**Journal of Neonatal Surgery**
***ISSN(Online): 2226-0439***
***Vol. 14, Issue 14s (2025)***
*https://www.jneonatalsurg.com*

OPEN ACCESS

# Signature Forgery Detection

**Sandra C[1], Vediyyappan V[2], Ms.B. Jijitha[3], Md Sibtain Ansari[4], Kankadiyil Fahshad Mohammed Haneefa[5], Nafees H M[6], Mohammed Dhiyan N[7]**

[1]Project student, Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: Sandrachinnduraii@gmail.com

[2]Project student, Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: vediyappanv42004@gmail.com

[3]Assistant professor, Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: jiji.akshu@gmail.com

[4]Project student Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: mdsibtain28@gmail.com

[5]Project student Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: Fahshadaju@gmail.com

[6]Project student, Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: deennafeesu@gmail.com

[7]Project student Department of Computer Applications, Nehru Arts and Science College, Coimbatore, India
Email ID: dhiyannmohamed@gmail.com

Cite this paper as: Sandra C, Vediyyappan V, Ms.B. Jijitha, Md Sibtain Ansari, Kankadiyil Fahshad Mohammed Haneefa, Nafees H M, Mohammed Dhiyan N, (2025) Signature Forgery Detection. *Journal of Neonatal Surgery*, 14 (14s), 475-482.

**ABSTRACT**

Digital signatures are widely used in recent times by organisations public and private alike. Similar to fingerprints the signatures are legally binding. Another reason why they are being used is that they are easy to handle and store. The digital signatures are utilized mainly in e-commerce websites for delivery authentication to the customers, bank customer procedures and verification, government organisations and various other businesses big and small. Nowadays, the government uses digital signatures for contracts and verifying documents. When there is an advancement in IT, it has its advantages and disadvantages. Signature is one of the important biometric techniques that may be used for manipulating the signature data and using them for malicious purposes. Two efficient machine learning algorithms VGG16 and random forest are implemented in the research attempt to identify a way to mitigate the risk caused by signature forgery. The machine language techniques are being trained and tested to check whether the signatures given are original or fake using a data set.

**Keywords** *Signature verification, forgery detection, offline signature verification, online signature verification, feature extraction, machine learning models, convolutional neural networks (CNN), support vector machine (SVM), k-nearest neighbors (KNN), data augmentation, transfer learning, synthetic signatures, feature vector representation, classification algorithms, validation and testing, cross-validation..*

## 1. INTRODUCTION

Signatures were being used in the world for nearly a thousand years. It is written in a variety of patterns some may be the letters in different languages. It is considered as evidence or consent of someone's agreement with someone else. This can be a contract agreement, sales agreement or anything relating to someone's identity that can be described in simple letters. As trade and market expanded, the use of signature has also expanded. After the digitalization of the industry, various conventional methods were converted into digital formats including signatures. This has helped in improving security standards but as the cybercriminals are getting smarter day by day cyber-crimes have also increased. Now it's been a great challenge for organizations to safeguard the digital information of the customers also identifying the authenticity of this digitally stored information has become a great challenge for organizations. Therefore, identifying the authenticity of digital signatures has been an important fact in the current scenario. Signature forgery detection is a critical area of research in biometric security, aiming to distinguish between genuine and forged signatures using machine learning techniques. With the growing reliance on handwritten signatures for authentication in various sectors like banking, legal

documents, and identity verification, detecting forgeries has become increasingly important. Traditional methods of signature verification

often struggle to differentiate subtle nuances between authentic and forged signatures. However, machine learning offers a powerful solution by automating the process and improving accuracy. By extracting various features from signature samples—such as shape, velocity, pressure, and timing—machine learning models, such as Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN), can be trained to identify patterns indicative of forgeries. These systems can be applied to both offline signatures (static images) and online signatures (dynamic data, such as pen pressure and speed), providing a robust framework for signature verification.

