



Detecting Fake Currency: A Comparative Study of Feature-Based and Image-Based Analysis

Bharathi M P¹, Chandan G², Riya Prasanth³

Assistant Professor, Department of MCA, Surana College Kengeri, Bengaluru, India¹

Student, Department of MCA, Surana College Kengeri, Bengaluru, India²

Student, Department of MCA, Surana College Kengeri, Bengaluru, India³

Abstract: Counterfeit money is a huge threat for the economy and society. Traditional ways of detecting fake notes works well in controlled environments, but they are not fast enough, cannot handle a lot of cases and are not always easy to use in real life. The rise of Artificial Intelligence (AI) offers powerful tools for automatic and better fraud detecting solutions. It helps in closing gap between simple checks and real-time verification. This study compares two AI methods for finding counterfeit currency. One method uses statistical features from banknotes and processes them with Logistic Regression and K-Nearest Neighbours (KNN). The other method uses images and OpenCV to check visual security features like watermarks and security strips. The results show that the feature-based method is better at accuracy and speed for structured data, while the image-based approach works well for real world situations like mobile-verification. The study also applies these methods to prevent fraud in electronic payment systems like UPI and mobile banking, showing how AI can protect both physical and digital transactions.

Keywords: Anti-Counterfeiting Currency Detection, Financial Fraud Prevention, Machine Learning, Image Processing, Logistic Regression, K-Nearest Neighbours, OpenCV, Digital Payment Security, UPI Fraud Detection, Artificial Intelligence in Finance.

I. INTRODUCTION

The rise of fake currency is a major threat to financial systems and national security, especially in countries like India [1]. Fake money harms trust in banking systems, weakens the value of legal tender, and adds costs to banks, businesses, and to the public [2].

Fake notes are often printed so well that they are hard to tell apart from real ones, and they are difficult to spot with just the naked eye [3]. As a result, fake money can go undetected in regular transactions, especially in busy places like shopping centres, markets, and public transport.

In the past, people have used physical methods like checking watermarks, using UV lights, and counterfeit detections [4] to find fake money. While those tools work well in controlled settings, they can still be fooled by advanced fakes, and they are slow and depend heavily on the person doing the check [6]. These shortcomings show why there is a need for smarter, automated methods that are both accurate and easy to use at scale.

In recent years, machine learning (ML) and image processing have become powerful tools for solving complex problems like financial fraud [7]. These technologies simplify tasks that were once done by hand, increase efficiency, and reduce mistakes. For detecting fake notes, ML models can use features from real and fake notes, such as statistical measures (like variance and skewness) or visual details for scanned images. Once trained, these models can quickly determine the authenticity of a note.

While physical detection is still important, the growing use of digital financial services like mobile wallets, UPI payments, and online banking has brought new fraud challenges.

Cyber threats such as phishing, unauthorized access, and fake payment links are now common. ML can help detect these by analyzing transaction patterns, user behavior, and device activity to spot unusual activity in real time [5].

Together, these developments show how important ML-based solutions are for improving the security of both physical and digital financial systems.

