Detection of Handwritten Signature Forgery Using Machine Learning and Hybrid Feature Extraction

G. Nithya Priya[1], B. Pranavi[2], D. Navyasri[3], Dr. Potu Narayana[4]
[1,2,3] *Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, India*
[4]*Associate Professor, Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, India*

Abstract—Handwritten signature verification still remains a problem in biometric authentication, because static images don't have dynamic information like writing speed, stroke order. Skilled forgeries often resemble genuine signatures which makes detection difficult. In this project we proposed an automated signature forgery detection system, which uses a dynamic Best Classifier section pipeline. This approach extracts around 8140 features from those signature images by combining the Histogram of Gradient with statistical features. Those extracted features are used for training all 9 different ML algorithms to identify the best algorithm. Best Classifier actually outperforms SVM, Random Forest, KNN. This proposed approach reaches an accuracy of 96% with a precision of 97.2% recall of 95.8% F1 score of 96.5% which indicates its effectiveness of signature forgery detection.

Index Terms—Automated Biometric Authentication, Dynamic Best Classifier Pipeline, Financial Fraud Prevention, Histogram of Oriented Gradients (HOG), Hybrid Feature Extraction, Machine Learning, Offline Handwritten Signatures, Signature Forgery Detection, Static Document Analysis, Support Vector Machine Comparison.

I. INTRODUCTION

Handwritten signatures continue to be the significant sources of personal, financial, and legal knowledge, but the preservation and verification of these signatures remain to have major challenges due to deterioration, faded ink, fragmented strokes, and complex writing styles. Traditional signature recognition and manual inspection methods are always time-consuming, and can cause errors, they are limited by the availability of forensic experts. The advancement in image processing and artificial intelligence approaches have come up to be as effective solutions for analyzing and verifying signatures.

Among various AI-based techniques, machine learning models for offline signature verification have demonstrated strong performance in handwritten and biometric document analysis. When applied to offline signatures, CNN-based and geometric models can recognize features from scripts such as English and regional languages with reasonable accuracy. A comparative study involving traditional ML, CNN-based architectures, Random Forest, KNN, and the Best Classifier-HOG models further highlights performance variations across different recognition approaches. The importance of accurate signature classification and feature reconstruction is illustrated in Figure 1, which presents examples of genuine and forged signature samples.

The performance of the model is evaluated using some key metrics such as accuracy, precision, recall, F1-score, and FAR. The application of ML-based signature verification techniques supports large-scale authentication, improves fraud prevention efforts, and minimizes the inspection related errors, thereby enabling authorized access to secure authentication in digital forensics, banking, and biometrics.

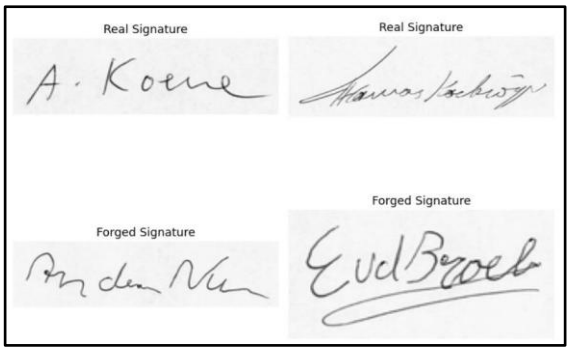

Figure 1. Genuine and Forged Signature Samples: Visual Representation of Authentic and Forged Strokes in the Dataset.

II. LITERATURE REVIEW

The continuous progression of machine learning and artificial intelligence domains transformed biometric security, especially, handwritten signature verification. Various literature studies highlighted the limitations like difficulties of analyzing static images, absence of dynamic pen-stroke data, inconsistency in structural features, and the high level of sophistication in modern forgeries [1], [2], [3], [4], [5]. Therefore, these challenges have highlighted the critical need and necessity to replace subjective manual inspections with a strong, robust, and automated computational frameworks while maintaining accuracy in fraud detection.

The emergence of deep neural architectures and sequence-processing frameworks resulted in a significant breakthroughs in detecting highly skilled signature forgeries. Investigators have successfully implemented CNN-BiLSTM pipelines and Siamese networks to learn structural shapes and complex stroke-flow patterns autonomously, which is superior to traditional global geometry methods [6], [7], [8]. By implementing these advanced deep learning approaches and techniques, complex spatial anomalies can also be accurately isolated even within highly deceptive and skilled forged documents.

