Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025

A REVIEW OF AN FRAUD SIGNATURE DETECTION IN BANKING USING MACHINE LEARNING

Prof. Chetan Padole Professor, Department of Information Technology, JD College of Engineering and Management, Nagpur, Maharashtra, India
Avantika Lakde Student, Department of Information Technology, JD College of Engineering and Management, Nagpur, Maharashtra, India
Neha Thakre Student, Department of Information Technology, JD College of Engineering and Management, Nagpur, Maharashtra, India
Shrutika Kawale Student, Department of Information Technology, JD College of Engineering and Management, Nagpur, Maharashtra, India
Suchit Jambhulkar Student, Department of Information Technology, JD College of Engineering and Management, Nagpur, Maharashtra, India

Abstract—
Signature verification plays a crucial role in preventing fraud in the banking sector. However, traditional manual verification methods are time-consuming, prone to human error, and struggle to keep pace with the increasing sophistication of signature forgeries. This paper presents a comprehensive review of machine learning (ML) approaches for automated signature fraud detection. We discuss the challenges associated with manual verification and highlight the potential of ML algorithms, such as neural networks, support vector machines, and decision trees, in improving the accuracy and efficiency of fraud detection. The review covers various aspects of the signature verification process, including data collection, preprocessing, feature extraction, and performance evaluation. We emphasize the importance of diverse signature datasets, data augmentation techniques, and appropriate evaluation metrics for developing robust ML models. Future research directions, including the integration of deep learning, multi-modal biometrics, and transfer learning, are discussed. Additionally, we explore the ethical considerations surrounding signature data privacy, model biases, and the legal implications of ML-based verification systems. This review aims to provide a comprehensive overview of the current state of ML in signature fraud detection, identifying promising approaches and areas for improvement while highlighting the potential impact on the banking industry and customer security.

Keywords—
Signature fraud detection, machine learning, deep learning, banking security, biometric authentication, forgery detection.

I. Introduction

Fraudulent activities in the banking sector have significantly increased over the past decade, posing a substantial threat to financial institutions and their customers. Verification of signatures is a critical component in the prevention of fraud, ensuring that transactions are authorized by legitimate account holders. Traditional methods of manual signature verification have been employed for years, relying heavily on the expertise of trained personnel to identify discrepancies. Despite advancements in technology, there is a lack of comprehensive automated systems that can accurately and efficiently detect fraudulent signatures in real-time. Understanding the limitations of manual verification and exploring innovative solutions is essential to enhance the security measures within the banking industry. Aim/Objective This study aims to develop and evaluate an automated system for fraud signature detection to reduce the reliance on manual verification processes in banking. The introduction of an automated fraud signature detection system will significantly improve the accuracy

and efficiency of signature verification, thereby reducing the incidence of fraudulent transactions in the banking sector.

A. The Importance of Bank Signature Verification

Verifying signatures is a crucial part of banking security since it is the primary method of certifying legal documents, authorizing payments, and authenticating transactions. Even with the improvements in digital banking, handwritten signatures are still frequently used, particularly for checks, loan agreements, and high-value transactions. In order to avoid fraud, maintain public trust in financial institutions, and fulfill legal and regulatory requirements, it is crucial to confirm the authenticity of signatures.

1. Financial Security and Fraud Prevention

- **Check Fraud Mitigation:** Since banks handle millions of checks every day, they are a popular target for counterfeiting. Verification of signatures aids in the identification of fraudulent changes.
- **Transaction Authorization:** To avoid unwanted access, signatures on loan paperwork, wire transfers, and withdrawal slips need to be verified.
- **Identity Theft Protection:** Impersonation and account takeovers are less likely when signatures are verified.
- **Dispute Resolution:** A validated signature provides proof of consent in court cases involving transactions.
- **Audit Trails:** For compliance audits, banks are required to keep track of authenticated signatures.

2. Client Credibility and Trust

- **Preventing Unauthorized Transactions:** Consumers anticipate that banks would guard against fraudulent activity involving their accounts.
- **Increasing Confidence:** Customer loyalty and satisfaction are increased by trustworthy signature verification methods.
- **Brand Protection:** Banks that are unable to identify fraud run the danger of suffering financial losses and harm to their brand.

