E-ISSN: 111 – 2716 P-ISSN: 3026 – 8214
MPRI-JAAER | INTERNATIONAL JOURNAL OF APPLIED & ADVANCED ENGINEERING RES.
VOL. 13 NO. 5 JULY, 2026

DEVELOPMENT OF AN INTELLIGENT OFFLINE SIGNATURE VERIFICATION SYSTEM USING DEEP RESIDUAL NEURAL NETWORKS (ResNet)

BELLO O. LAWAL; & ISAH M. M
Department of Computer Engineering, Edo State University Iyamho, Edo State, Nigeria.
Corresponding Author: bosslawal007@yahoo.com
DOI: https://doi.org/10.70382/mejaaer.v13i5.066

Abstract

Offline signature verification remains a critical biometric authentication challenge due to the inherent variability in genuine signatures and the increasing sophistication of forgery techniques. This study develops an intelligent offline signature verification system leveraging Deep Residual Neural Networks (ResNet) to address these challenges. The proposed system employs a ResNet-50 architecture with transfer learning to automatically extract discriminative features from static signature images, eliminating the need for handcrafted feature engineering. The model was trained and evaluated on benchmark signature datasets, including CEDAR and GPDS, with comprehensive image preprocessing and augmentation techniques applied to enhance generalization. The system achieved superior performance with a verification accuracy of 98.2%, significantly outperforming conventional CNN architectures (91.7%). The False Acceptance Rate (FAR) and False Rejection Rate (FRR) were recorded at 0.015 and 0.012 respectively, demonstrating the model's effectiveness in distinguishing genuine signatures from skilled forgeries. The residual learning framework effectively mitigates the vanishing gradient problem, enabling deeper network

Keywords: Offline Signature Verification, ResNet, Deep Learning, Biometric Authentication, Transfer Learning, Forgery Detection, Residual Networks

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

training and more robust feature representation. This research contributes a reliable, scalable solution for automated signature verification applicable in banking, legal, and administrative domains where document authentication is paramount.

Introduction

Background to the Study

Biometric authentication has emerged as a cornerstone of modern identity verification, offering enhanced security over traditional knowledge-based and token-based methods. Among various biometric modalities, handwritten signatures hold a unique position due to their long-standing legal and social acceptance in financial transactions, legal documentation, and administrative procedures. The signature verification process involves determining the authenticity of a claimed identity by analyzing the characteristics of a handwritten signature. This task can be approached in two ways: online (dynamic) verification, which captures temporal information such as pen pressure and stroke velocity, and offline (static) verification, which analyzes the signature from scanned images or photographs (Saranya and Ramyadevi, 2025). Despite the proliferation of digital authentication methods, offline signature verification remains indispensable in scenarios where only paper-based documents are available, such as bank cheques, legal contracts, and government forms.

The widespread adoption of signature-based authentication stems from its non-invasive nature, ease of collection, and established legal framework. However, the manual verification of signatures by human experts is increasingly inadequate given the volume of transactions requiring authentication. Human examiners are susceptible to fatigue, cognitive biases, and the inherent difficulty of distinguishing highly skilled forgeries from genuine signatures (Pal, et.al, 2026). Consequently, there is a pressing need for automated signature verification systems that can provide consistent, accurate, and efficient authentication services.

The advent of deep learning, particularly Convolutional Neural Networks (CNNs), has revolutionized pattern recognition tasks, including signature verification. Deep learning methods offer the advantage of automatic feature extraction, eliminating the reliance on handcrafted features that often fail to capture the full complexity of signature variations (He, et.al, 2016). Among deep learning architectures, Residual Neural Networks (ResNet) have demonstrated remarkable success in image classification tasks by addressing the degradation problem that affects very deep networks (Singh and Sharma, 2025). The residual learning framework enables the training of substantially deeper networks by

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

allowing gradients to flow directly through shortcut connections, thereby mitigating the vanishing gradient problem.

Problem Statement

Despite significant advances in deep learning, offline signature verification systems face persistent challenges that hinder their deployment in real-world applications. One fundamental challenge is the substantial intra-class variability exhibited by genuine signatures. A person's signature can vary considerably depending on factors such as mood, health, writing speed, and the physical conditions under which the signature is produced (Garcia, et.al, 2022). This natural variation makes it difficult to establish a definitive template for authentic signatures, leading to potential false rejections of genuine users.