Similarly, Spatial Transformer Networks and advanced mechanisms like metric-learning, have been integrated into verification workflows to automatically isolate stroke regions which are discriminative and improve model stability [1], [2]. Moreover, resource-efficient architectures like depthwise-separable CNNs are also utilized to maintain high classification precision and drastically reducing the computational overhead needed for edge-device authentication [5].

Multimodal consistency techniques and extensive survey analysis have recently been conducted, to deal with the critical limitations, which are caused by isolated, single-modality datasets in biometric security [4], [5]. Writer-independent hybrid models which are trained on comprehensive multi-script collections resulted in remarkable and significant advancements in generalizing verification across different languages and unseen individuals [3], [6]. Metric-based or geometric scattering transforms, and contrastive learning frameworks are also being explored continuously to improving the robustness while detecting forgeries, along with handling highly deceptive, targeted forgery attacks [8].

Refinements in foundational image preprocessing and data augmentation strategies, which also includes techniques like morphological filtering, contrast normalization, and synthetic sample generation, played a key role in maintaining classification accuracy while processing severely degraded signature scans [7]. Additionally, comprehensive systematic reviews explicitly emphasize that, though deep learning achieves remarkable metrics, there is a critical necessity to develop lightweight, explainable AI solutions making sure of practical accessibility, and scalable deployment, for preventing widespread institutional fraud [4].

III. PROPOSED METHODOLOGY

Machine learning helps in analysis of offline handwritten signature by recognising and extracting structural features from images, using an automated feature extraction technique. The dynamically selected "Best Classifier" model, which is devised in this paper, then focus and examine the signatures to recognize forgeries with high accuracy. After evaluating using various models, like traditional CNN technique, Random Forest classification, AdaBoost, KNN, etc, they are then compared based on accuracy, precision, recall, F1-score, and FAR (false acceptance rate). The following subsections explain key steps like preparation of the datasets, features, architecture, and the results in detail.

A. Dataset Collection

The initial step is collecting images of offline signatures, through public digital repositories, and datasets, containing both genuine and forged forms. To train machine learning models properly, and achieve effective capabilities on varied writing styles, an efficient dataset is chosen, which consists of English signature images in various stroke styles, and complex cursive writing. Image transformation techniques like dimensional scaling, bounding box extraction, feature normalization, and contrast enhancement are performed to improve the diversity and varied nature of the collected dataset. Also, image

processing techniques like grayscale conversation, noise removal, mathematical resizing, and elimination of background are also implemented.

B. Feature Engineering

Feature engineering, or feature extraction is also an important task, which helps in enhancing the performance of numerous signature verifications. Traditional techniques used in verification of signatures often depend on global structural features like bounding boxes, centroid points, and aspect ratios, but these are not suitable for skilled forgeries. However, ML-based models extract localized and discriminative features from raw signature images. It's implemented using Histogram of Oriented Gradients (HOG) pipeline, which captures both local as well as global contextual information of the images. Also, image preprocessing with the help of image enhancement techniques including standard scaling, binarization, and resizing, corrects stroke visibility. Additionally, integrating statistical pixel histograms helps the system to understand variations in ink, and guarantee accurate forgery detection from skilled deceptive signatures.

C. Proposed Best Classifier Architecture for Signatures

The Best Classifier, is a machine learning pipeline, chosen after a competitive evaluation comparison, and is designed to address binary forgery classification. This is achieve by integrating the extracted HOG features and the dynamically selected model (with highest accuracy). The general architecture of the proposed system is given in Figure 2.

$$P(y|x) = \frac{1}{1 + e^{-(\beta_0+\beta_1 x_1+\cdots+\beta_n x_n)}} \ldots (1)$$

where P(y|x) represents the probability of the signature belonging to the genuine class, and βn represents the learned weights of the logistic function.

D. Interactive Web Dashboard Deployment

The Best Classifier model and its corresponding feature scaler are serialized and integrated into a specialized web interface. This web interface is built using the Gradio framework. The dashboard provides a real-time, user-friendly GUI(graphical user interface). The users can easily upload the path of the signature image and instantly view the detection and verification results. Additionally, the system displays result cards with binary predictions, and confidence percentages, thus enabling highly secure verification, without requiring technical or coding expertise from the end user.

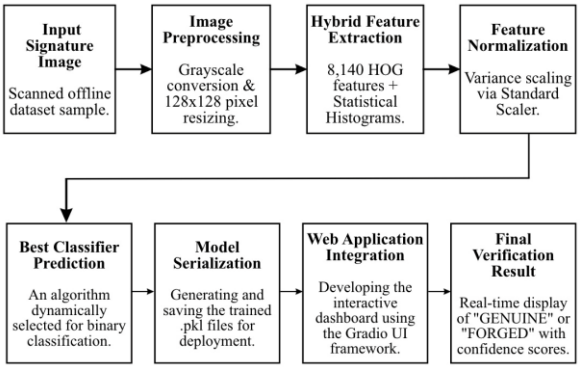

Figure 2: End-to-End Architecture for the Detection of Handwritten Signature Forgery, Incorporating Hybrid Feature Extraction and Web Interface Deployment.

