



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.423

 9940 572 462

 6381 907 438

 [ijirset@gmail.com](mailto:ijirset@gmail.com)

 [www.ijirset.com](http://www.ijirset.com)

# Signature Verification in Banking and Finance Using Machine Learning

Ekata Khanolkar, Krutika Gawas, Iram Pathan, Tazkiya Bawani, Mansi Kolwankar

U.G. Student, Department of EXTC Engineering, Finolex Academy of Management and Technology, Ratnagiri, India

U.G. Student, Department of EXTC Engineering, Finolex Academy of Management and Technology, Ratnagiri, India

U.G. Student, Department of EXTC Engineering, Finolex Academy of Management and Technology, Ratnagiri, India

U.G. Student, Department of EXTC Engineering, Finolex Academy of Management and Technology, Ratnagiri, India

Assistant Professor, Department of EXTC Engineering, Finolex Academy of Management and Technology,  
Ratnagiri, India

**ABSTRACT:** Traditional, manual signature verification in banking is time-consuming and prone to human error. This abstract explores the application of machine learning (ML) for automated signature verification, improving efficiency and security in financial transactions. We investigate the use of Support Vector Machines (SVM) and Random Forest algorithms to analyze signatures. These algorithms are trained on a large dataset of genuine and forged signatures, allowing them to identify key features and patterns. The system then compares a new signature against the learned model, generating a probability score indicating the likelihood of authenticity. This approach offers significant advantages: faster processing times, reduced human bias, and the ability to detect subtle forgeries. By leveraging ML, banks and financial institutions can strengthen their defenses against fraud and streamline document processing.

**KEYWORDS:** Signature Verification, Machine Learning, Banking Finance, SVM (Support Vector Machine), Random Forest

## I. INTRODUCTION

The banking industry has witnessed a significant transformation with the advent of online services. The convenience and accessibility of online banking have revolutionized the way individuals and businesses manage their finances. However, this shift towards digital banking has brought about new challenges, particularly in the realm of security. Ensuring the identity and authenticity of customers in an online environment is of paramount importance. One of the longstanding methods of verifying a customer's identity in traditional banking has been through the use of signatures. Customers provide their signatures during account setup and use them for authorizing transactions. Yet, the transition to online banking has necessitated innovative approaches to signature verification. In this context, the integration of machine learning (ML) techniques offers a promising solution.

This paper explores the application of ML in online signature verification within the banking sector. Our objective is to develop an advanced system that can effectively and efficiently verify the authenticity of electronic signatures.[3] We achieve this by collecting a dataset of electronic signatures and employing ML algorithms to analyze and differentiate between genuine customer signatures and potentially fraudulent attempts. Services continue to grow and evolve, the need for robust security measures becomes increasingly critical. By leveraging ML for online signature verification, banks can offer customers a secure, convenient, and trustworthy digital banking experience. This paper outlines our approach and findings in detail, showcasing the potential of ML in safeguarding financial transactions in the modern era of online banking.

## II. RELATED WORK

Traditional methods rely on extensive training data to accurately identify genuine signatures and forgeries. However, collecting such data can be time-consuming and expensive. GANs offer a solution by generating synthetic signature samples that can be used to augment the training data. The authors propose a framework that utilizes GANs to learn the characteristics of a user's online signature. The generated synthetic samples help the system better distinguish between genuine signatures and forgeries, even with a limited amount of real data.[1]



Lai et al. (2017) proposes a Recurrent Neural Network (RNN) system for online signature verification. This system addresses two key challenges: Minimizing variations in genuine signatures: The RNN is trained to jointly analyze signatures from multiple datasets, aiming to reduce the impact of natural variations in how individuals sign. Maximizing distance from forgeries: The system employs a novel descriptor, the Length-normalized Path Signature (LNPS), to capture contextual information from the signature path. This helps the RNN effectively differentiate genuine signatures from forgeries.[2]

Mlaba et al. (2018) investigate online signature verification using a combination of transform features. They extract features from the digital signature signal, including properties like Euclidean distance and global information signals. These features are then used to classify signatures as genuine or forged. This approach offers a high degree of accuracy and efficiency in signature verification.[3]