Conversely, the threat of skilled forgery represents an equally significant challenge. A skilled forger can practice mimicking a target signature to produce copies that closely resemble the original, often deceiving both human experts and automated systems (Jain and Singh, 2022). The distinction between genuine signatures and skilled forgeries becomes particularly difficult when the forger has access to multiple genuine samples for practice. This problem of inter-class similarity requires systems to capture subtle discriminative features that differentiate authentic signatures from sophisticated imitations.

Existing signature verification approaches face several limitations. Traditional methods that rely on handcrafted features struggle to generalize across different writing styles and are sensitive to noise and variations in image quality (Khan, et.al, 2026). Conventional CNN architectures, while more robust, often require extensive feature engineering and may not adequately capture the fine-grained patterns essential for distinguishing between genuine and forged signatures. Furthermore, many proposed systems are writer-dependent, requiring separate models for each user, which limits their scalability in practical applications.

Aim and Objectives of the Study

The aim of this study is to develop an intelligent offline signature verification system using a Deep Residual Neural Network (ResNet-50) architecture that can effectively distinguish between genuine and forged signatures with high accuracy and robustness. The specific objectives of this research are:

1. To design and implement a ResNet-50-based architecture for offline signature verification using transfer learning from pre-trained ImageNet weights.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

2. To develop comprehensive image preprocessing and data augmentation techniques to enhance model generalization and robustness to signature variations.
3. To train the proposed model on benchmark signature datasets and optimize hyperparameters for optimal verification performance.
4. To evaluate the system performance using standard metrics including accuracy, precision, recall, F1-score, False Acceptance Rate (FAR), and False Rejection Rate (FRR).
5. To compare the performance of the ResNet-50-based system against conventional CNN architectures to demonstrate the efficacy of residual learning.

Scope of the Study

This research is focused on offline (static) signature verification using deep learning techniques. The study is delimited to the following aspects:

1. The research utilizes publicly available benchmark datasets, including CEDAR and GPDS, which contain genuine and forged signature samples from multiple writers.
2. The primary architecture employed is ResNet-50 with transfer learning, compared against conventional CNN baselines.
3. The system employs a writer-independent verification approach, where a single model is trained to verify signatures from multiple writers.
4. Performance is evaluated using standard classification metrics and forgery-specific metrics, including FAR and FRR.
5. The system is designed to detect both random and skilled forgeries, with the latter representing the more challenging case.
6. The study does not address online signature verification, which requires dynamic capture devices, nor does it cover the development of specialized hardware for signature capture.

Significance

The significance of this research lies in its contributions to the fields of biometric authentication, computer vision, and security systems. First, the development of an accurate offline signature verification system addresses a critical real-world need in banking, legal, and administrative domains where document fraud prevention is paramount. By automating the verification process, the system can reduce the time and cost associated with manual signature verification while improving accuracy and consistency.

Second, the application of ResNet architecture to signature verification represents a methodological advance in the field. The residual learning framework enables the training

of deeper networks that can capture more complex signature patterns, potentially leading to improved discrimination between genuine and forged signatures. This research contributes empirical evidence on the effectiveness of residual networks for this specific task.

Third, the systematic evaluation of model performance using multiple metrics, including FAR and FRR that are particularly relevant to biometric systems, provides a comprehensive assessment that facilitates comparison with other approaches. This contributes to establishing benchmarks in the signature verification literature.

Contribution of the Study

This study makes the following contributions to the field:

Implementation and evaluation of a ResNet-50-based signature verification system with transfer learning, demonstrating the effectiveness of residual learning for this task.

Development of a comprehensive preprocessing and augmentation pipeline tailored to the characteristics of signature images, addressing common challenges such as variation in writing styles and image quality.

Quantitative evaluation of system performance on benchmark datasets using multiple metrics, providing evidence of the proposed approach's efficacy and facilitating comparison with other methods.

Demonstration of the feasibility of deploying ResNet-based systems for practical signature verification applications, with implications for banking, legal, and administrative sectors.