### *SYSTEM ANALYSIS*

Signature forgery detection has become an essential field in security systems, especially with the increasing digitalization of transactions and authentication processes. In traditional authentication systems, handwritten signatures serve as a key method for verifying identity. However, the challenge lies in differentiating genuine signatures from forged ones, which can range from simple imitations to highly skilled forgeries. This challenge is further compounded by the complexity of the human writing process, where slight variations in handwriting or signature style can lead to inaccuracies in detection. As a result, traditional methods of forgery detection, which rely on visual inspection or manual comparison, often fall short in providing a high level of accuracy and efficiency. Machine learning (ML) provides a transformative solution by automating the signature verification process and offering a robust framework for detecting forgery. By leveraging advanced algorithms and deep learning models, signature forgery detection systems can be trained to recognize the unique characteristics of a signature, including shape, pressure, velocity, and timing. The system analyzes features such as stroke order, curvature, and pen lift patterns, learning from vast datasets of genuine and forged signatures. This allows the model to distinguish between authentic and forged signatures with high precision. The system analysis of signature forgery detection using machine learning involves multiple stages, beginning with data collection and preprocessing. Signature data, whether captured through online (dynamic) or offline (static) methods, must be carefully processed to extract meaningful features. These features are then fed into machine learning algorithms, where the model undergoes training and optimization. Common algorithms such as Convolutional Neural Networks (CNNs), Support Vector Machines (SVMs), and Recurrent Neural Networks (RNNs) are often employed to classify signatures accurately. The system also incorporates various evaluation techniques, such as cross-validation and accuracy assessment, to ensure its robustness and reliability in real-world applications. Ultimately, the goal of implementing machine learning for signature forgery detection is to create an automated, scalable, and highly accurate system that can be seamlessly integrated into various sectors, including banking, legal, and governmental operations. By minimizing human error and enhancing the speed of verification, these systems provide a significant improvement over traditional manual processes, ensuring secure and trustworthy authentication methods.

### *Limitations of the Existing System:*

- Data Quality and Availability: Limited access to high-quality, large datasets of both genuine and forged signatures can hinder the model's ability to generalize across different signature styles and forgeries**.**
- Feature Extraction Complexity: Extracting meaningful and relevant features from signatures is challenging. Variations in writing style, pressure, speed, and angle can lead to inconsistent features, making accurate detection difficult.
- Forgery Detection Accuracy: Existing systems may not be highly accurate in detecting more sophisticated forgeries, especially those created by skilled forgers who mimic the original signature closely.
- Scalability Issues: Systems may struggle to scale when dealing with a large number of signatures, leading to longer processing times and decreased efficiency in real-time applications.
- Overfitting and Underfitting: Machine learning models may suffer from overfitting (when the model is too closely aligned with the training data and performs poorly on unseen data) or underfitting (when the model is too simplistic and unable to capture complex patterns).
- Data Privacy and Security Concerns: Storing sensitive biometric data, such as signatures, raises privacy and security concerns, especially when using cloud-based solutions or public datasets.
- Dependency on Signature Consistency: Many current systems rely heavily on the assumption that signatures are consistent over time. However, human signatures can naturally evolve, and people may alter their signature over time, affecting the accuracy of detection.

### *Literature Review*

Several researchers have proposed automated systems for detecting plant diseases. Some notable works include:

- **Kaur and Arora (2014)** - Used Zernike moments with SVM to improve offline signature forgery detection.
- **Antal et al. (2019)** - Applied CNNs for feature extraction and classification in offline signature verification.

- **Zhang et al. (2016)** - Explored RNNs for online signature verification to model temporal dynamics.
- **Jain and Gupta (2019)** - Combined CNN-LSTM hybrid models for better detection of forged dynamic signatures.
- **Deng et al. (2017)** - Introduced multi-feature extraction combining geometric and time- series data for online signature verification.
- **Zhao et al. (2020)** - Utilized Generative Adversarial Networks (GANs) for synthetic forgery generation to improve model training.

***PROPOSED SYSTEM METHODOLOGY ANDANALYSIS***

## 2. METHODOLOGY

The proposed system for signature forgery detection employs a combination of image processing techniques and machine learning algorithms to accurately differentiate between genuine and forged signatures. Initially, the system captures a high-resolution image of the signature, which undergoes preprocessing steps such as resizing, normalization, and noise reduction to ensure clarity and consistency. Feature extraction is then performed, where critical characteristics such as stroke dynamics, pressure, and velocity patterns are analyzed using techniques like edge detection, contour analysis, and Fourier transform. These features are extracted from both static and dynamic aspects of the signature. Next, a classification model, typically based on machine learning algorithms such as Support Vector Machines (SVM), Convolutional Neural Networks (CNN), or deep learning models, is trained using a dataset of genuine and forged signatures. The trained model learns to identify subtle differences in the signature features that are often indicative of forgeries.