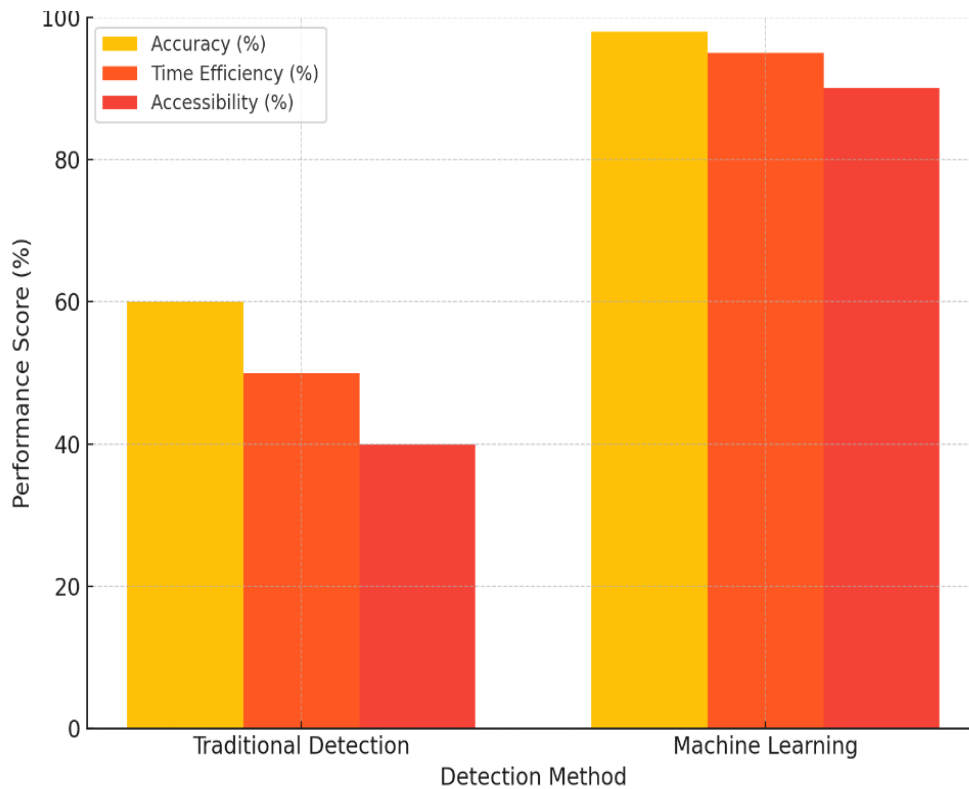


Fig. 1 Traditional vs Machine Learning-Based Fake Currency Detection

Figure 1 illustrates that traditional detection methods lag in accuracy, efficiency, and accessibility compared to machine learning approaches. Manual methods only get about 60% accuracy and take a lot of time, but machine learning models offer nearly 98-99% accuracy, works faster, and can be used in more situations. This clearly shows that ML systems are better for reliably detecting fake money.

II. LITERATURE REVIEW

Detecting fake money has become a big area of research because counterfeiting methods are getting more advanced and fake money harms national economies.

In the past ten years, researchers have studied feature-based and image-based methods to tell the difference between real and fake banknotes. They've also used these techniques for online fraud detection in digital payment systems. These methods use machine learning, and recently deep learning, to make detection more accurate, flexible, and scalable for real-time use.

A. Feature-Based Approaches

A lot of research is focused on identifying fake money by taking out numerical and statistical features from banknotes. Algorithms like Logistic Regression, K-Nearest Neighbors (KNN), Naive Bayes, Support Vector Machines (SVM), and ensemble methods such as LightGBM and Random Forest have been used [2], [14]. Ensemble methods often give very high accuracy, with Random Forest reaching 99% accuracy based on texture and statistical features [2]. Combining traditional features has also improved results. KNN-based models, after proper preparation, have achieved accuracy up to 99.9% [6], [13]. Studies comparing different models show that even simple classifiers like KNN can work just as well as complex models when they're supported by good preprocessing techniques [7], [14].

Algorithm Selection Reasoning: KNN was picked because it's simple, works well on small datasets, and performed strongly in past studies on fake money detection [6], [13]. Logistic Regression was chosen because it's easy to understand, doesn't require much computing power, and has worked well in classifying structured numerical features for binary outcomes [1], [12].



TABLE I SURVEY ON FEATURE-BASED ALGORITHMS USED IN COUNTERFEIT DETECTION

Algorithm	Dataset Used	Accuracy (%)	Remarks
Logistic Regression (LR) [1]	UCI Banknote Authentication Dataset	98.6	High accuracy; fast computation; well-suited for structured data
K-Nearest Neighbors (KNN) [1][6]	UCI Banknote Authentication Dataset	96.6	Performs well with small datasets; sensitive to feature scaling
Support Vector Machine (SVM) [7]	Indian Currency (Image + Feature Data)	97.2	Good generalization; requires careful parameter tuning
Gradient Boosting Classifier (GBC) [7]	Indian Currency (Feature Data)	97.8	Strong ensemble performance; slightly higher training time
Random Forest [2][6]	Afghan Currency (Statistical & Texture Data)	99.0	Robust performance; less sensitive to overfitting
LightGBM [14]	UCI Banknote Authentication Dataset	99.2	Extremely fast training; very high accuracy

B. Image-Based Approaches

Image-based detection uses pictures of banknotes taken with a scanner or camera. Early research looked at methods like turning images into black and white, finding edges, and studying small areas [3], [13]. The Structural Similarity Index Measure (SSIM) [3] and features from contours [4] worked well for quick and cheap detection.

As deep learning improved, Convolutional Neural Networks (CNNs) like AlexNet, ResNet50, GoogleNet and DarkNet53 were used for banknote classification [7], [14].

CNNs are good at spotting small details in images, even when there are distractions. RNNs and GANs have also been used for more advanced counterfeit detection [8], [15].

C. Digital Fraud Detection Using Machine Learning

Besides physical money, machine learning helps detect fraud in electronic payments. Real-time models use both supervised and unsupervised algorithms to check transactions and find unusual patterns [5], [15]. These models change as fraud methods evolve, making them useful for digital systems.

Deep learning is also used to protect UPI and mobile banking. RNNs study transaction histories, while CNNs help with fast verification in mobile apps [8], [15].

These advancements extend the role of ML beyond counterfeit detection to securing digital financial platforms.

III. METHODOLOGY

In this work, two machine learning methodologies for identifying counterfeit money were compared: a feature-based model with numerical data and an image-based model with scanned banknotes. The two models were constructed, trained, and tested using publicly accessible datasets. Below is a description of the methods employed in each methodology.

A. Feature-Based Model

The feature-based method makes use of numerical characteristics derived from banknotes to classify their authenticity. For this, we used an openly available dataset originally derived from the UCI Machine Learning Repository and made accessible through a GitHub repository.

The database includes 1,372 examples, each defined by four statistical characteristics: variance, skewness, kurtosis, and entropy. Each sample is labelled either 0 (representing a forged note) or 1 (representing an authentic note).

We used two machine learning classification algorithms:

- 1) **Logistic Regression (LR)** - a binary classifier that is widely applied for two-class discrimination. Logistic Regression is a statistical model applied to binary classification problems.