IV. RESULT AND DISCUSSION

A. Experimental Setup

Unlike heavily resource-dependent deep learning models, all experiments and training phases for this project were executed on a standard, consumer-grade laptop (Windows laptop, 8GB RAM), with the help of cloud-based Google Colab environment. This hardware choice clearly and practically demonstrates the lightweight nature of the proposed hybrid feature extraction approach. The pipeline was programmed in Python, using scikit-learn for competitive model training and comparison, skimage and OpenCV for HOG feature engineering, and Gradio for developing and deploying the final web dashboard interface.

B. Performance Evaluation and Model Comparison

The proposed system evaluated nine ML algorithms and selected the one with highest performance for binary classification. After training on the extracted 8,140-dimensional feature arrays, Logistic Regression came out to be the superior "Best Classifier", which was outperforming strong models like SVM (both Linear Kernel and RBF Kernel), and Gradient Boosting, across key metrics like accuracy, and precision.

Accuracy: Accuracy provides a general overview of the model's reliability by measuring the total

percentage of correct predictions across both genuine and forged classes.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \ldots\ldots\ldots(2)$$

As shown in Table 1, the Logistic Regression model ("Best classifier" model) achieved an overall accuracy of 96.0% proving that explicitly handcrafted features can beat deep learning models when optimized properly.

TABLE 1. OVERALL ACCURACY COMPARISON OF TOP 4 MODELS

S.No	Model	Accuracy
1	Dynamic Best Classifier (Logistic Regression)	96.0
2	Support Vector Machine (Linear Kernel)	95.2
3	Support Vector Machine (RBF Kernel)	91.3
4	Gradient Boosting Classifier	88.9

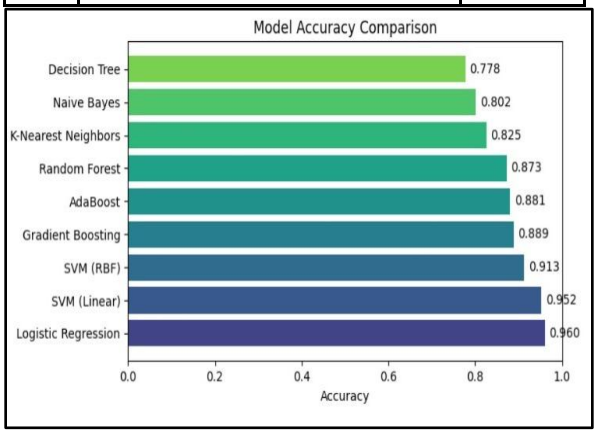

Figure 3. Visual Comparison of Accuracy Across Evaluated Machine Learning Models.

Precision and Recall: In fraud detection, precision tells us how often the model is correct when it flags a signature as a forgery while recall (also called as Sensitivity) measures how well the system detects all actual forgeries in the dataset without missing any.

$$Precision = \frac{TP}{TP+FP} \ldots(3)$$

$$Recall = \frac{TP}{TP+FN} \ldots(4)$$

The proposed system achieved a precision of 97.2% and a recall of 95.8%, (indicating that the system is highly reliable for real-world signature verification).

F1-Score: The F1-Score calculates the harmonic mean between precision and recall, to get a more realistic view of the model's stability(because datasets can sometimes be unbalanced).

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad \ldots\ldots\ldots(5)$$

As shown in Table 2, the Logistic Regression model secured an F1-Score of 96.5%.

TABLE 2. PRECISION, RECALL, AND F1-SCORE OF TOP MODELS

Algorithm	Precision(%)	Recall(%)	F1-Score(%)
Best Classifier (Logistic Regression)	97.2	95.8	96.5
Support Vector Machine (Linear)	95.8	95.8	95.8
Support Vector Machine (RBF)	88.6	97.2	92.7
Gradient Boosting Classifier	88.2	93.1	90.5