### Preprocessing

The proposed system for preprocessing in signature forgery detection begins with the acquisition of a high-quality image of the signature. This image is then subjected to several essential preprocessing steps to ensure the consistency and accuracy of subsequent analysis. The first step is resizing, where the image is adjusted to a standard size, ensuring uniformity across all input signatures. Next, noise reduction techniques, such as Gaussian blurring or median filtering, are applied to remove any unwanted artifacts or distortions that might hinder feature extraction. The image is then normalized, which involves adjusting the brightness and contrast to ensure the signature is clear and distinguishable from the background. Additionally, binarization is performed to convert the image into a black-and-white format, enhancing the visibility of the signature's strokes.

### Feature Extraction

Feature extraction in signature forgery detection involves identifying distinctive characteristics of the signature, such as stroke dynamics, pressure, velocity, and spatial patterns. Techniques like contour analysis, edge detection, and curve fitting are applied to capture the signature's unique shapes and movement.

### Signature Classification using CNN

signature forgery detection, classification using Convolutional Neural Networks (CNN) involves training a deep learning model to recognize and differentiate between genuine and forged signatures. The CNN is fed with preprocessed signature images, where it automatically learns hierarchical features such as edges, textures, and complex patterns through multiple convolutional layers. After training on a labeled dataset of authentic and forged signatures, the CNN classifies new signatures by analyzing these learned features, accurately determining whether the signature is genuine or forged.

### Diagnosis and Recommendations

The diagnosis of signature forgery detection involves assessing the accuracy of the detection system in distinguishing genuine signatures from forgeries. Key factors for evaluation include the false positive rate, false negative rate, and overall classification accuracy. A robust system should minimize errors and reliably detect forgeries. Recommendations for improving performance include using a diverse and comprehensive dataset for training, enhancing feature extraction methods (e.g., incorporating both static and dynamic features), and fine-tuning the machine learning model with techniques like transfer learning or data augmentation to address challenges like variability in writing styles. Additionally, integrating multi-modal approaches combining both visual and behavioral data can further enhance the system's robustness.

### User Table

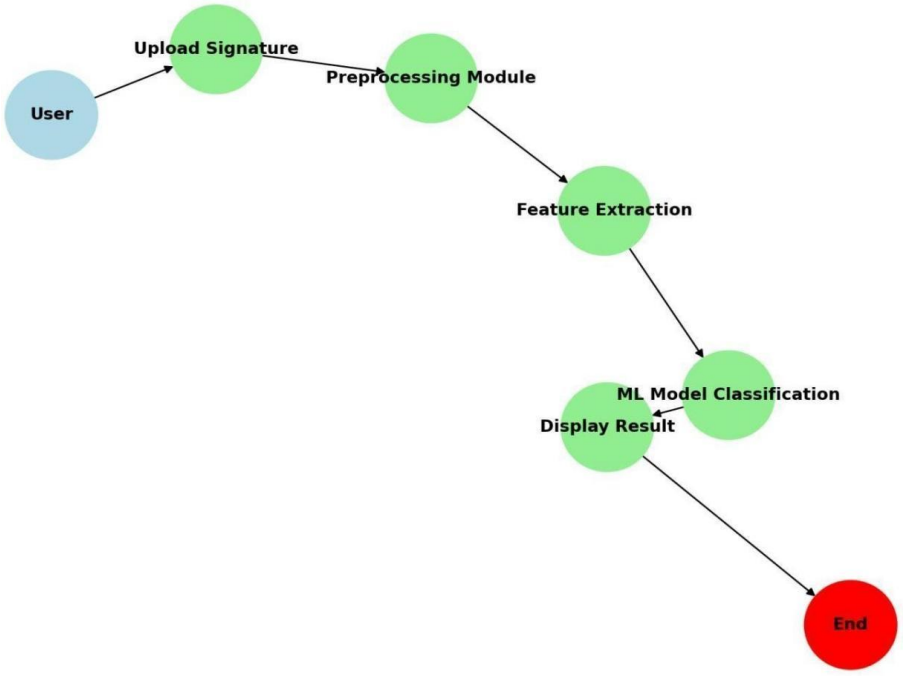
A user table for signature forgery detection typically includes key data fields to manage and authenticate signatures. This table would store information such as the user's unique ID, name, registered signature image (or dynamic signature data), and associated metadata (e.g., the date of registration or the device used). The system may also record multiple signature samples per user for comparison during verification. Additionally, the table might include flags or logs to track whether a signature has been verified as genuine or flagged as a potential forgery based on detection results. This structure ensures efficient signature verification and storage for future reference or audits

**Signature Table**

A signature table for signature forgery detection stores relevant data about each signature enrolled in the system. It typically includes fields such as the signature ID, user ID (linking the signature to a specific individual), the actual signature image or extracted features, the type of signature (e.g., static or dynamic), and the timestamp of when the signature was recorded. The table may also store verification results, such as whether the signature was classified as genuine or forged. This structured data enables efficient retrieval and comparison during the forgery detection process, helping to ensure accurate and reliable authentication of signatures.