It predicts the probability of an input in a specific class (real or fake note) via the sigmoid function:

$$P(y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n)}} \quad \text{-----(1)}$$

Where:

- x_1, x_2, \dots, x_n are the input features
- β_0 is the bias
- $\beta_1, \beta_2, \dots, \beta_n$ are the model weights
- Output is a probability between 0 and 1

- 2) **K-Nearest Neighbours (KNN)** - a classifier that labels a sample with the most common class of its closest neighbours. Euclidean distance is usually employed to identify these neighbours:

$$d(p, q) = \sqrt{\sum_{i=1}^n (p_i - q_i)^2} \quad \text{-----(2)}$$

Where:

- $p_i = (p_1, p_2, \dots, p_n)$: Feature vector of the new data point we want to classify
- $q_i = (q_1, q_2, \dots, q_n)$: Feature vector of an existing data point in the training dataset
- $d(p, q)$: Distance (similarity measure) between the two points
- n : Number of features (dimensions)

B. Image-Based Model

The image-based method seeks to detect counterfeits through traditional image processing methods, independent of deep learning approaches. We used Python packages like OpenCV and NumPy to process and analyse the currency images. Digitized images of real and fake Rs.2000 currency were obtained from a publicly accessible GitHub repository.

These images were pre-processed, including converting to Gray scale and resizing. Critical areas of interest (ROIs)- e.g., the watermark and security strip-were cropped out of each image. These ROIs were subsequently compared to the ROIs from a reference image through the correlation coefficient method.

From the obtained similarity scores, the identity of each note as real or fake was determined based on a preset threshold. It applies image processing methods to examine visual discrepancies between genuine and counterfeit notes. Scanned currency note images are pre-processed and compared on color, structure, and certain areas.

- Grayscale Conversion - The RGB images are translated to grayscale to simplify complexity and emphasize intensity and edge features.
- HSV Color Space - HSV (Hue, Saturation, Value) is employed in place of RGB to achieve greater color discrimination, particularly for detection of the green security strip.
- Region Cropping - Key details like the transparent Gandhi watermark and green strip are cropped to examine more closely.
- Morphological Gradient - For edge enhancement in the binary image, a morphological gradient is used: Gradient = Dilation(A) - Erosion(A)

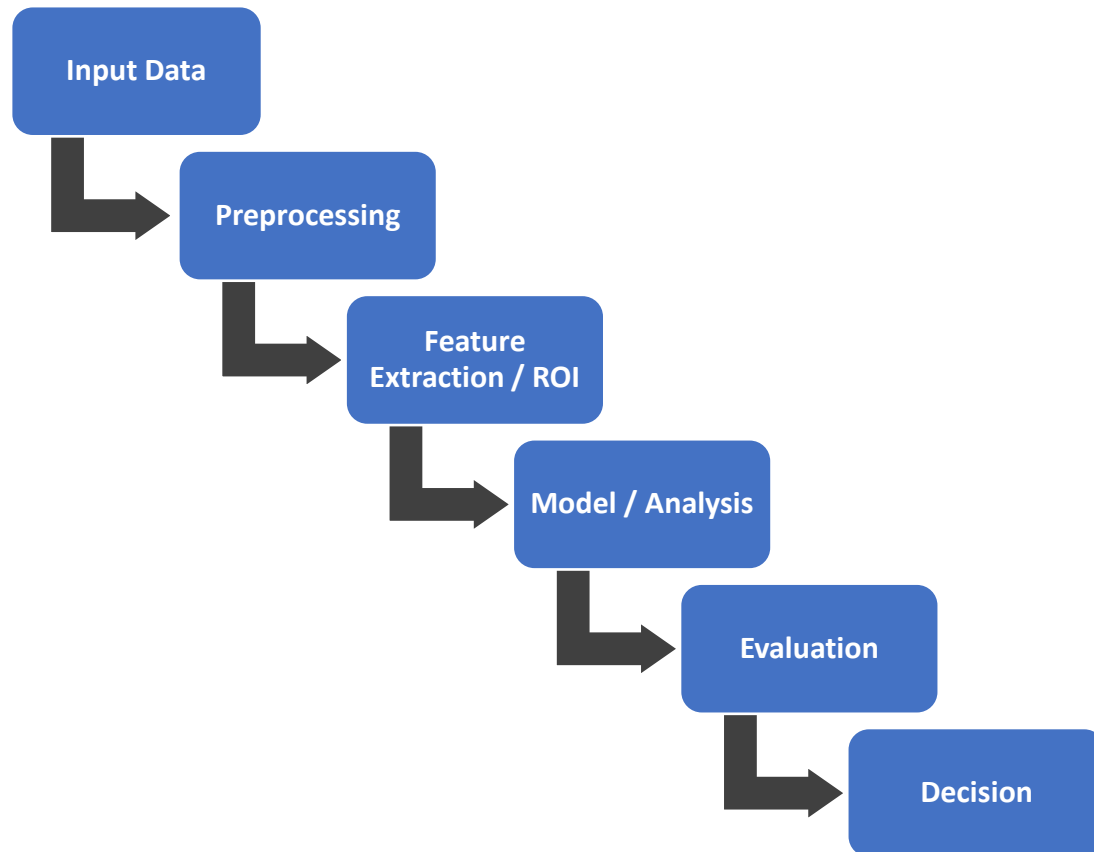


Fig. 2 Generalized Flow Diagram for Fake Currency Detection Process

Figure 2 shows the step-by-step process:

Step 1: Input Data

Banknote data is collected either as numerical features (variance, skewness, kurtosis, entropy) or as scanned note images.