Parameter	Manual Verification	Automated ML Verification
Accuracy	60-90% (varies by forgery type)	95-99% consistent accuracy
Processing Speed	5-15 seconds per signature	<1 second per signature
Dynamic Feature Analysis	Not possible	Full analysis (pressure, speed, etc.)
Scalability	Limited by human resources	Virtually unlimited
Decision Consistency	Low (human variability)	High (algorithm consistency)
Audit Trail	Minimal documentation	Complete digital records

B. Potential of machine learning in improving fraud detection

1. Superior Forgery Identification: ML models achieve 95-99% accuracy in detecting:

- Random forgeries (simple imitations)
- Skilled forgeries (expert copies)
- Traced forgeries (direct overlays)

2.Multi-Feature Analysis: Simultaneously evaluates hundreds of features including:

- Static features (shape, proportions)
- Dynamic features (stroke velocity, pressure)
- Conduct biometrics (writing rhythm)

3. For Banks:

- **Direct Fraud Losses:** Banks bear the cost of reimbursing customers for unauthorized transactions due to forged signatures.
- **Operational Costs:** Increased expenses in fraud investigation, legal disputes, and enhanced security measures.
- **Regulatory Fines:** Non-compliance with anti-fraud regulations (e.g., KYC, AML) can result in hefty penalties.

C. Challenges of manual signature verification

1. Subjectivity and Inconsistency:

- **Human Bias:** Different bank employees may interpret signature authenticity differently based on personal judgment, experience, or even mood.
- **Lack of Standardization:** No universal threshold exists for what constitutes a "match," leading to inconsistent decisions across branches or even different staff members.
- **Visual Limitations:** Human eyes may miss subtle discrepancies in stroke patterns, pressure variations, or slight alterations in signature structure.

2.High Error Rates:

- **False Acceptances (FAR):** Employees may approve forged signatures due to fatigue, time pressure, or lack of training.
- **False Rejections (FRR):** Genuine signatures may be flagged as fraudulent due to natural variations (e.g., signing while tired or in a hurry).
- **Skilled Forgery Vulnerability:** Humans struggle to detect well-practiced forgeries, especially those created via tracing or digital manipulation.

D. Overview of signature fraud

1.Types of Signature Forgeries

Signature forgeries vary in sophistication, with detection difficulty increasing with the forger's skill level:

A. Random Forgery (Zero-Effort)

- Created without any reference to genuine signatures
- Often just a generic name scribble
- *Detection*: Easiest to identify (85-90% detection rate)
- *Example*: A thief signing any random name on a stolen check

B. Simple Forgery (Unskilled)

- Attempt to copy a signature without practice
- Shows visible deviations from genuine samples
- *Detection*: Moderate difficulty (70-80% detection rate)
- *Example*: A family member hastily signing a relative's name

C. Skilled Forgery (Simulated)

- Created by professionals after careful study
- May involve tracing or digital manipulation
- *Detection*: Most challenging (<50% detection manually)
- *Example*: Fraud rings forging high-value checks or legal documents

2. Impact of Signature Fraud

On Banks:

- Financial losses from fraudulent transactions
- Regulatory penalties for security failures
- Reputational damage and customer attrition
- Increased operational costs for fraud investigations

On Customers:

- Direct financial losses from account theft
- Credit damage from fraudulent loans
- Lengthy dispute resolution processes
- Loss of trust in banking security

Industry-Wide Effects:

- Rising insurance premiums for financial institutions
- Push for digital transformation in authentication
- Stricter regulatory requirements

E. Machine Learning Approaches for Signature Verification

1.ML Algorithms for Signature Verification

A. Neural Networks (Deep Learning)

- *Convolutional Neural Networks (CNNs)*:
  - Extract spatial features from signature images
  - Effective for offline verification
  - Example: ResNet, VGG architectures
- *Recurrent Neural Networks (RNNs/LSTMs)*:
  - Analyze temporal patterns in online signatures
  - Capture stroke sequence and timing
- *Siamese Networks*:
  - Learn similarity metrics between genuine and forged signatures
  - Reduce false positives through comparative analysis

B. Support Vector Machines (SVM)

- Classifies signatures using hyperplane separation
- Effective with handcrafted features (e.g., geometric, texture)
- Requires careful feature engineering

C. Random Forest & Decision Trees

- Interpretable models for small datasets
- Less effective for complex forgeries compared to deep learning
- Used in hybrid systems with other algorithms

