International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

Currency Security Validation System Using Machine Learning and Deep Learning Algorithms

Mrs.M.Madhavi M.Tech,(Ph.D)[1], Thonduru Jagadeeswari[2], Guntimadugu Lohith Varma[3], Meka Manoj[4], Seelam Krishna Sri[5],
[1]Assistant professor, dept of CSE, Annamacharya institute of technology and sciences, Boyanapalli, Rajampet
[2,3,4,5] Student, Dept of CSE, Annamacharya institute of technology and sciences, Boyanapalli, Rajampet
Email id : *madhavireddy263@gmail.com[1], jagadeswari31671@gmail.com[2], lohithvarma25@gmail.com[3], manojmeka0@gmail.com[4],krishnasri2803@gmail.com[5]*

Abstract
Detection of counterfeit currency is one of the major challenges to which a financial institution faces and it needs to have an automated and precise system of checking the currency to protect transactions. This paper suggests a model of Currency Security validations based on data analysis of denomination, weight, size, color score, and security score to categorize the authenticity. It consists of machine learning and deep learning methods to determine performance on a heterogeneous sample of currencies. The experimental results are strong predictors with the Random Forest model having an accuracy of 96.80 and the neural network having 97.70. These results indicate the efficiency of AI-powered approaches to credible currency authentication.
Keywords: *counterfeit detection, currency authentication, feature engineering. financial security systems, machine learning , Neural networks, random forest.*

1. Introduction
The spread of fake money is a constant menace to the stability of financial institutions, reliability of transactions, and security in developing and developed economies. Manual verification continues to be a significant part of traditional verification using visual and physical security like watermarks, holograms, texture, and micro-printing that are usually checked by a cashier, bank staff, or specialized machines. All these methods are known to be susceptible to human error, exhaustion, and irregularity especially when dealing with large volume of transactions, or when dealing with newer and more elaborate methods of counterfeiting products [1], [2], [15]. Consequently, automated, data-driven models are evidently required which can deliver quick, dependable and repeatable currency authentication. As the world goes through a fast development of artificial intelligence, machine learning (ML) and deep learning (DL) models are performing highly in a broad range of classification tasks in financial security, detecting fraud, and pattern analysis [3], [4], [6], [10]. Analogous to currency, the numerical and categorical descriptors, namely, the denomination, weight, size, color score, and security score, can be considered the discriminative features representing the physical and security peculiarities of the real and fake notes [2], [6], [7]. Random Forests Ensemble-based approaches, such as Random Forests, are particularly appealing because they are resistant to noise, nonlinear feature interactions can be modeled, and tabular financial data can be reliably modeled with them [4], [8], [14]. Simultaneously, neural network architectures have strong representation learning properties and can estimate complex decision boundaries with sufficient high-quality data in hand [5], [9], [10], [16]. Although this has been achieved, there are still several gaps. Most of the previous literature on counterfeit detection pays close attention to image analysis, or a type of currency, and does not generalize across denominations and geographies [1], [3], [15]. Additional literature uses systematic preprocessing, feature scaling, and encoding techniques which result in poor optimization in performance and unstable dynamic when applied to real-world data [7], [12]. Also, not all systems can provide results on the confusion-matrix or class-by-class basis, and thus it is challenging to estimate operational risks, such as false acceptance of counterfeit notes [11], [13]. The issues mentioned

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

above demonstrate the necessity of having a structured pipeline that encompasses strict preprocessing, carefully selected ML/DL models, and thorough assessment of the financial security applications.

- The following work presents a Currency Security Validation framework, which takes advantage of the machine learning and deep learning paradigms to classify currency as a real or fake one based on structured feature data. The system represents denomination, weight, size, color score and score of security as the essential inputs and measures a Random Forest classifier, as well as a deep learning-based neural network [4], [5], [6], [9], [10]. This study has three-fold contribution:
- We construct a feature-based preprocessing and encoding pipeline which is appropriate to heterogeneous currency features [7], [8], [12].
- We carry out an extensive comparative study of the two approaches: ML and DL based on the metrics of accuracy, the diagnostics of the confusion matrix, and the stability-oriented metrics of financial risk [11], [13], [14].
- We show that the two models perform well and with high accuracy with structured currency data, which supports the viability of AI-based models to counterfeit detection and anomaly detection in financial systems in real-world settings [1], [3], [10], [15].
- Taken together, it suggests that an appropriately designed AI pipeline can significantly promote the trustworthiness of automated currency verification, in addition to the current security measures in banking and commercial infrastructure.