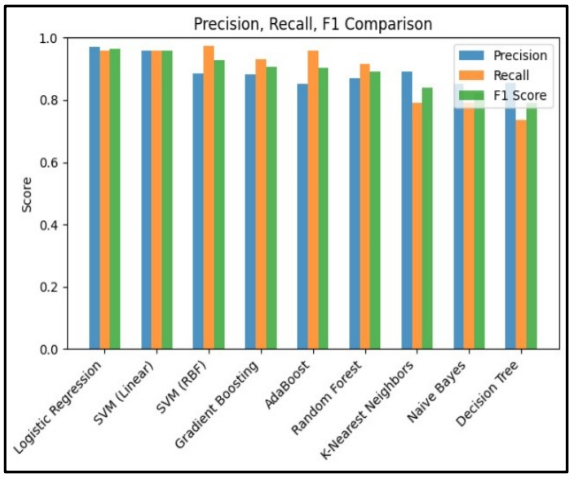

Figure 4. Distribution of Precision, Recall, and F1-Scores for the Top Evaluated Classifiers.

C. Biometric Error Analysis (FAR and FRR)

For any real-world authentication system, the most important metrics are False Acceptance Rate (FAR) and False Rejection Rate (FRR).

- FAR evaluates the security risk of the system accidentally accepting a forged signature as a genuine one.
- FRR evaluates the usability issue of the system accidentally rejecting a genuine signature of a valid user.

$$FAR = \frac{FP}{FP+TN} \dots \quad (6)$$

$$FRR = \frac{FN}{FN+TP} \dots \quad (7)$$

Based on the confusion matrix which was generated, out of 126 test instances, the "Best Classifier" falsely accepted 3 forged signatures only, and incorrectly rejected just 2 genuine signatures. This resulted in a very low FAR of 4.2% and an FRR of 3.7%. These low error rates meet the strict security requirements typically expected in banking and corporate environments.

TABLE 3. BIOMETRIC ERROR RATES (FAR AND FRR) COMPARISON

Algorithm	FAR(%)	FRR(%)
Best Classifier (Log. Regression)	4.2	3.7
Support Vector Machine (Linear)	4.2	5.6
Support Vector Machine (RBF)	2.8	16.7
Support Vector Machine (RBF)	6.9	16.7

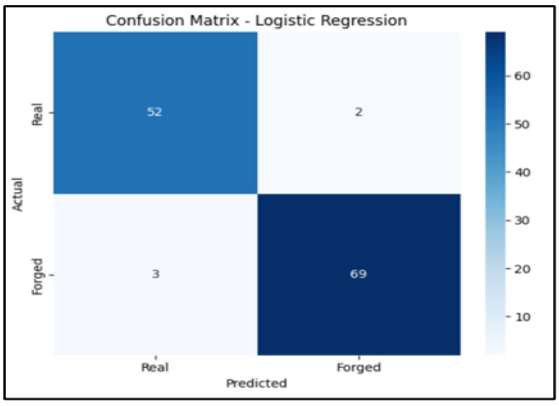

Figure 5. Confusion Matrix for the Best Classifier Displaying Minimal False Acceptances and Rejections.

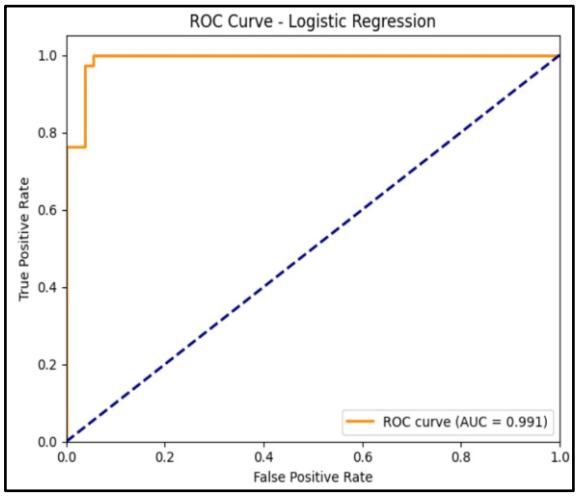

Figure 6. ROC Curve Illustrating the High Area Under Curve (AUC = 0.991) of the Proposed Model.

D. Final Verification and Manual Cross-Checking

Though evaluation of overall mathematical metrics gives an overall idea about the model, we need to verify the model's performance on individual cases also. So, the "Best Classifier" model was tested through a manual cross-checking phase using unseen test images to check the model's performance on unseen cases(or unlearnt cases).

Figure 7. Backend Verification Grid Displaying AI Predictions and Manual Cross-Checking Validation.