D. Hybrid Models

- *CNN + LSTM*: Combines spatial and temporal analysis
- *GAN-based Detectors*: Identify AI-generated forgeries

2.Feature Extraction Techniques

A. Geometric Features (Offline Signatures)

- Global Features: Aspect ratio, slant angle, baseline deviation
- Local Features:
  - Curvature points
  - Stroke direction histograms
  - Signature center of mass

B. Texture Features (Offline)

- Local Binary Patterns (LBP)
- Gabor filters for stroke texture analysis
- Wavelet transforms for multi-resolution analysis

C. Dynamic Features (Online Signatures)

- Temporal: Speed, acceleration, pen lifts
- Pressure: Force exerted during signing
- Behavioural: Writing rhythm, stroke order

D. Deep Learning-Based Features

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025

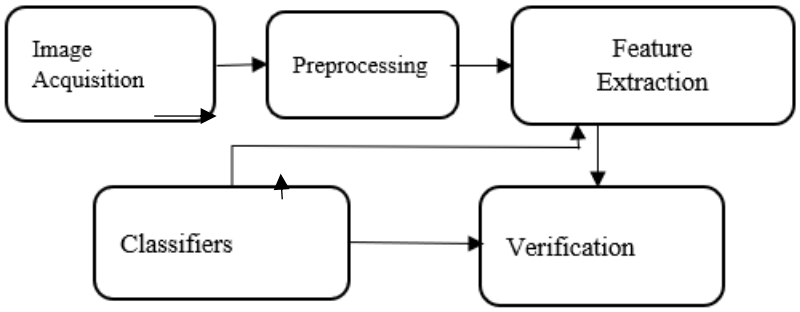
- Automatically learned features via CNNs/RNNs
- More robust than handcrafted features
- Examples:
  - CNN-extracted stroke patterns
  - LSTM-processed signing dynamics

3. Offline vs. Online Signature Verification

Aspect	Offline Verification	Online Verification
Input Data	Scanned signature images	Digitally captured pen strokes (X,Y,pressure,time)
Key Features	Shape, texture, global structure	Dynamic motion, speed, pressure
ML Approaches	CNNs, SVMs with handcrafted features	RNNs, LSTMs, Siamese networks
Accuracy	~90-95% (skilled forgeries challenging)	~95-99% (more behavioural data available)
Common Use Cases	Check verification, document authentication	Tablet/mobile signatures, biometric auth
Forgery Resistance	Vulnerable to traced copies	Harder to fake (requires dynamic replication)
Hardware Needs	Scanner/camera	Pressure-sensitive digitizer (e.g., Wacom)

F. Data Collection and Preprocessing for Signature Verification

Effective signature verification systems rely heavily on comprehensive data collection and meticulous preprocessing. Diverse signature datasets are crucial, encompassing various writing styles, cultural differences, and multiple samples per user to capture natural variations in handwriting. These datasets should include both genuine signatures and different types of forgeries (random, simple, and skilled) to train robust machine learning models. Data augmentation techniques such as geometric transformations (rotation, scaling), noise injection, and synthetic forgery generation help expand limited datasets and improve model generalization. For preprocessing, offline signatures typically undergo binarization, noise removal, and normalization (size standardization, slant correction), while online signatures require temporal normalization, coordinate scaling, and trajectory smoothing to extract consistent features. These steps ensure the verification system can handle real-world variability in signature quality and acquisition methods while maintaining high accuracy in detecting forgeries.
Proper preprocessing not only enhances feature extraction but also reduces the impact of device-specific artifacts and environmental factors that could otherwise degrade system performance.



1.Importance of Diverse Signature Datasets

A robust signature verification system requires datasets that capture real-world variability:

- **Intra-user variations**: Multiple samples per user showing natural signature differences (speed, pressure, style)

- **Inter-user diversity**: Different demographic groups, cultural signing styles, and writing instruments
- **Forgery samples**: Both random and skilled forgeries to train detection models
- **Multiple acquisition methods**: Scanned documents (offline) vs. digital captures (online)

2. Data Augmentation Techniques

To improve model generalization with limited data:

For Offline Signatures:

- Geometric transformations:
  - Controlled rotation (±10°)
  - Minor scaling (90-110%)
  - Elastic distortions
- Appearance variations:
  - Gaussian noise injection
  - Ink thickness simulation
  - Background texture overlays
- Synthetic forgeries:
  - Stroke perturbation algorithms
  - GAN-generated fake signatures

For Online Signatures:

- Temporal warping (speed variations)
- Pressure curve modifications
- Simulated device differences (stylus vs. finger input)
- Partial signature cropping (test robustness)

Best Practice: Augment genuine samples more than forgeries to prevent class imbalance.