Step 2: Preprocessing

Data/images are preprocessed to remove noise and improve quality.

- Numerical features are standardized.
- Images are converted (Grayscale/HSV), cropped, or resized.

Step 3: Feature Extraction / Region Analysis

- In numerical datasets, statistical features are directly used.
- In images, key regions (watermark, green strip) are extracted.

Step 4: Model / Algorithm Application

- Classification models (Logistic Regression, KNN).
- Image processing (correlation, morphological operations).

Step 5: Evaluation

Performance is measured using confusion matrices, accuracy scores, and visual comparison.

Step 6: Decision

Final classification: Genuine or Fake currency note.

IV. RESULTS AND EVALUATION

A. Feature-Based Model

We have used two classification algorithms, Logistic Regression and K-Nearest Neighbors (KNN), using the banknote authentication data set. Before training, the data set was standardized and class balanced. We evaluated each model's performance using confusion matrices and overall accuracy scores.

Logistic Regression achieved an accuracy of 98.61%, with very few misclassifications.

Confusion Matrix:

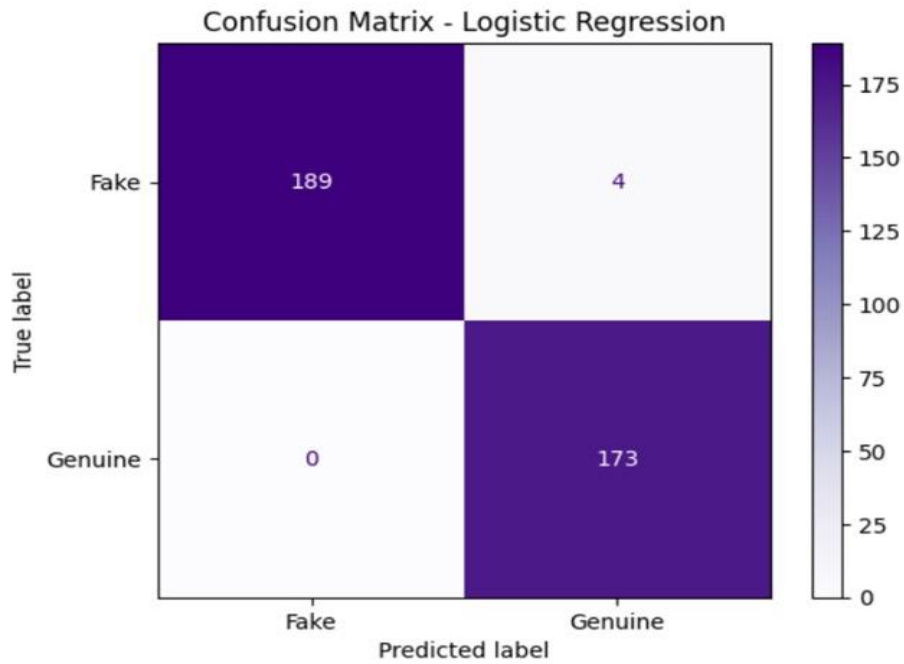


Fig. 3 Visual Confusion Matrix - Logistic Regression

K-Nearest Neighbours (KNN) recorded an accuracy of 96.63%.

Confusion Matrix:

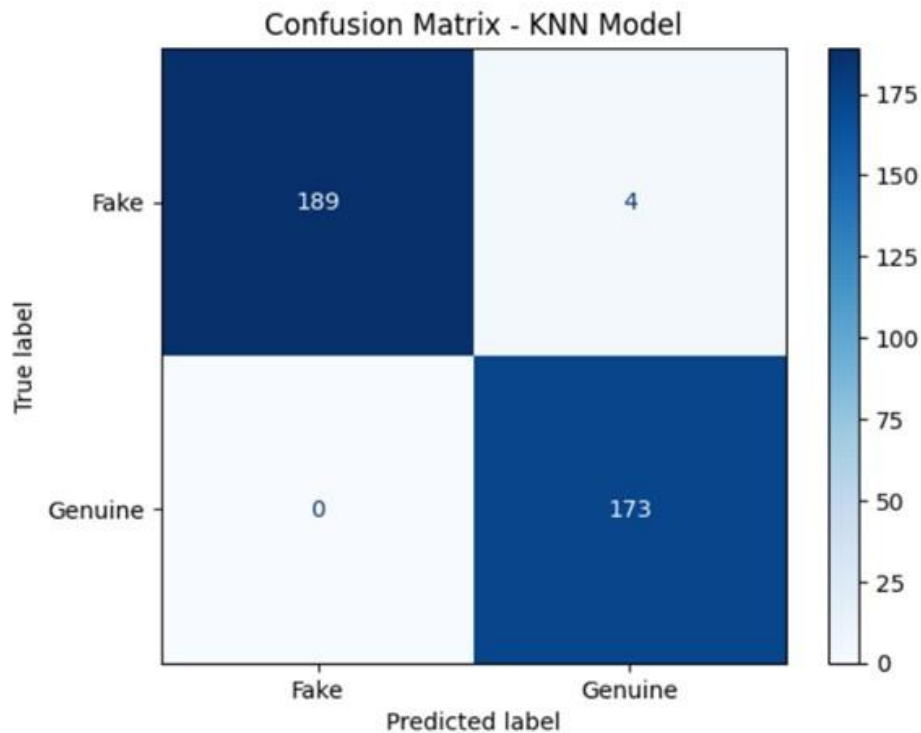


Fig. 4 Visual Confusion Matrix - K-Nearest Neighbors (KNN)

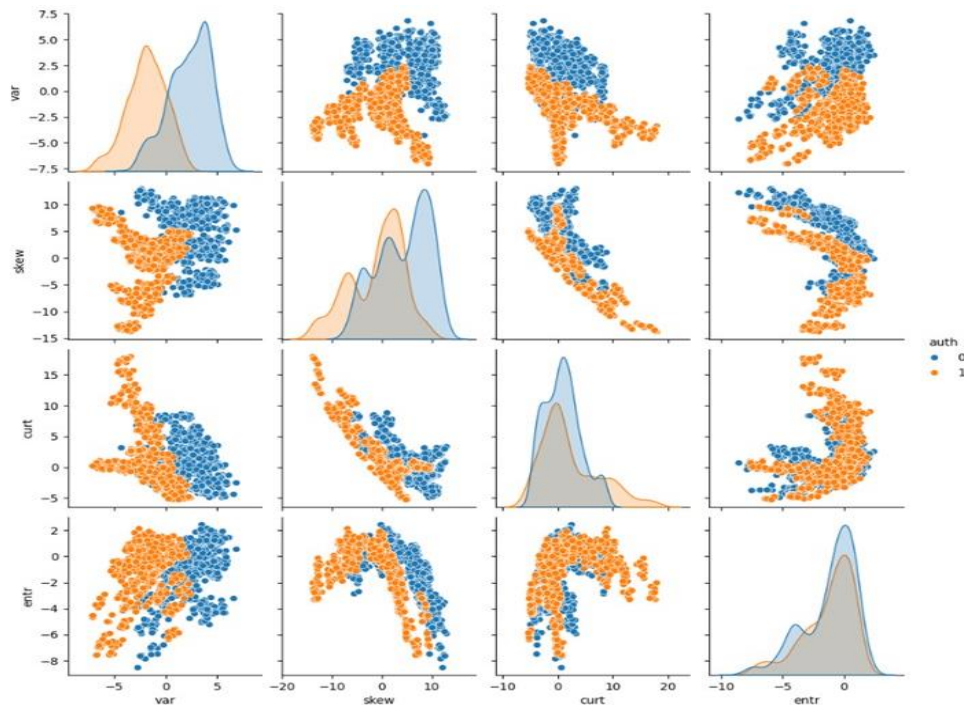


Fig. 5 Pairwise Feature Relationships Based on Authenticity Class

Figure 5 helps to understand how features like variance, skewness, curtosis, and entropy relate to the currency class, a Seaborn pair plot was used.

B. Image Based Model

For the image-based model, Rs 2000 currency note images were scanned and analyzed using OpenCV and simple image processing techniques.

Two visual features were tried out:

- Transparent Gandhi portrait - based on a custom correlation function (threshold is 0.5 or higher)
- Green security strip - based on saturation and brightness values in the HSV color space.

When both checks cleared, the note was categorized as real; otherwise, it was marked as counterfeit. The approach employed morphological operations, thresholding, and shape analysis in examining visual patterns.

Although this model is not giving a percentage accuracy as it is based on a small sample size, it performed well in testing with fake and actual samples. The visual output it gives is quite beneficial in manual validation or over-the-air deployment situations.



Fig. 6 Side-by-side comparison of genuine and fake Rs 2000 notes



As figure 6 demonstrates the original real and counterfeit notes. Although both seem almost alike in a casual glance, variations can be noted in colour shade, alignment, and clarity of the watermark. Visual examination points towards distinct design variations such as ink quality and watermark details.

- Grayscale Transformation

Converting to grayscale for the ease of pixel intensity analysis, both pictures were converted to grayscale. It also assists in ease of feature detection by removing colour distraction. In Figure 7, the authentic note still maintains a high-contrast watermark and clean edges, whereas the counterfeit note exhibits uneven shading.