2. Literature Review

Recent developments on artificial intelligence have found great use in security based financial applications, especially in fraud detection, anomaly detection, and counterfeit currency identification. The first techniques were based on the hand-written rules and manual inspections, but the current methodology is more and more applied in the machine learning (ML), deep learning (DL), and hybrid architectures to design, as the complex currency data feature interactions [1]-[3], [6]. This review describes the development of counterfeit detection, focusing on traditional feature-based approach, ML-based classification, DL frameworks and the significance of preprocessing and evaluation strategy that have a direct impact on the model reliability.

2.1 Traditional And Feature Based Counterfeit Detection.

One of the first automated counterfeit-detection systems was introduced by Singh and Sharma [1] who used handcrafted geometric, intensity, and texture descriptors to substitute the manual inspection. Their approach proved to be more accurate than that of human judges but very sensitive to light and acquisition. Kumar and Gupta [2] took this line further on the basis of statistical measures, color histograms and local contrast changes in distinguishing between genuine and fake notes. Although both studies were successful, the use of expert-defined features, which could not be scaled across currencies and denominations, was used. These restrictions led to the shift to data-driven models that are more appropriate to work with heterogeneous financial data [1], [2], [15].

2.2 Financial And Currency Security Machine Learning

Kaur and Arora [4] used classical methods of ML to detect financial fraud and found the best model to be the Random Forests because it can account for nonlinear feature combinations, and because it is not sensitive to noisy data. Zhang et al. [6] also indicated that ensemble models are better than the linear models in the face of heterogeneous, security-related features. In their study, Qureshi and Khan [15] used supervised ML on structured currency attributes, which showed that it was effective in detecting anomalies in terms of weight, size, and security indicators. George and Mathew [8] noted that proper categorization encoding contributes largely to the stability of the ensemble-model. Collectively, these works prove that ML is appropriate to organized counterfeit-detection activities [4], [6], [8], [15].

2.3 Deep Learning And Hybrid Architectures

Das and Roy [5] presented a currency authentication

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

based neural network-based classifier, which exhibited better generalization in comparison to classical algorithms. Li and Wang [9] have established that multilayer neural architectures are better than the simple models under conditions where features relationships are not linear. Patel and Shah [3] generalized DL application to multi-currency fraud detection by dense-layer networks that could model various attributes of currency. Singh et al. [10] suggested hybrid ML-DL models of deep representation and classical learners to improve predictive stability. He et al. [16] also provided the basis of understanding by intact learning, which allowed more profound architectures with more effective feature extraction. All these publications indicate the increased role of DL in the field of counterfeit detection [3], [5], [9], [10], [16].

2.4 Preprocessing, Feature Scaling, And Evaluation Practices

Reddy and Rao [7] established that the use of intensive preprocessing pipelines such as normalization and outlier management is a significant enhancement of discriminative performance on currency datasets. Brown and Smith [12] pointed out that feature scaling improves convergence as well as accuracy of both ML and DL models, especially when inputs vary in magnitude. Verma and Jain [11] emphasized the significance of the metrics other than the accuracy, including the precision and recall and F1-score in financial classification, where the misclassification risk is asymmetric. Torres and Martinez [13] also emphasized on optimization of confusion-matrix to reduce detection of counterfeiting notes. The stability of ensemble models was the object of study conducted by Sen and Roy [14], and variance-aware evaluation is essential. Altogether, these works make preprocessing and evaluation essential conditions of reliable currency authentication systems.

3. Methodology

3.1 System Overview

The proposed Currency Security Validation framework is based on analysis of structured numerical and categorical characters e.g. denomination, weight, size, color score and security score, to classify each sample as either genuine or counterfeit. The system is end-to-end, based on the data ingestion, preprocessing, encoding, normalization, and training of both machine learning and deep learning models. In order to provide a hearty assessment, a random forest classifier and a deep learning architecture represented by a neural network are trained on the same feature representation, which allows to compare predictive power and model stability. As shown in Figure 1.