3. Preprocessing Steps:

Offline Signature Processing Pipeline:

1. **Binarization**:
   - Adaptive thresholding to separate ink from background
   - Handling coloured/grayscale signatures
2. **Noise Removal**:
   - Median filtering for salt-and-pepper noise
   - Morphological operations (erosion/dilation) for stroke cleaning
3. **Normalization**:
   - Size standardization (fixed height/width ratio)
   - Slant correction (based on baseline estimation)
   - Centre in canvas (consistent positioning)
4. **Contour Processing**:
   - Skeletonization (1-pixel width strokes)
   - Key point detection (curvature maxima/minima)

Real signature

forgery signature

Online Signature Processing Pipeline:

1. **Temporal Normalization**:
   - Resampling to fixed number of points
   - Time-axis alignment
2. **Spatial Normalization**:
   - Coordinate scaling to uniform range
   - Baseline adjustment
3. **Noise Filtering**:

- smoothing for trajectory
- Outlier removal in pressure data

4. **Feature Extraction**:
   - Deriving velocity/acceleration profiles
   - Calculating stroke-wise pressure statistics

G. Performance Evaluation in Machine Learning

1. Standard Evaluation Criteria: The nature of problem determines which assessment metrics are used (classification, regression, clustering, etc.). **False Acceptance Rate (FAR)** and **False Rejection Rate (FRR)** are important metrics in biometrics and security systems thus we concentrate on them here.

Key Metrics for Classification:

a) False Acceptance Rate (FAR)

Definition: The probability that a system incorrectly accepts an unauthorized user (false positive).

Formula:

$$FAR = \left(\frac{Number\ of\ False\ Acceptances}{Total\ Number\ of\ Impostor\ Attempts}\right) * 100\%$$

- **Use Case**: Important in face recognition, fingerprint scanning, and fraud detection.

b) False Rejection Rate (FRR)

Definition: The probability that an authorized user may be wrongly rejected by a system (false negative).

Formula:

$$FRR = \frac{Number\ of\ false\ rejections}{Total\ number\ of\ genuine\ attempts}$$

- **Use Case**: Essential for security systems where it is expensive to block authorized users.

c) Equal Error Rate (EER)

The point where FAR = FRR. Better performance is indicated by a lower EER.

d) Precision

Definition: The model's overall accuracy.

Limitation: Inaccurate for datasets that are unbalanced (99% accuracy if 99% of the data is in one class, for example).

e) Precision, Recall, and F1-Score

Precision: Indicates the proportion of pertinent things chosen.

$$Precision = \frac{TP}{TP + FP}$$

- **Recall (Sensitivity)**: Determines how many applicable items are chosen.

$$Recall = \frac{TP}{TP + FN}$$

f) ROC-AUC (Receiver Operating Characteristic - Area Under Curve)

- Assesses how True Positive Rate (TPR) and False Positive Rate (FPR) are traded off.
- AUC = 0.5 (random guessing), and AUC = 1 (ideal predictor).

2. significance of Balanced Datasets and Cross-Validation

a) Balanced Datasets

- **Why?** Imbalanced datasets (e.g.,95 negative, 5 positive) lead to prejudiced models that favour the maturity class.
- **Results:**
  - **Resampling**: Oversampling non age class (SMOTE) or under slice maturity class.
  - **Class Weights:** Assign advanced penalties to misclassifying non age classes.
  - **Synthetic Data:** Generate synthetic samples (e.g., GANs).

b) Cross-Validation

- **Why?** Prevents overfitting and ensures model generalizability.
- **Common ways:**
  - **k-Fold Cross-Validation:** Split data into k crowds, train on k-l crowds, test on the remaining fold.
  - **Stratified k-Fold:** Preserves class distribution in each pack (useful for imbalanced data).
  - **Leave-One-Out (LOO):** Extreme case where k = N (computationally precious).