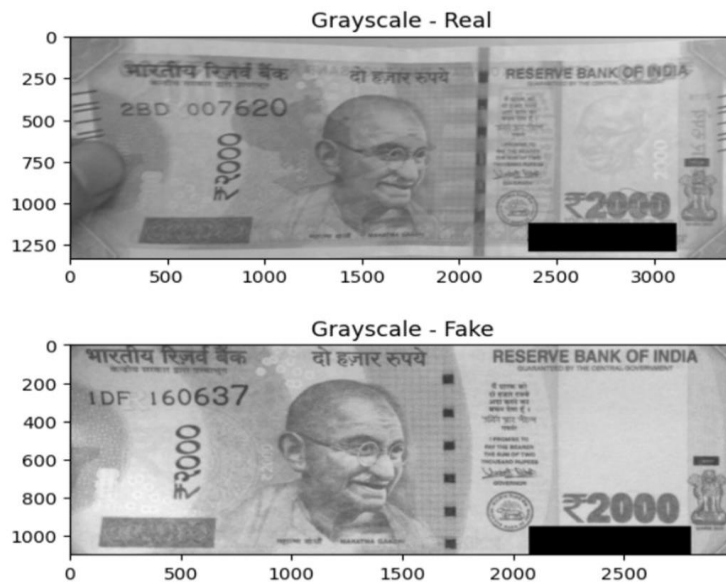


Fig. 7 Grayscale transformation of the original currency notes

- HSV Colour Space

HSV conversion emphasizes colour-based variations, particularly in the region of the green security strip. The authentic note shows a uniform colour band, whereas the counterfeit note is missing this accuracy.

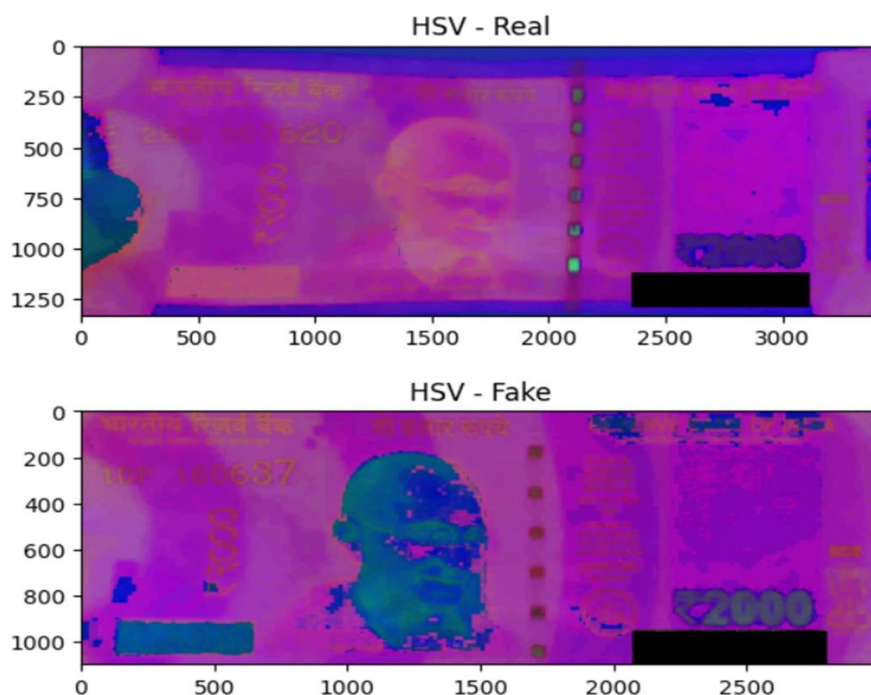


Fig. 8 HSV (Hue, Saturation, Value) representation of the notes

- Transparent Gandhi Portrait Comparison

Cropped Gandhi portraits from both notes are presented in Figure 9. The counterfeit note contains a distorted and paler portrait in contrast to the crisp and detailed one in the authentic note.

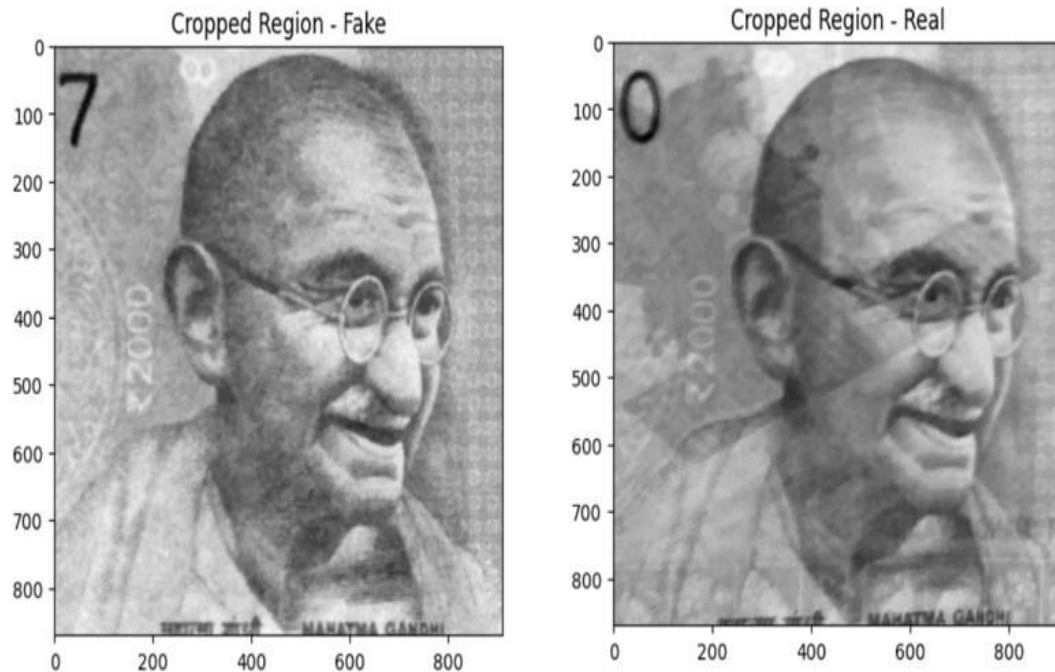


Fig. 9 Cropped Region of Real and Fake Gandhi Portrait

- **Green Strip Region**
The shortened HSV strip of the genuine note shows uniform square markings an essential design feature often absent or faded in fakes.