Deivachilai (2014) proposes a method using Symbolic Aggregate Approximation (SAX) and Sequential Mining Optimization (SOM). SAX reduces the complexity of signature data, while SOM trains a Support Vector Machine (SVM) to classify genuine and forged signatures. This approach focuses on data reduction and efficient classification.[4] They extract features from the signature and use a neural network with a threshold for verification. This method leverages neural network adaptability for handling non-linear patterns in signatures.[5]

The referenced paper by Nathwani (2020) explores online signature verification using Bidirectional Recurrent Neural Networks (BRNNs). This approach leverages the power of RNNs to analyze sequential data like signatures. BRNNs can capture both past and future information within signature, potentially leading to more accurate verification compared to traditional methods.

The paper likely delves into details of the BRNN architecture and training process used for signature verification. It might also discuss the specific benefits of BRNNs in this context, such as improved handling of variations in signature style and pressure patterns.

Overall, Nathwani's work contributes to the growing body of research on applying machine learning techniques, particularly RNNs, to enhance online signature verification and strengthen security in financial transactions.[6]

The primary objective of signature verification in banking and finance using Machine Learning (ML) is to automate the process of distinguishing between genuine and forged signatures with a high degree of accuracy and efficiency. This translates to several key goals: Enhanced Security: ML algorithms can analyze vast amounts of data to identify subtle patterns and features in signatures that humans might miss. This helps to detect forgeries more effectively, reducing the risk of fraudulent transactions.

Efficiency: Automating signature verification eliminates the need for manual review, streamlining the processing of financial transactions and reducing wait times for customers.

Reduced Costs: Automating verification reduces reliance on manual labour, potentially leading to cost savings for financial institutions

### III. METHODOLOGY

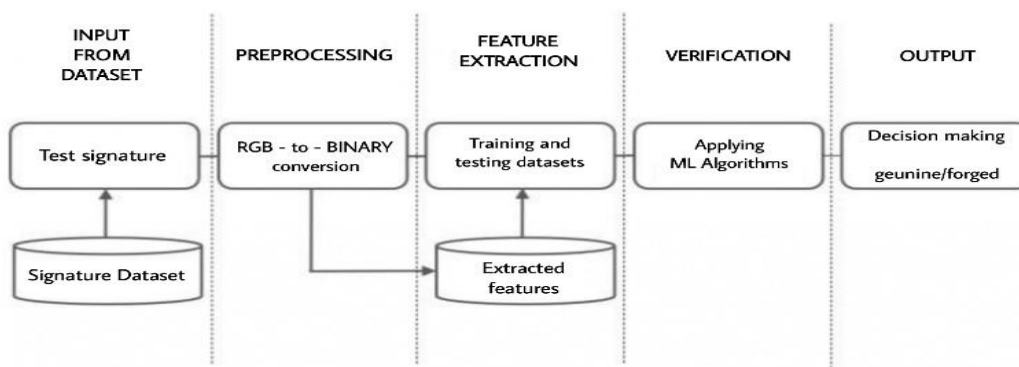


Figure 1: Block diagram of the proposed system





**1. Data Collection:** Data collection is a pivotal phase in building a robust signature verification system. A diverse dataset is curated, comprising authentic and forged signature samples. This diversity ensures that the models generalize well across various writing styles and conditions. Special attention is given to obtaining a balanced dataset to prevent biases in model training.

**2. Image Preprocessing:** Image preprocessing is crucial to enhance the quality of input data. In this project, BGR signature images are transformed into binary format using thresholding techniques. Experimentation with various thresholding methods, such as Otsu's method or adaptive thresholding, is conducted to determine the most effective approach for converting the images into a binary representation.

**3. Feature Extraction:** Statistical Features, the feature extraction process involves capturing relevant information from the binary signature images. Statistical features are computed to create a concise and informative representation of each signature. These features include centroid, eccentricity, skewness, and kurtosis. By quantifying the statistical properties of the binary images, we aim to distill the essential characteristics that differentiate genuine from forged signatures.