### *SYSTEM ANALYSIS DIAGRAM*

Below is a high-level system architecture diagram illustrating interactions between users and system components:




**TABLES User Table**

| Column Name | Data Type | Description |
|---|---|---|
| User _id | INT (PK) | Unique user ID |
| name | VARCHAR (50) | User's full name |
| email | VARCHAR (50) | User’s email address |
| password | VARCHAR (100) | Encrypted password |
| Created _at | TIMESTAMP | Account creation date |

**Signature Table**

| Column Name | Data Type | Description |
|---|---|---|

| | | |
|---|---|---|
| Signature _id | INT (PK) | Unique signature ID |
| user_ id | INT (FK) | Reference to User table |
| Signature _image | BLOB | Uploaded signature file |
| Upload _date | TIMESTAMP | Date of upload |

**Feature Extraction Table**

| Column Name | Data Type | Description |
|---|---|---|
| Feature _id | INT (PK) | Unique feature ID |
| Signature _id | INT (FK) | Reference to Signature table |
| Stroke _width | FLOAT | Width of signature strokes |
| Texture _analysis | FLOAT | Texture feature values |
| Pressure _variation | FLOAT | Variation in writing pressure |

**Classification Result Table**

| Column Name | Data Type | Description |
|---|---|---|
| Result _id | INT (PK) | Unique result ID |
| Signature _id | INT (FK) | Reference to Signature table |
| classification | VARCHAR (10) | "Genuine" or "Forged" |
| Confidence _score | FLOAT | ML model's confidence level |
| Classification _date | TIMESTAMP | Date of classification |

## 3. SEGMENTATION

Segmentation in signature forgery detection refers to the process of dividing a signature into smaller, manageable components, such as strokes or regions, for analysis. This allows for more detailed examination of individual features like pen pressure, speed, and stroke dynamics, which are crucial for identifying inconsistencies or forgeries. By focusing on specific segments of a signature, forgery detection systems can more accurately compare the characteristics of the genuine

signature with the suspected forgery, improving detection accuracy.

***Feature Extraction***

Feature extraction is critical in identifying signature patterns. Key features analyzed include:

- **Stroke Patterns:** The sequence and direction of strokes are unique to individuals.
- **Pen Lifting:** The number and position of pen lifts during signature writing can be an indicator of authenticity.
- **Contour and Curvature:** The curves, loops, and sharp turns in a signature's contours are highly individual.

***Classification***

Signature forgery detection classification involves categorizing signatures into genuine or forged types using various machine learning techniques. The process typically includes two main approaches static and dynamic classification. In static classification, features like shape, size, and stroke patterns are analyzed without considering the writing process itself. Dynamic classification, on the other hand, takes into account temporal factors such as speed, pressure, and stroke dynamics during signature execution.

***Prediction Output***

The prediction output of signature forgery detection typically categorizes a signature as either genuine or forged. Based on the analysis of extracted features like stroke patterns, pressure, speed, and dynamic characteristics, machine learning models predict the likelihood of a signature being authentic or fraudulent. The output may be binary (genuine or forged) or probabilistic, providing a confidence score for the prediction. In more advanced systems, the prediction can also include a level of certainty or an error margin, helping assess the reliability of the detection process. The final result assists in decision-making regarding the authenticity of the signature.

## 4. MODEL ARCHITECTURE

The CNN model includes:

- **Image Preprocessing:** CNN-based models rely on high-quality input images of signatures.
- **Hierarchical Feature Extraction:** CNNs automatically learn hierarchical features from raw signature images.
- **Spatial Invariance:** CNNs are capable of handling spatial variations in signature orientation, position, and scale.
- **Pooling Layers:** Max-pooling layers in CNNs help reduce the dimensionality of the image data while preserving important features.
- **Training on Signature Datasets:** The model is trained using large datasets of authentic and forged signatures.

***Performance Evaluation***

The output design defines how results are presented to the user after processing. The system must display clear, accurate, and user-friendly results.

| Signature ID | Classification | Confidence Score | Date |
|---|---|---|---|
| 101 | Genuine | 98.5% | 10-03-2025 |
| 102 | Forged | 85.2% | 10-03-2025 |

Displays whether the signature is "Genuine" or "Forged". Includes a confidence score (%) from the ML model.