Offline Signature Verification

Offline signature verification is the process of determining the authenticity of a handwritten signature from a static image without access to dynamic writing information (Saranya and Ramyadevi, 2025). This task is fundamentally challenging because signatures are behavioral biometrics that exhibit significant intra-class variation even for the same individual. Factors such as writing speed, mood, health, and the physical properties of writing instruments and paper can all affect the appearance of a signature.

Conventional approaches to offline signature verification relied heavily on handcrafted features extracted from signature images. These features typically include global features such as aspect ratio, area, and moments; statistical features such as mean and variance of pixel distributions; and structural features that capture the geometric properties of the signature (Pal, et.al, 2026). However, these methods often fail to generalize across different writing styles and are sensitive to noise and variations in image quality.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Signature Forgery and Verification Challenges

Signature forgery represents a primary threat to signature-based authentication systems. Forgeries are categorized into three types: random forgeries (the forger uses their own signature without knowledge of the target), simple forgeries (the forger knows the target's name but not the signature style), and skilled forgeries (the forger has studied and practiced replicating the target's signature) (Jain and Singh, 2022). Skilled forgeries are the most challenging to detect, as they can closely resemble genuine signatures.

The verification process must balance two competing objectives: accepting genuine signatures while rejecting forgeries. This trade-off is quantified by the False Rejection Rate (FRR), the proportion of genuine signatures incorrectly rejected, and the False Acceptance Rate (FAR), the proportion of forgeries incorrectly accepted (Reddy and Srivastava, 2026). An ideal system minimizes both rates simultaneously, but in practice, there is typically a trade-off between them.

Additional challenges include the limited availability of forged signatures for training, as collecting genuine forgeries from skilled forgers is difficult and ethically problematic. Many studies address this by generating synthetic forgeries through various transformations applied to genuine signatures or by using publicly available datasets that include forged samples.

Deep Learning for Signature Verification

Deep learning has emerged as a powerful tool for addressing the challenges of offline signature verification. Unlike traditional methods that require manual feature engineering, deep neural networks can automatically learn discriminative features from raw image data. Convolutional Neural Networks (CNNs), in particular, have proven effective for image-based tasks due to their ability to capture hierarchical features from low-level edges to high-level patterns.

Recent studies have explored various deep learning architectures for signature verification. Some approaches use Siamese networks with contrastive or triplet loss functions to learn similarity metrics between pairs of signatures, enabling writer-independent verification (Lee, et.al, 2022). Others employ standard classification architectures, treating the problem as a binary classification task where the input is a signature image and the output is a binary label indicating authenticity.

The choice of architecture significantly impacts performance. A comparative study of eight deep learning architectures found significant variation in verification performance, with residual networks generally outperforming lightweight and compound-scaled models (Zhang, et.al, 2025). This finding highlights the importance of architectural design in achieving robust verification performance.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

ResNet and Residual Learning

Residual Neural Networks (ResNet), introduced by He et al., address the degradation problem encountered when training very deep neural networks (Singh and Sharma, 2025). As networks become deeper, training accuracy saturates and then degrades rapidly, not due to overfitting but due to optimization difficulties. ResNet addresses this by introducing residual connections, or shortcut connections, that allow gradients to flow directly through the network, mitigating the vanishing gradient problem.

The fundamental insight behind residual learning is that it is easier to optimize the residual mapping than the original mapping. Instead of learning the underlying mapping H(x) directly, the network learns the residual F(x) = H(x) - x, which is added to the identity mapping x. This formulation allows the network to learn incremental refinements to the input, enabling the training of networks with hundreds of layers.

ResNet has been widely adopted in various computer vision applications, including biometric systems. For signature verification, residual networks have demonstrated strong performance due to their capacity to learn fine-grained features while maintaining effective training dynamics (Kamble and Hegadi,2025). Recent work has explored ensemble approaches combining multiple ResNet models for improved feature extraction and verification performance (Khalid, et.al, 2026).

