make it accessible for implementation in image processing tasks.

**C. Detection Pipeline**

Legit scan’s detection process involves:

*Preprocessing:* Images are resized to (224 × 224 × 3) and normalized.

*Feature Extraction:*

The VGG16 model extracts feature patterns like fine threads, ink consistency, and watermarks.

*Authenticity Metrics:* The output consists of:

- Authenticity percentage
- Graphs representing trends in ink, watermark, micro patterns, and more
- Verdict: Genuine/Counterfeit

**D. System Architecture**

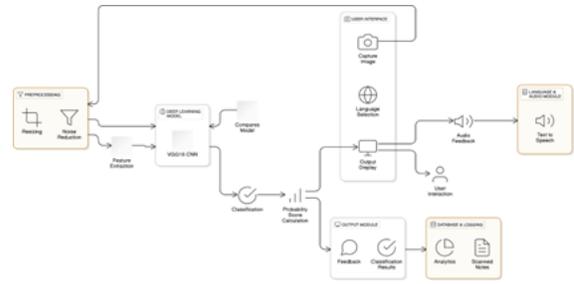


Fig. 3: System Architecture

The proposed currency authentication system leverages deep learning to verify the authenticity of banknotes. The workflow is outlined as follows:

- 1) *Image Capture:* The user captures an image of the currency note via the application.
- 2) *Preprocessing:* The image undergoes resizing and noise reduction to enhance feature extraction.
- 3) *Feature Extraction:* The preprocessed image is fed into a VGG16-based Convolutional Neural Network (CNN) to extract key features.
- 4) *Classification:* The extracted features are compared against a trained model to classify the note as genuine or counterfeit.
- 5) *Probability Score Calculation:* A confidence score is computed to quantify the classification certainty.
- 6) *Output Display:* The classification result, along with feedback options, is presented to the user.
- 7) *Audio Feedback:* A text-to-speech module provides verbal confirmation, enhancing accessibility.

This structured pipeline ensures real-time, accurate, and user-friendly currency verification. The incorporation of deep learning enhances classification accuracy, while the audio module improves accessibility, particularly for visually impaired users.

**IV. IMPLEMENTATION & FEATURES**

*Describes Legit scan’s user interface and system features.*

Legit scan is implemented as an Android application using TensorFlow Lite for inference. The following features enhance usability:

- A. *User Interface (UI)*
  - a. Users select a regional language, e.g., Hindi, Telugu, or English (Fig. 4).
  - b. The app supports scanning via the camera or gallery uploads (Fig. 5).

c. Results include authenticity scores, verdicts, and graphical representations (Fig. 6).

**B. Audio Feedback**

The app supports audio feedback, and reading out authenticity results in the user’s preferred language for improved accessibility.

**V. RESULTS & PERFORMANCE**

**A. Performance Metrics**

Legit scan achieves high precision under vary- ing conditions, summarized in Table II. The performance metrics are calculated as follows:

- **Accuracy:** This measures the proportion of correct predictions made by the model relative to the total number of instances evaluated.
- **Precision:** This indicates the proportion of instances identified as positive by the model that are truly positive.
- **Recall:** This measures the proportion of ac- tual positive instances that the model correctly identifies as positive.

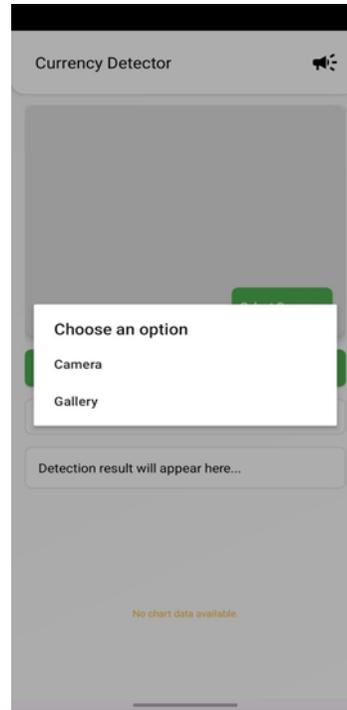


Fig. 5: Currency scanning and image upload inter- face.

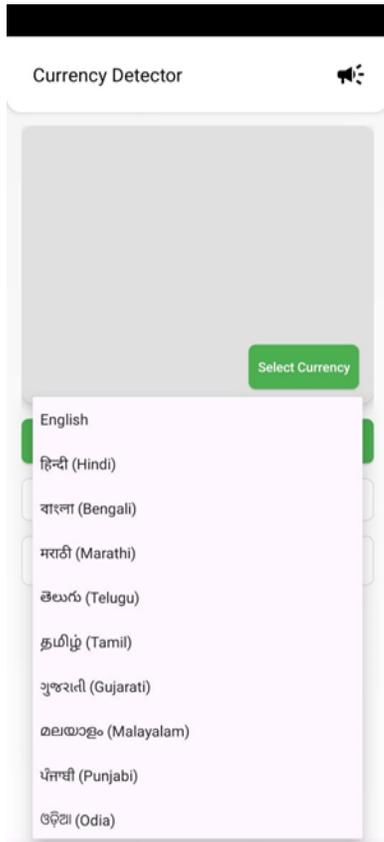


Fig. 4: Language selection menu.



Fig. 6: Graphical trends for features like ink align- ment and watermarks.

- **F1 Score:** A single metric that combines precision and recall to provide a balanced assessment of a model’s performance.
- **False Positives:** These are instances where the model incorrectly predicts a positive outcome when the true outcome is negative.