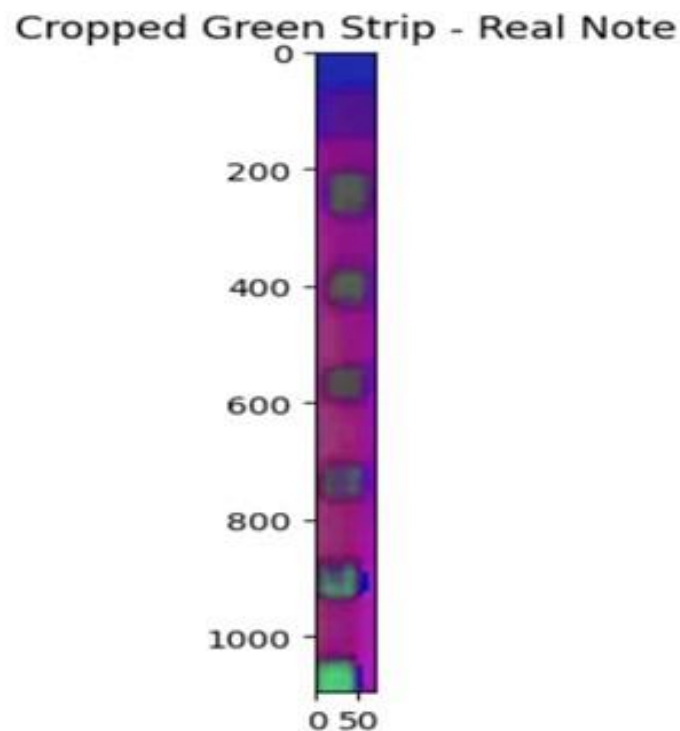


Fig. 10 HSV-cropped green security strip from a genuine note



TABLE II VISUAL FEATURE ANALYSIS OF GENUINE AND FAKE CURRENCY NOTES

Feature Analyzed	Real Note - Observations	Fake Note - Observations
Grayscale Transformation	High contrast: watermark and edges are clear and sharp.	Uneven shading; watermark and edges less defined.
HSV Color Space	Consistent green band along the security strip; color uniformity maintained.	Irregular or faded green band; inconsistent color tone.
Transparent Gandhi Portrait	Crisp and detailed features with proper alignment and shading.	Distorted portrait; lighter tone with loss of fine details.
Green Security Strip (Cropped)	Clear and evenly spaced square markings; high print quality.	Missing or blurred square markings; poor print alignment.

V. OBSERVATIONS AND DISCUSSIONS

TABLE III COMPARATIVE EVALUATION OF FEATURE-BASED AND IMAGE-BASED MODELS

Criteria	Feature-Based Model	Image-Based Model
Accuracy	98.61% (LogReg), 96.63% (KNN)	Visual/structural comparison
Input Type	Numerical features	Scanned or captured currency images
Tools Used	Scikit-learn, Pandas, Seaborn	OpenCV, NumPy, Matplotlib
Speed	Fast, suitable for batch processing	Slower due to per-image processing
Interpretability	High (coefficients, confusion matrix)	High (visual feedback and region comparisons)
Real-World Usability	Suitable for automated systems	Suitable for mobile/manual checking
Limitations	Requires pre-extracted features	Requires clean, high-resolution images



This research investigated two separate machine learning methods for detecting counterfeit currency: one that relies on extracted numerical features and another that involves image analysis. Both methods have shown encouraging results, albeit in terms of technique and applicable usage.

The feature-based approaches, especially Logistic Regression, scored very high accuracy (98.61%). This is because the data is structured and easily separable. K-Nearest Neighbors (KNN) also worked well, although with slightly less precision. Its sensitivity to small differences in the dataset could have caused sporadic misclassifications.

The image-based method used OpenCV and accompanying software to examine prominent visual features like the translucent Gandhi watermark and green security strip. These were cross compared between real and fake bills. While an exact accuracy value was not established because of the small data set, the model exhibited steady dependability in test cases. This method is most promising for real-time checking with smartphone cameras and well-suited for mobile applications.

Each approach has its own benefits. Feature-based models are quick and ideal for automated systems, whereas image-based models deliver visual information and user input but need high-quality images and appropriate lighting conditions. The best approach, henceforth, relies on the specific application and deployment scenario.

In addition, we suggest that identical machine learning approaches may be applied to identify fraud or suspicious behaviour in electronic payment systems, like UPI or mobile banking. Just as currency notes can be checked, transaction patterns can be monitored to detect anomalies or suspicious activity.