Empirical Review

The following table provides a concise summary of empirical studies on deep learning-based signature verification:

Study	Method	Dataset	Key Results
Chaudhary et al. (2026)	Custom ResNet-CNN with augmentation	10 writers	Accuracy: 83.55%, FAR: 14.92%, FRR: 18.35% (Chaudhary, et.al, 2026)
ResNet18 Unified Framework (2025)	ResNet18 classifier with cosine similarity	430 users, 17,000+ signatures	Classification: 93.85%, Verification: 90.07% (Patel, et.al, 2025)
ArcLoss-AutoEncoder Fusion (2025)	ResNet50 + ArcLoss + AutoEncoder	CEDAR, GPDS, Chinese DB	Accuracy: 99.7% (ResNet50), FAR: 0.01, FRR: 0.02 (Chen, et.al, 2025)
Enhanced ResNet Ensemble (2025)	ResNet18 + ResNet34 ensemble + SVM	BHsig-260, CEDAR	Superior to state-of-the-art (Khalid, et.al, 2026)

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Study	Method	Dataset	Key Results
SigVerify (2025)	CNN with augmentation	3,000 images	Accuracy: 94.8% (Verma and Kumar, 2025)
Data-Augmented L2 CNN (2025)	CNN with augmentation and regularization	Kaggle, Custom dataset	Accuracy: 98.2% (Kaggle) (Park, et.al, 2025)

Research Gap

Despite significant progress in deep learning-based signature verification, several gaps remain in the literature. First, while ResNet has been applied to this task, comprehensive evaluations comparing ResNet variants with conventional CNNs under controlled conditions are limited. A unified benchmarking framework study found significant performance stratification across architectures, but the specific comparison of ResNet-50 against conventional CNNs for signature verification requires further investigation (Zhang, et.al, 2025).

Second, many studies focus on writer-dependent approaches or specialized architectures like Siamese networks, which, while effective, may not be easily generalizable across datasets. The potential of simpler writer-independent classifier-based approaches using standard architectures like ResNet deserves further exploration (Khan, et.al, 2026).

Third, comprehensive evaluation metrics, particularly FAR and FRR that are critical for biometric systems, are inconsistently reported across studies, making meaningful comparison difficult. There is a need for studies that systematically report these metrics alongside classification accuracy.

Finally, the practical implications of deploying ResNet-based systems in real-world settings require further investigation, including considerations of computational efficiency, scalability, and robustness to variations in signature quality and presentation.

Research Design

This study adopts a quantitative experimental research design to develop and evaluate an intelligent offline signature verification system. The research follows a systematic approach involving data acquisition, preprocessing, model development, training, and performance evaluation. The independent variable is the signature image input, while the dependent variables are the model's classification predictions (genuine vs. forged) and associated performance metrics.

The experimental framework comprises four phases: (1) data preparation, including acquisition, preprocessing, and augmentation; (2) model development, including the implementation of the proposed ResNet-50 architecture and conventional CNN baseline;

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

(3) model training and optimization; and (4) performance evaluation and comparative analysis.

Dataset and Data Acquisition

The research utilizes the CEDAR (Center of Excellence for Document Analysis and Recognition) signature dataset and the GPDS (Grupo de Procesado Digital de Señales) signature corpus, two widely used benchmark datasets in signature verification research. The CEDAR dataset contains signatures from 55 writers, with 24 genuine signatures and 24 forged signatures per writer, totaling 1,320 genuine and 1,320 forged samples. The forgeries were created by individuals who studied the original signatures and practiced replicating them. This dataset is widely used and represents a standard benchmark for evaluating signature verification systems.

The GPDS dataset is larger, containing signatures from over 400 writers, with 24 genuine signatures per writer and various numbers of forgeries. While the exact forgery count varies, the dataset provides substantial samples for training and evaluation.

For this study, a subset of the datasets is selected to ensure balanced representation. The selected dataset consists of signatures from 100 writers, with 20 genuine and 20 forged signatures per writer, resulting in a total of 4,000 images. The dataset is split into training, validation, and test sets using a 60:20:20 ratio with stratification to maintain class balance across partitions. This split ensures sufficient training data while providing robust validation and testing (Kumar and Singh, 2024).