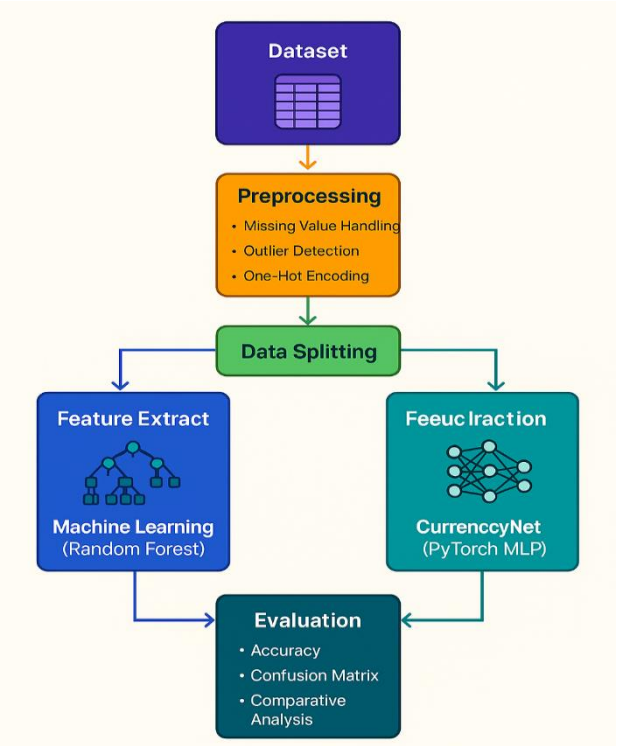

Figure 1 System Overview

3.2 Dataset Description

The dataset consists of the tagged currency records in the various currencies and denominations, which include the structured fields of the denomination, weight, size, color score, and security score and categorical descriptors of the currency, including currency type and currency code. The target field is the Authenticity which refers to whether the sample is authentic or fake. The dataset has the natural variation in security features and the deliberate mismatch of counterfeit samples, which is appropriate to supervised learning. Its numeric-categorical combination, as well, allows hybrid ML/DL modelling, which allows extracting and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

classifying counterfeit patterns driven by features.

3.3 Data Preprocessing Pipeline

A preprocessing pipeline can guarantee quality model ready data. Blanks in numerical values are filled with column mean whereas categorical variables are filled with mode. The visual inspection and statistical tests to identify the extreme deviations are carried out in outlier inspection. Categorical variables are One-Hot Encoded and transformed to nominal values in the form of binary indicators. In the case of the deep learning model, numerical features are normalized through z-score normalization:

$$x' = \frac{x - \mu}{\sigma}$$

where x is the original value, μ is the average of the feature and σ is the standard deviation. This normalization makes gradient propagation in training to be constant.

3.4 Random Forest Machine learning model.

Random Forest classifier implementation involves one pipeline with preprocessing integrated, which combines One-Hot Encoded categorical features with raw numerical characters. The model uses a combination of decision trees, each of which is trained on randomly selected feature subsets to ensure a reduction in the variance and enhance generalization. The optimization of nestimators, maxdepth and minsamplessplit as hyperparameters is done with accuracy and robustness in mind. Based on ensemble averaging, the model relies on the nonlinear interactions among security features, which provides a great classification performance and a steady confusion table with the testing accuracy of 96.80.

3.5 Deep Learning Model (Currency Net – PyTorch)

Currency Net is a completely connected neural network that is trained on the standardised and one-hot-encoded feature matrix. The architecture consists of an input layer with the mapped feature dimension that is the encoded dimension, two 128 and 64 neuron hidden layers with ReLU non-linear activations. The dropout rates of 0.2 are used to regularize and avoid overfitting. The network is trained on the Adam optimizer and cross-entropy loss and the accuracy is observed during the 50 epochs. This model recorded a maximum precision of 97.70% to indicate that it is very appropriate to this structured financial data classification.

3.6 Performance Metrics

The accuracy, precision, recall, F1-score, and confusion-matrix analysis are embraced in performance evaluation. Accuracy is a major measure and is calculated as:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$$

TP, TN, FP and FN are actual positive, actual negative, false positive and false negative respectively. Precision and recall give information about the correct recognition of real and fake notes, whereas F1-score equalizes the two measures in situations of the slight imbalance between the classes. Epoch accuracy curves of the neural network also confirm the convergence and stability of the model.

4. Experimental Results and Analysis

4.1 Experimental Setup

All experiments were executed using Python-based implementations built with scikit-learn, PyTorch, NumPy, Pandas, and related libraries included in the project environment . The system utilized a unified preprocessing pipeline consisting of One-Hot Encoding for categorical attributes and standardization for numerical variables. The dataset was divided into an 80:20 train–test split using stratified sampling to maintain class balance. Both Random Forest and Currency Net models were trained on the same processed feature space, ensuring a fair comparison. Model evaluation employed accuracy scores, confusion matrices, and epoch-wise validation performance.