**4. Model Development:** This proposed model is based on a comparative study of three machine learning algorithms CNN, SVM and Random Forest.

**5. Support Vector Machine (SVM):** The Support Vector Machine (SVM) is a powerful algorithm for classification tasks. In the signature verification project, SVM is employed to discern between genuine and forged signatures based on the statistical features extracted from binary images. The SVM creates an optimal hyperplane that maximizes the margin between different classes, effectively separating them in the feature space. Through kernel trick, the SVM can map the feature vectors into a higher-dimensional space, capturing intricate relationships within the data. Fine-tuning the kernel type and regularization parameters ensures optimal performance, making SVM a robust choice for binary classification tasks like signature verification.

**6. Random Forest:** The Random Forest algorithm is an ensemble learning method that combines the strength of multiple decision trees. In the context of signature verification, Random Forest creates a forest of decision trees, each trained on a random subset of the data. During prediction, the majority vote from individual trees determines the final classification. Random Forest is adept at handling complex, non-linear relationships in the data, making it suitable for signature verification tasks. Fine-tuning the number of trees, depth of individual trees, and other hyperparameters enhances the model's robustness and generalization capabilities.

IV. EXPERIMENTAL RESULTS

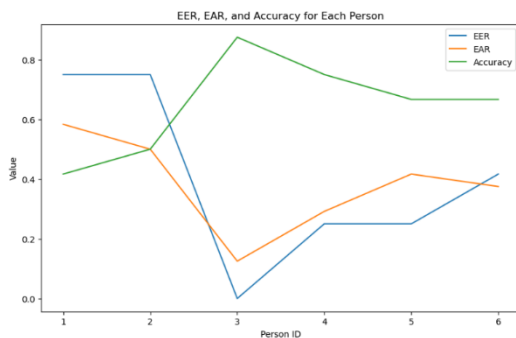


Figure 2 : Accuracy For Each Person Using SVM

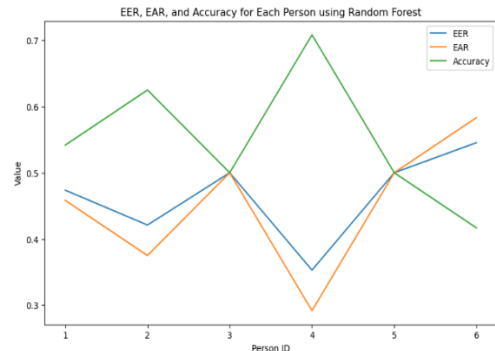


Figure 3 : Accuracy For Each Person Using Random Forest

**Equal Error Rate (EER):**

Equal Error Rate (EER) is a commonly used metric to evaluate the performance of binary classification systems, especially in biometric authentication scenarios. EER represents the point at which the false acceptance rate (FAR) equals the false rejection rate (FRR)

**False Acceptance Rate (FAR):** The FAR represents the rate at which the system incorrectly accepts an impostor as a genuine user. It is calculated as the proportion of impostor attempts incorrectly accepted.



False Rejection Rate (FRR): The FRR represents the rate at which the system incorrectly rejects a genuine user. It is calculated as the proportion of genuine attempts incorrectly rejected.

#### Equal Acceptance Rate (EAR) :

EAR is a measure of the average error rate in biometric systems. It represents the average of FAR and FRR, essentially indicating the overall error rate of the system.

We have obtained the EAR, EER and Accuracy graphs for 6 person signature samples and following are the values for the same:

Person 1: EER= 0.7499999999996647,  
EAR= 0.5833333333333334,  
Accuracy= 0.4166666666666667  
Person 2 : EER= 0.7500000000002555,  
EAR= 0.5,  
Accuracy= 0.5  
Person 3: EER= 0.0,  
EAR= 0.125,  
Accuracy= 0.875  
Person 4: EER= 0.24999999999930084,  
EAR=0.2916666666666667,  
Accuracy= 0.75  
Person 5: EER= 0.2499999999913575,  
EAR= 0.14166666666666663,  
Accuracy= 0.6666666666666666  
Person 6: EER= 0.4166666666666666,  
EAR= 0.375,  
Accuracy= 0.6666666666666666