TABLE II: Performance Metrics

| Metric          | Value (%) |
|-----------------|-----------|
| Accuracy        | 98.7      |
| Precision       | 98.9      |
| Recall          | 98.5      |
| F1 Score        | 98.7      |
| False Positives | 1.3       |

**B. Mobile UI Results**

Figures 7 and 8 illustrate examples of graphical feedback provided by the app.

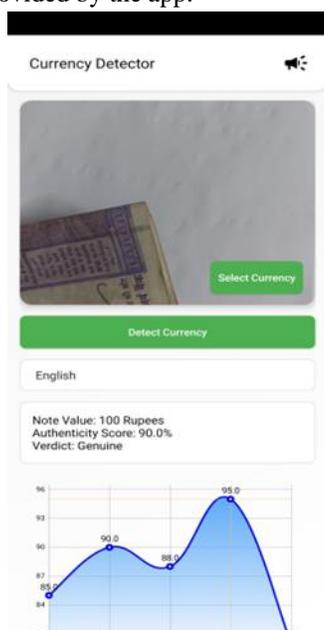


Fig. 7: Detection Example: 100 Note - Genuine (Score: 90.0%). Feature trends such as watermark clarity, ink quality, and serial number integrity are depicted.

**C. Real-World Evaluation**

- *Bright Lighting*: Accuracy 94% across clean and properly focused images.
- *Low Light*: Accuracy dropped to 85%, indicating the need for enhanced preprocessing.
- *Blurred Images*: Detection accuracy reduced due to feature loss.

**VI. CONCLUSION & FUTURE WORK**

By combining image classification with Android accessibility, Legit scan is a potent AI-driven application for counterfeit currency detection that achieves high accuracy.

- 1) Adding ultra-modern counterfeits to the dataset is one of the upcoming breakthroughs.
- 2) Including blockchain based transaction logging verification.
- 3) Improving preprocessing methods for low-light images.

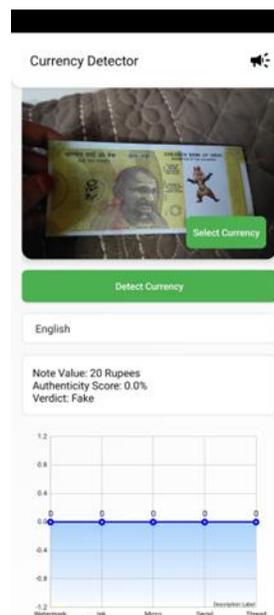


Fig. 8: Detection Example: 20 Fake Note (Score: 0%). Graph highlights very weak score trends for micro-pattern analysis.

The project has enormous scalability potential, particularly in areas without access to sophisticated counterfeit detection equipment.

**REFERENCES**

- [1] K. Simonyan and A. Zisserman, ‘Very Deep Convolutional Networks for Large-Scale Image Recognition,’ arXiv preprint arXiv:1409.1556v6, Apr. 2015.
- [2] J. Brownlee, ‘A Gentle Introduction to Transfer Learning for Deep Learning,’ Machine Learning Mastery, Dec. 2017. [Online]. Available: <https://machinelearningmastery.com/transfer-learning-for-deep-learning/>
- [3] OECD/EUIPO, ‘Trends in Trade in Counterfeit and Pirated Goods,’ OECD Publishing, 2019.
- [4] A. Sharma, V. Srinivasan, V. Kanchan, and L. Subramanian, ‘The Fake vs. Real Goods Problem: Microscopy and Machine Learning to the Rescue,’ in Proceedings of KDD ’17, Aug. 13-17, 2017. [Online]. Available: <https://dl.acm.org/doi/10.1145/3097983.3098186>

- [5] Entrupy Inc., ‘AI Authentication for Luxury Goods,’ 2020. [Online]. Available: <https://www.entrupy.com/technology/>
- [6] A. S. erban, G. Ilas, , and C. Porus, niuc, ‘SpotTheFake: A CNN-Enhanced Platform for Counterfeit Goods Detec- tion,” in *Journal of Computational Intelligence*, vol. 38, no. 3, pp. 257–270, 2022.
- [7] M. Tan and Q. Le, ‘EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks,” in *International Con- ference on Machine Learning*, 2019. [Online]. Available: <https://arxiv.org/abs/1905.11946>
- [8] United Nations Office on Drugs and Crime (UNODC), ‘Counterfeit Currency and Emerging Threats in Asia,” *Tech. Rep.*, 2022.
- [9] Y. Jia, W. Deng, and H. Li, ‘Augmentation and Fine-tuning Strategies for Counterfeit Detection Models,” in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 2, pp. 530–543, 2022.
- [10] C. Chen, G. G. Lee, and M. Davis, ‘Counterfeit Detection by Image Processing Techniques: A Review,” in *IEEE Access*, vol. 8, pp. 125384-125399, 2020.
- [11] N. A. Arayal, M. F. C. Abud, and N. H. Alshamrani, ‘A Comparative Study of Machine Learning Algorithms: Ap- plication in Currency Recognition,” in *2021 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, pp. 375-380.
- [12] X. Zhan and K. Lam, ‘Multi-Spectral Imaging for De- tecting Counterfeit Banknotes,” in *Journal of Sensors*, vol. 2018, Article ID 7260573, 2018.
- [13] M. Caputo, L. de Rop, and T. Voelker, ‘How to Fight Counterfeiting: Blockchain Applications in Currency De- vices and Detection Systems,” in *Journal of Cryptography and Security*, vol. 4, no. 2, pp. 99-118, 2021.
- [14] S. Misra, S. Gupta, and A. Kumar, ‘Automatic currency recognition using deep learning: A comparative analysis of CNNs and SVMs,” in *International Journal of Computer Applications*, vol. 175, no. 1, pp. 14-19, 2021.