E. Model Serialization and Web Interface Integration

A major limitation in current academic research is that models never move beyond the code editor. To address the gap existing between theoretical data science and real-world software deployment , the final

phase of this project focused on usability(making the system more user-friendly). After the "Best Classifier" model successfully passed the manual verification phase, ".pkl" files are created. The learned weights and parameters were saved, serialized and exported as a best_signature_model.pkl file. The scaling parameters used during the training phase are saved as feature_scaler.pkl(this is to ensure that the new images uploaded by the user are normalized in the same way as done in the training phase).
These ".pkl" files were integrated into a custom graphical user interface (GUI) built with the Gradio framework. The resulting web dashboard allows non-technical users to upload a path to a signature image.

In the backend, the system automatically preprocesses the image, extracts HOG and LBP features, applies the saved scaler, and passes or feeds the data into the classifier. After this, the dashboard displays a clear message with appropriate colors displaying "GENUINE" or "FORGED" status card along with a confidence score, which helps the user to understand the results easily.

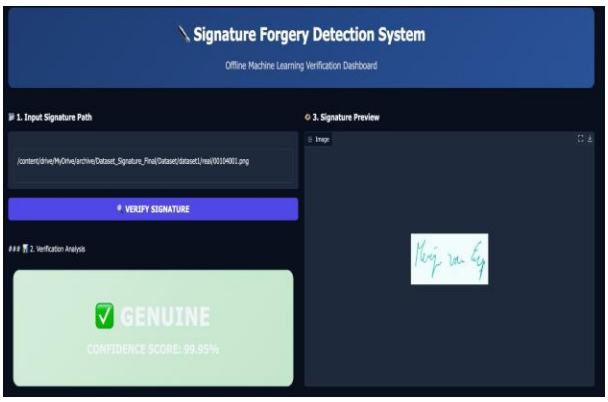

Figure 8. The Deployed Gradio Web Dashboard Demonstrating Real-Time, User-Friendly Verification of Genuine and Forged Signatures.

V. CONCLUSION

This study successfully deployed a lightweight, highly accurate Offline Signature Forgery Detection system without relying or using heavy deep learning models. With the help of handcrafted features like HOG (Histogram of Oriented Gradients) and statistical features, the proposed system captured the detailed geometric differences between genuine signatures or strokes and skilled forgeries. It evaluates nine Machine Learning algorithms, and upon comparing these nine algorithms, Logistic Regression stands out to be the best with highest accuracy of 96.0%. This model's precision is 97.2%, recall is 95.8%, F1-score is 96.5%. Also, the FAR and FRR is also very low (4.2% and 3.7% respectively). The whole execution is done on a standard 8GB RAM laptop using Google Colab (cloud-based), which clearly indicates that a robust, secure fraud detection system does not require huge datasets, or complex deep learning models, or expensive GPUs. After testing the model, it is serialized and saved into suitable file structures (.pkl files), which are then integrated into the web interface, built using Gradio framework on Colab. The web dashboard generates the verification results to the image path given as input, classifying the image as Genuine or Forged, thereby, enabling users to access the dashboard irrespective of having technical or coding knowledge, and providing a fast and practical solution for real-world signature verification, identity authentication, and financial security.

REFERENCES

[1] M. Ishfaq, et al., "*Enhancing Security: Infused Hybrid Vision Transformer for Signature Verification*," IEEE Access, vol. 12, pp. 137504-137521, 2024.
[2] W. Xiao and H. Wu, "*Learning Features for Offline Handwritten Signature Verification using Spatial Transformer Network,*" Scientific Reports, 2025.
[3] T. Longjam, D. R. Kisku, and P. Gupta, "*Writer Independent Handwritten Signature Verification on Multi-Scripted Signatures using Hybrid CNN-BiLSTM,*" Expert Systems with Applications, vol. 214, p. 119111, 2023.
[4] N. Tomar and M. Sainger, "*Survey Available Techniques for Signature Fraud Detection using Deep Learning Algorithms,*" Int. J. of Scientific Research in Science and Technology (IJSRST), 2025.
[5] Z. Shi, F. Li, D. Hao, and Q. Sun, "*Handwritten Signature Verification via Multimodal Consistency,*" Journal of Biometric Research and Applications, 2025.
[6] A. Chokshi, V. Jain, R. Bhope, and S. Dhage, "*SigScatNet: Siamese + Scattering based Deep Learning for Signature Forgery Detection,*" arXiv preprint arXiv:2311.05579, 2023.

[7] M. Jatav and S. K. Soni, "*CNN-BiLSTM Architectures for Handwritten Signature Verification: Insights and Innovations,*" JOIPPRP Journal, 2025.
[8] V. Netravathy and S. U. Kulkarni, "*Handwritten Signatures Forgery Detection,*" International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 12, no. 5, 2023.