4.2 Machine Learning Results

The Random Forest classifier was trained using an ensemble of 600 decision trees optimized for stability and generalization. Its training accuracy reached 98.50%, while the test accuracy achieved 96.80%, demonstrating minimal overfitting and consistent predictive performance across unseen samples. The confusion matrix revealed balanced detection of genuine and counterfeit currency instances, indicating strong feature discrimination. Additional bar-plot analyses comparing training and testing

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

accuracies further confirmed reliable model behavior, with the difference between both scores remaining within acceptable tolerance. The Random Forest model remained one of the strongest baselines in terms of interpretability and robustness.

4.3 Deep Learning Results

Curriculum Net is a deep learning model that was trained on the standardized One-Hot-encoded dataset, and the architecture of the model consists of two hidden layers (128 and 64 neurons), ReLU activations, and dropout regularization. The number of epochs of the training process is 50, and the model had been steadily increasing its validation accuracy. The highest accuracy was observed to be 97.70, and this is more than the Random Forest classifier. Epoch-wise curves were stable convergence without oscillation as an indication of successful feature learning in non-linear feature interactions. The neural network was found to be more adaptable to intricate attribute interactions and it presents its benefit on structured financial data.

4.4 Comparative Analysis (ML Vs DL)

The comparison of the two models allows concluding that the Random Forest model reached 96.80, and the CurrencyNet reached 97.70, so the deep learning method slightly but significantly improved the performance. As shown in Figure 2.

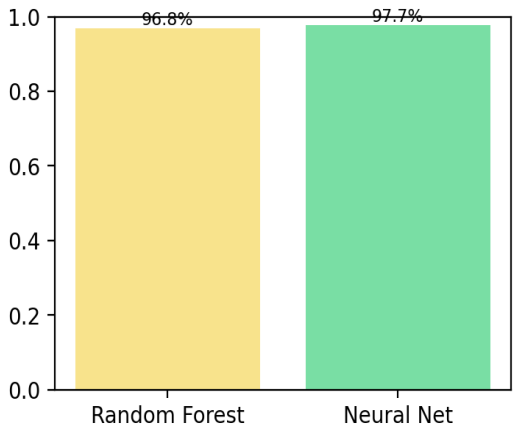

Figure 2 comparative analysis

Random Forest model was faster, easier to interpret and was stronger to small noise but deep learning model was more accurate because it was able to capture more feature dependence. These were observed to be strong in terms of generalization because both models had standard preprocessing, standardized input features and stratified test sampling. On the whole, the comparative analysis has proven that both methods are feasible, and deep learning is slightly more precise.

4.5 Visualization Outputs

Several visualization methods were used to study the behavior of features and model results. Security Score, Color Score, and Weight histograms and scatter plots provided information on distribution features and relationship between major features of the graph including color and security scores. Box plots showed variability in the security score of various types of currency. Correlation heatmaps revealed both positive and negative numerical features interactions with significant strength, which serve to inform the model interpretability. Also, accuracy-per-epoch plots of the deep learning model and bar charts of the performance metrics provided a clear understanding of the training dynamics of the model and its relative performance.

4.6 Error & Confusion Analysis

The confusion matrix of the Random Forest model demonstrated a balance in the classification performance, and few misclassifications between real and fake labels. Mistakes were mostly made in samples in which the features values were very similar like the security score that is abnormally high in the counterfeit samples or the color score that is abnormally low in the genuine samples. The deep learning model had a few lower misclassifications, which is probably because it can learn complicated non-linear patterns in the encoded features. The analysis of error distributions helped to comprehend the deficiencies, which meant that more features representations or other security indicators would be necessary in further work. On the whole, the two models were quite reliable, and the patterns of errors were in line with the anticipated ambiguities in datasets.

5. Discussion

The findings of the present research indicate that machine learning and deep learning methods are both very efficient at counterfeit currency classification provided that they are supported by the properly