## 5. CONCLUSION

In conclusion, signature forgery detection is an essential process for ensuring the authenticity and integrity of documents in various sectors, including banking, legal, and identity verification. The increasing sophistication of forgeries calls for

advanced detection methods that can accurately distinguish between genuine and forged signatures. Approaches such as feature extraction, which analyzes geometrical, dynamic, and temporal characteristics, play a crucial role in identifying inconsistencies in signatures. Machine learning models, especially Convolutional Neural Networks (CNNs), have revolutionized the field by automatically learning and recognizing complex patterns in signature images, making the detection process more efficient and precise.

The combination of static and dynamic classification techniques, along with a robust training process using large datasets of authentic and forged signatures, enables the development of reliable prediction systems. These systems can generate accurate predictions, providing confidence scores that help in decision-making. Moreover, with the continuous advancement in deep learning and the availability of high-quality datasets, forgery detection models are becoming increasingly sophisticated, adapting to new types of forged signatures. Transfer learning and hierarchical feature extraction further enhance the ability of these systems to detect subtle anomalies, even in varied writing conditions.

Despite these advancements, challenges remain, such as variations in signature writing styles, the impact of environmental factors, and the need for real-time detection. However, ongoing research and the integration of newer technologies continue to improve the accuracy, efficiency, and robustness of signature forgery detection systems. Ultimately, the future of signature forgery detection lies in refining these methods and models to stay ahead of evolving forgery techniques, ensuring a higher level of security and trust in signature-based transactions.

This study demonstrates that deep learning and signatures processing techniques can significantly enhance Signature Forgery detection future enhancements may include:

- **Integration of Multimodal Approaches:** Combining static features (shape, size, and stroke patterns) with dynamic features (speed, pressure, and timing) can enhance detection accuracy.
- **Real-Time Forgery Detection:** Future systems could focus on real-time signature verification, integrating with mobile and digital platforms to provide instant feedback.
- **Improved Dataset and Transfer Learning:** Expanding signature datasets to include more diverse handwriting styles and variations will help models generalize better across different individuals.

### *FUTURE ENHANCEMENT*

The research conducted was able to implement VGG16 and random forest algorithms to find the forged signature data from the data set containing signature data both original and fake. The data was trained and tested on them without any difficulties. In future, we can try to analysis what can be done to increase the accuracy of the random forest algorithm as its accuracy was low when compared to VGG16. Due to the limitation of time the proposed 100 epochs could not be run which would have provided much better accuracy than the current result.

I am proposing to use the same technique with much better host machine with the required hardware and software and to have an additional period of time so that everything can be done much more efficiently. The use of larger datasets or multiple datasets can be implemented given more time in the future. With the help of more than one dataset, we can compare and contrast the difference in accuracy ranging among different datasets. Additionally, we can also try to update the project by including more algorithms. The number can be increased from two to five or six, which will help in testing and comparing the data and understanding the precision and accuracy of each algorithm. More output will mean more insight into how to tackle the issue of signature forgery efficiently. Thus, a better outlook on the subject can be attained in this way.

## REFERENCES

[1] R. Plamondon and S. Srihari, "On-line signature verification," Pattern Recognition, vol. 22, no. 2, pp. 107-131, 1999.

[2] P. Y. Cheng, L. J. Lee, and C. W. Chen, "Off-line signature verification using a novel feature extraction technique," Pattern Recognition, vol. 37, no. 1, pp. 221-229, 2004.

[3] N. R. Pal, R. C. Dubes, and A. K. Jain, "Signature verification: An overview," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, no. 1, pp. 1-12, 1990.

[4] M. Y. Lee, S. W. Kim, and J. H. Kim, "Offline signature verification using local directional pattern," Proceedings of the International Conference on Computer Vision and Image Processing, 2012.

[5] G. N. K. S. Kumar, R. Srinivasan, and S. Rajasekaran, "Forgery detection in signatures using deep learning," International Journal of Computer Applications, vol. 148, no. 3,

pp. 24-29, 2016.

[6] M. A. Bhuiyan, A. K. M. Z. Islam, and M. S. Hossain, "Automatic signature verification using dynamic

features," Proceedings of the International Conference on Image Processing, 2014.

[7] . Zhang, W. Liu, and C. Xu, "Forgery detection in handwritten signatures based on a deep learning approach," Expert Systems with Applications, vol. 42, no. 22, pp. 9121-9127, 2015.

...