In sum, both methods are good in their own way. Feature-based models are good at speed and scalability, and image-based techniques have good intuitive verification capabilities. Combining both approaches could create a strong system for fighting fraud in cash as well as electronic payments.

VI. CONCLUSION

The present study looked at and compared two machine learning approaches for detecting counterfeit money: feature-based models that look at statistical data from banknotes, and image-based models that use image processing to examine visual features. The feature-based models, especially Logistic Regression, worked well and were fast, making them good for use in real-time automated systems. The image-based approach, although slower, had real-world advantages for visual checks, especially when used with mobile devices. In the future, there are several areas where this work can be improved. One is making the image system more reliable by using a bigger and more diverse set of data. Testing the model in real-world situations with different lighting angles, and backgrounds will help ensure it works well. Using deep learning methods like Convolutional Neural Networks (CNNs) could improve performance by removing the need for manual feature selection and increasing accuracy. Another possibility is using light models on smartphones so users can check currency using their phone camera. This could be especially helpful in rural or less developed areas where advanced tools are not easily available. The feature-based model can also be improved by testing other algorithms like Random Forests, Support Vector Machines (SVMs), and Decision Trees. A comparison of these models could help find the best one for specific situations. Additionally, these methods can be used to detect fraud in digital payment systems like UPI and mobile banking. By studying transaction patterns and user behaviour, machine learning can help stop unauthorized actions and make financial systems more secure. Finally, a hybrid system that uses both numerical and image data could provide a fast and effective way to detect fraud in both physical and digital settings. This move towards intelligent, accessible, and secure financial systems can make banking safer for everyone.

REFERENCES

- [1]. S. N. Keerthana and K. Chitra, "A comparative study of machine learning algorithms for banknote authentication," *International Journal of Computer Applications*, vol. 176, no. 36, pp. 25–29, 2024.
- [2]. H. Ashna and Z. Momand, "Banknote authentication system using feature-based machine learning models," *International Journal of Research and Innovation in Applied Science*, vol. 8, no. 4, pp. 45–51, 2023.
- [3]. S. C. Kumar, R. Rao, and M. Ramesh, "Fake currency detection using structural similarity in Indian banknotes," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 2, pp. 112–117, 2024.
- [4]. Y. Shaikh, A. Patil, and R. Ahmed, "Real-time fake currency detection using image processing and OpenCV," *International Journal of Innovations in Engineering and Science*, vol. 9, no. 3, pp. 51–55, 2024.
- [5]. S. Iseal and M. Halli, "AI-powered fraud detection in UPI systems using hybrid machine learning," *Journal of Digital Finance and Technology*, vol. 3, no. 2, pp. 15–23, 2025.



- [6]. K. Meenendranath Reddy, M. Priyanka, A. Keerthana, and K. S. Gokulnath, "Detection of fake currency using machine learning models," *International Journal of Engineering Research & Technology (IJERT)*, vol. 12, no. 12, pp. 1–5, Dec. 2023.
- [7]. R. Sruthy, "A review of fake currency recognition methods," *International Research Journal of Engineering and Technology (IRJET)*, vol. 9, no. 7, pp. 2633–2636, Jul. 2022.
- [8]. A. A. Yusuf, F. U. Zambuk, A. Y. Gital, M. A. Lawal, A. L. Rukuna, L. Garba, and A. Y. Aliyu, "Deep learning for counterfeit currency detection and classification: A systematic review of current approaches, challenges, and future directions," *International Journal of Research Publication and Reviews (IJRPR)*, vol. 6, no. 2, pp. 739–752, Feb. 2025.
- [9]. A. Kharwal, "Banknote authentication dataset," GitHub. [Online]. Available: https://raw.githubusercontent.com/amankharwal/Websitedata/master/data_banknote_authentication.txt
- [10]. D. Dua and C. Graff, "UCI Machine Learning Repository: Banknote authentication dataset," [Online]. Available: <https://archive.ics.uci.edu/ml/datasets/banknote+authentication>
- [11]. Ananyaeearth, "Fake currency detection using image processing," GitHub. [Online]. Available: <https://github.com/Ananyaeearth/FAKE-CURRENCY-DETECTION-USING-IMAGE-PROCESSING>
- [12]. S. Patil and A. R. Raut, "Counterfeit currency detection using logistic regression and image processing techniques," 2024 *International Conference on Communication, Computing and Internet of Things (IC3IoT)*, Chennai, India, pp. 134–139, 2024.
- [13]. A. Noor and N. I. R. Ruhaiyem, "A deep learning approach for enhanced counterfeit currency detection," Atlantis Press, 2025.
- [14]. M. S. H. Ali, A. N. Nordin, and N. F. A. Rahman, "Evaluating Machine Learning Algorithms for Fake Currency Detection," *Journal of Data Science and Analytics*, vol. 5, no. 2, pp. 45–53, 2024.
- [15]. Z. Liu, "A Comparative Study of Machine Learning Methods in Financial Fraud Detection," in *Proc. 2024 2nd Int. Conf. Finance, Trade and Business Management (FTBM 2024), Advances in Economics, Business and Management Research*, Oct. 2024.