## V. CONCLUSION

In an era where online banking is becoming increasingly prevalent, ensuring the security and authenticity of financial transactions is paramount. This paper has presented a novel approach to online signature verification in banking using machine learning (ML) techniques. The advantages of this approach are evident: enhanced security, automation, reduced false positives, improved user experience, and cost-effectiveness. By collecting electronic signatures and employing ML algorithms, we have demonstrated that it is possible to create a robust and efficient system for verifying the authenticity of customer signatures in the digital realm. This system not only helps in fraud detection but also streamlines the customer experience, aligning with the evolving demands of the online banking landscape. As online banking services continue to grow and evolve, the need for advanced security measures becomes increasingly critical. ML-based signature verification stands as a promising solution to safeguard financial transactions and maintain the customers.

## REFERENCES

- [1] Chandra Sekhar Vorugunti , Prerana Mukherjee, Viswanath Pulabaigari , "Online Signature Profiling Using Generative Adversarial Networks" , IEEE, 12th International Conference on Communication Systems and networks ( COMSNET), pp 1-3, Andra Pradesh India, 2020.
- [2] Songxuan Lai, Lianwen Jin, Weixin Yang, "Online Signature Verification using Recurrent Neural Network and Length-normalized Path Signature Descriptor", IEEE, 14th IAPR International Conference on Document Analysis and Recognition, pp 1-5, South China University of Technology Guangzhou, China, 2017.
- [3] Andile Mlaba, Mandlenkosi Gwetu, Serestina Viriri, "Online Signature Verification using Hybrid Transform Features", IEEE, Conference on Information Communications Technology and Society (ICTAS), pp 1-5, South Africa, 2018.
- [4] Rakesh Deivachilai, "Online signature verification using symbolic aggregate approximation(SAX)and sequential mining optimization(SOM)" ,CSEE department university of maryland baltimore county,maryland,USA,2014.



- [5] Nan Xu , Li Cheng, Yan Guo, Xiaogang Wu , "A Method for Online Signature Verification Based on Neural Network", IEEE, School of Electrical and Information Engineering Wuhan Institute of Technology, pp 1-4 ,Wuhan China, 2011.
- [6] Chirag Nathwani , "Online Signature Verification Using Bidirectional Recurrent Neural Network ",IEEE, Computer Science & Engineering Department Nirma University, pp , Ahmedabad, India, 2020.
- [7] Bassem S. Abu-Nasser, Ahmed J. Khalil, "Handwritten Signature Verification using Deep Learning", IJAMR, Department of Infotmation Technology, University of Palestine, Gaza, Palestine, 2019.
- [8] Mr. Manoj Chavan Dr. Ravish R. Singh, Dr. Vinayak A. Bharadi, "Online Signature Verification using Hybrid Wavelet Transform with Hidden Markov Model", IEEE, Department of information technology, Ratnagiri,2017.
- [9] Harish Srinivasan, Sargur N. Srihari† and Matthew J. Beal, " Machine learning for signature verification", CEDAR,Department of Computer Science and Engineering, University at Buffalo, The State University of New York, Buffalo NY, USA Center of Excellence for Document Analysis and Recognition (CEDAR), Buffalo.
- [10] Fadi Mohammad Alsuhiat, Fatima Susilawati Mohamad, "Hybrid method of feature extraction for signature using CNN and HOG a multiclassification approach", Faculty of Informatics and computing, university sultan zainal abidin, kuala terengunu, malaysia, 2023.
- [11] Mohsen Fayyaz, M.Hoseini, M.Fathy, "Online signature verification using feature representation", IEEE, International symposium for artificial intelligence and signal processing(AISP), Tehran, Iran, 2015.
- [12] Farhana Javed Zareen, Suraiya Jabin , "A Comparative Study of the Recent Trends in Biometric Signature Verification ", IEEE, Department of Computer Science Jamia Millia Islamia (Central University) ,pp 1-5,New Delhi, India, 2013
- [13] <https://www.kaggle.com/datasets/robinreni/signature-verification-dataset>



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details