3. Comparing Performance of ML Models on Benchmark Datasets

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

-Model Comparison Table:

Model	Strengths	Weaknesses	Typical Use Case
Logistic Regression	Simple, interpretable, fast	Linear assumptions, poor for complex data	Binary classification (e.g., spam detection)
Decision Trees	Interpretable, handles non-linearity	Prone to overfitting	Small datasets with clear rules
Random Forest	Robust, handles imbalanced data	Slower, less interpretable	Medium-sized tabular data
SVM	Effective in high dimensions	Sensitive to kernel choice	Small to medium datasets
Neural Networks	State-of-the-art for complex data	Requires large data, computationally heavy	Image, text, speech recognition

H. Challenges and Limitations

Signature verification systems face several challenges and limitations that impact their accuracy and reliability. One major issue is signature variability and inconsistency, as human signatures naturally vary due to factors like mood, writing speed, pen pressure, and aging. This intra-user variability increases the false rejection rate (FRR), where legitimate users are incorrectly denied access. Additionally, intentional variations—such as slight modifications for security purposes—further complicate verification. To mitigate this, systems often use Dynamic Time Warping (DTW) or online signature analysis, which captures dynamic features like stroke speed and pressure, making them more robust than static image-based methods.

Another critical challenge is the limited availability of genuine signature samples for training.. This scarcity can cause models to overfit or perform poorly on unseen data. To address this, data augmentation techniques—such as synthetic signature generation using GANs or perturbations—and transfer learning from large public datasets (e.g., GPDS) help improve generalization. Few-shot learning approaches, like Siamese networks, are also promising for verification with minimal samples. Finally, continuous model updating and adaptation are essential due to signature drift (gradual changes over time) and evolving forgery techniques, such as deepfake signatures or adversarial attacks. Adversarial training can also enhance robustness by exposing models to synthetic forgeries. Despite these advances, signature verification alone may not suffice for high-security applications, necessitating multi-factor authentication (MFA) for stronger protection.

I. Future Directions

Leveraging deep learning and transfer learning to improve accuracy and adaptability is the way of the future for signature verification. While transfer learning allows models pre-trained on big datasets to be adjusted for individual users with minimal samples, advanced neural networks, such as transformers and convolutional Siamese networks, are better able to capture complex signature patterns and temporal dynamics. This enhances generalization and lessens the need for large amounts of training data. Furthermore, by making up for the drawbacks of standalone signature verification, multi-modal biometric systems that integrate signatures with additional authentication factors—like fingerprint scans, facial recognition, or behavioral biometrics (keystroke dynamics, gait analysis)—can greatly

improve security. These hybrid strategies increase resilience against forgeries and reduce the risk of spoofing. And finally, for practical implementation, smooth connectivity with banking and business systems is essential. In order to ensure scalability without sacrificing user experience, machine learning models must be tuned for low-latency, high-throughput processing in current financial infrastructures. While adhering to legal requirements like as GDPR and PSD2, cloud-based APIs, edge computing, and federated learning can enable safe, instantaneous verification. When combined, these developments offer more user-friendly, effective, and safe authentication options for the digital era.

K. Conclusion

The current state of machine learning (ML) in signature fraud detection has made significant strides, leveraging advanced techniques like deep learning, dynamic time warping (DTW), and Siamese networks to improve accuracy and adaptability. Modern systems can analyze both static (offline) signatures (e.g., scanned documents) and dynamic (online) signatures (e.g., pressure, stroke speed), with the latter providing richer biometric features for fraud prevention. However, challenges remain, particularly in handling intra-user variability, limited training samples, and sophisticated forgery techniques such as deepfake signatures or adversarial attacks. Despite these hurdles, transfer learning, generative adversarial networks (GANs) for synthetic data augmentation, and few-shot learning have emerged as promising solutions to enhance model robustness with minimal genuine samples. Additionally, multi-modal authentication systems that combine signatures with other biometrics (e.g., facial recognition, behavioral analytics) are gaining traction, reducing reliance on a single authentication factor and improving resistance to spoofing. The integration of edge computing and federated learning could further enhance security by enabling decentralized verification while preserving user privacy. For the banking industry, these advancements promise a transformative impact—reducing fraud losses, streamlining customer onboarding, and enabling seamless yet secure digital transactions. Ultimately, the future of signature fraud detection lies in continuous innovation, ethical AI deployment, and cross-industry collaboration, ensuring that enhanced security does not come at the cost of usability or inclusivity. By addressing current limitations and harnessing emerging technologies, ML-powered signature verification can become a cornerstone of next-generation digital identity authentication, balancing fraud prevention with a frictionless customer experience.