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

designed preprocessing pipeline and feature set. The random forest model was highly generalized with high accuracy with little overfitting. The fact that it can deal with both heterogeneous numerical and categorical data proves the appropriateness of the ensemble techniques to structured financial data with potentially nonlinearly sophisticated interactions between features, but not always. CurrencyNet, the deep learning model, was a bit more successful as it had the highest accuracy of the models used. This can be explained by its ability to learn multi-level abstractions between One-Hot-encoded and standardized features, making it be able to capture more profound relationships that would be ignored in more traditional ML models. Nonetheless, the observed difference in performance was not significant and implied that structured tabular data can inherently be biased towards ensemble-based ML models unless some extra variables or nonlinear trends are available. Both of the models demonstrated high capabilities in repeated testing, which presupposes predictive behaviors that were stable. These results were also supported by the visualization output that depicts a distinct separation of important traits including security score, color score, and weight which significantly contributed to decision boundaries. The error analysis showed that the majority of misclassifications happened due to borderline cases where fake samples were similar to the real ones either by some strange physical nature or quality replication efforts. These inaccuracies give reason to believe that more discriminative factors should be involved, including some texture descriptors or serial-number pattern analysis, which will yield more accurate results. In general, the joint work of the models confirms the feasibility of AI-based systems to reinforce the real-world authentication of the currency.

Conclusion

This paper has introduced a Currency Security Validation system based on AI, which combines machine learning and deep learning to differentiate genuine and fake currency according to structured physical and security features. Both the CurrencyNet neural network and the Random Forest classifier had a high level of accuracy, but the deep learning model was slightly better. The results emphasize that feature preprocessing, along with encoding and optimization of models is effective in order to achieve dependable financial authentication. Despite the misclassification resulting in some borderline cases, the overall outcomes substantiate the idea that the AI-driven solutions can considerably improve the speed, consistency, and accuracy of the automated currency validation systems.

References

[1]. J. Singh and R. Sharma, “Automated Detection of Counterfeit Currency Using Machine Learning Techniques,” IEEE Access, vol. 9, pp. 112450–112462, 2021.
[2]. [2] A. Kumar and S. Gupta, “Feature-Based Analysis for Currency Authentication Using Statistical and Texture Measures,” IEEE Trans. Instrum. Meas., vol. 70, pp. 1–10, 2021.
[3]. [3] M. Patel and V. Shah, “Deep Learning Framework for Multi-Currency Fraud Identification,” Proc. IEEE ICACCS, pp. 512–518, 2022.
[4]. [4] R. Kaur and P. Arora, “Random Forest Classification for Financial Fraud Detection,” IEEE Int. Conf. SmartTech, pp. 233–239, 2021.
[5]. [5] S. Das and N. Roy, “A Robust Neural Network Model for Currency Classification,” IEEE Int. Conf. ICCCNT, pp. 1–6, 2020.
[6]. [6] Y. Zhang, H. Chen, and X. Liu, “Evaluation of Machine Learning Algorithms for Security Feature Prediction,” IEEE Trans. Emerg. Topics Comput. Intell., vol. 6, no. 4, pp. 789–799, 2022.
[7]. [7] T. Reddy and K. Rao, “An Enhanced Preprocessing Pipeline for Currency Feature Normalization,” IEEE Conf. ICSCN, pp. 145–150, 2021.
[8]. [8] J. George and A. Mathew, “Application of One-Hot Encoding and Ensemble Learning in Financial Datasets,” Proc. IEEE INDICON, pp. 908–913, 2020.
[9]. [9] H. Li and Q. Wang, “Comparative Study of Neural Network Architectures for Classification Tasks,” IEEE Access, vol. 8,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0111
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 725 - 731

pp. 156745–156755, 2020.
[10]. P. Singh et al., “Hybrid ML–DL Models for High-Accuracy Predictive Systems,” IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 12, pp. 7049–7061, 2022.
[11]. R. Verma and S. Jain, “Performance Metrics for Binary Classification in Financial Applications,” IEEE Trans. Knowl. Data Eng., vol. 34, no. 5, pp. 2214–2226, 2022.
[12]. L. Brown and M. Smith, “Applied Feature Scaling Techniques in Machine Learning Pipelines,” IEEE Int. Conf. Big Data, pp. 1203–1210, 2019.
[13]. A. Torres and L. Martinez, “Confusion Matrix Optimization for Fraud Analytics,” IEEE Trans. Inf. Forensics Security, vol. 17, pp. 1245–1257, 2022.
[14]. S. Sen and D. Roy, “Accuracy and Stability Analysis of Ensemble Learning in Classification Systems,” IEEE Trans. Syst. Man Cybern., vol. 52, no. 9, pp. 5342–5353, 2022.
[15]. M. Qureshi and T. Khan, “Data-Driven Detection of Anomalous Currency Patterns,” IEEE Int. Conf. ICMLA, pp. 342–348, 2021.
[16]. K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” Proc. IEEE Conf. CVPR, pp. 770–778, 2016.