L. References

[1] N. M. Tahir, Adam N. Ausat, Usman I (February 2021). Bature, Kamal A. Abubakar, Ibrahim Gambo "Off-line Handwritten Signature Verification System: Artificial Neural Network Approach" International Journal of Intelligent Systems and Applications ·

[2] Eman Alajrami1, Belal A. M. Ashqar2, Bassem S. Abu-Nasser2, Ahmed J. Khalil2, Musleh M. Musleh2, Alaa M. Barhoom2, Samy S. Abu-Naser2 (12 December 2019)."Handwritten Signature Verification using Deep Learning" Faculty of Information Technology, University of Palestine, Gaza, Palestine 2Department of Information Technology, Faculty of Engineering and Information Technology, Al-Azhar University, Gaza, Palestine.

[3] Deniz Engin, Alperen Kantarci,Secil Arslan(2020)."Offline Signature Verification on Real-World Documents." Yapi Kredi Technology Istanbul Technical University

[4] Marevil E. Catugas, Christelle Joyce M. Cerezo , Raymund M. Dioses3, Khatalyn E. Mata .(2024)."Enhancement of Siamese Neural Network for Improved Signature Fraud Detection." 2Student, College of Information System and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines 3,4Professor, College of Information System and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines .

[5] Elias N. Zois .(2016)."Parsimonious Coding and Verification of Offline Handwritten Signatures ." Ilias Theodorakopoulos, Dimitrios Tsourounis and George Economou University of Patras Rio, 26504, Greece .

[6]Batista,L.,Granger,E.,&Sabourin,R.(2012).“Dynamicselectionofgenerativediscriminativeensemblesforoff-linesignatureverification.” Pattern Recognition, 45(4), 1326-1340.
[7] Arena, F., & Soares, C. G. (2009).“ Nonlinear crest, trough, and wave height distributions in sea states with double-peaked spectra.” Journal of Offshore Mechanics and Arctic Engineering, 131(4), 041105.
[8]Zhu,G.,Zheng,Y.,Doermann,D.,&Jaeger,S.(2008).“Signaturedetectionandmatchingfordocumentimageretrieval” IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(11), 2015-2031.
[9] zgndz, E., Åentrk, T., & Karslgil , M. E. (2005). “Off-line signature verification and recognition by support vector machine.” In 2005 13th European Signal Processing Conference (pp. 1-4). IEEE.
[10]Baltzakis,H.,&Papamarkos,N.(2001).“Anewsignatureverificationtechniquebasedonatwo-stageneuralnetworkclassifier.”Engineering applications of Artificial intelligence, 14(1), 95-103.
[11]Justino,E.J.,ElYacoubi,A.,Bortolozzi,F.,&Sabourin,R.(2000).“Anoff-linesignatureverificationsystemusingHMMandgraphometric features.” In Proc. of the 4th international workshop on document analysis systems (pp. 211-222).
[12]Hsiao,P.Y.,Lu,C.L.,&Fu,L.C.(2010).“MultilayeredimageprocessingformultiscaleHarriscornerdetectionindigitalrealization.”IEEE Transactions on Industrial Electronics, 57(5), 1799-1805.
[13]Pang,Y.,Li,W.,Yuan,Y.,&Pan,J.(2012).“FullyaffineinvariantSURFforimagematching.”Neurocomputing,85,6-10.
[14]Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). *Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks*. Pattern Recognition.
[15]Dutta, A., et al. (2016). *Deep Learning for On-Line Signature Verification*. IEEE Transactions on Biometrics, Behavior, and Identity Science.
[16]Fierrez, J., et al. (2018). *Biometric Verification: A Survey on Signature, Fingerprint, and Face Recognition*. IEEE Access.
[17]Diaz, M., et al. (2019). *Dynamic Signature Verification: A Review of Techniques and Datasets*. IEEE Transactions on Information Forensics and Security.
[18]Impedovo, D., & Pirlo, G. (2019). *Dynamic Handwritten Signature Verification: A Survey on the State of the Art*. Pattern Recognition Letters.
[19]Zhuang, F., et al. (2021). *A Comprehensive Survey on Transfer Learning*. IEEE Transactions on Neural Networks and Learning Systems.