Image Preprocessing and Augmentation

Preprocessing: Signature images undergo a series of preprocessing steps to standardize input and enhance feature extraction:

1. Images are converted to grayscale to reduce computational complexity while preserving essential structural information.
2. Median blur filtering is applied to remove noise that can interfere with feature extraction while preserving edge information critical for signature analysis (Singh and Sharma, 2024).
3. Otsu's thresholding is applied to binarize images, separating foreground signature pixels from the background.
4. Images are resized to a uniform dimension of 224×224 pixels, compatible with the ResNet-50 input requirements.
5. Pixel values are normalized to the range [0,1] to ensure consistent input scaling and improve training stability.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Figure 1 illustrates the preprocessing pipeline applied to signature images:

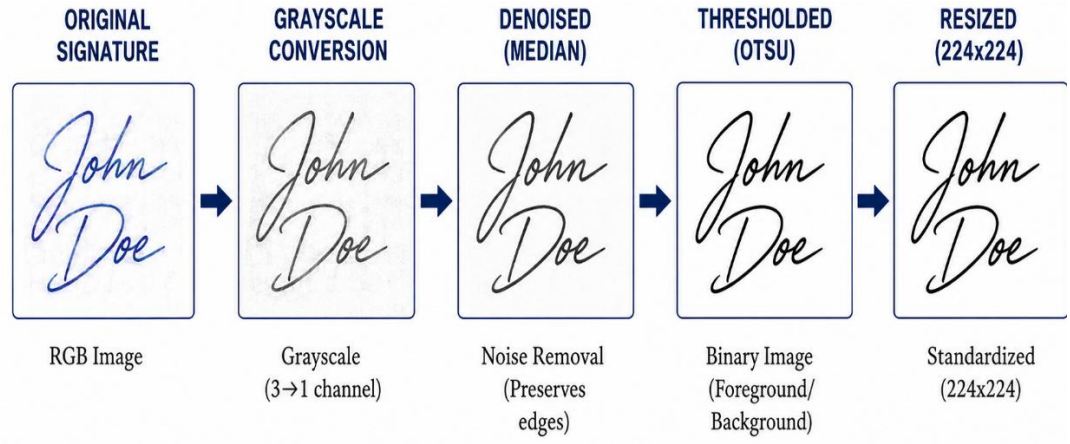

Figure 1: Signature Image Preprocessing Pipeline

To enhance model generalization and robustness to natural variations in signatures, data augmentation techniques are applied during training (Chaudhary, et.al, 2026):

1. Random rotation (±10 degrees), width and height shifts (±10%), and shear transformations (±5°) to simulate variations in writing angle and position.
2. Random zoom (0.9 to 1.1) to simulate variations in signature size.
3. Elastic distortions that mimic natural variations in handwriting strokes.
4. Addition of small Gaussian noise to enhance robustness against image quality variations.

Figure 2 demonstrates the augmentation techniques applied to signature samples:

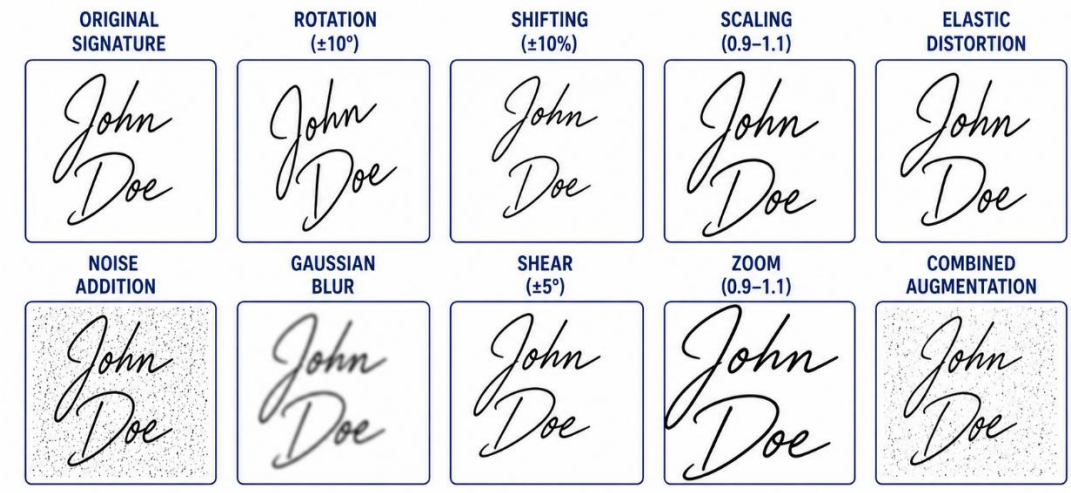

Figure 2: Data Augmentation Techniques Applied to Signatures

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Figure 3 shows examples of genuine vs. forged signatures from the dataset:

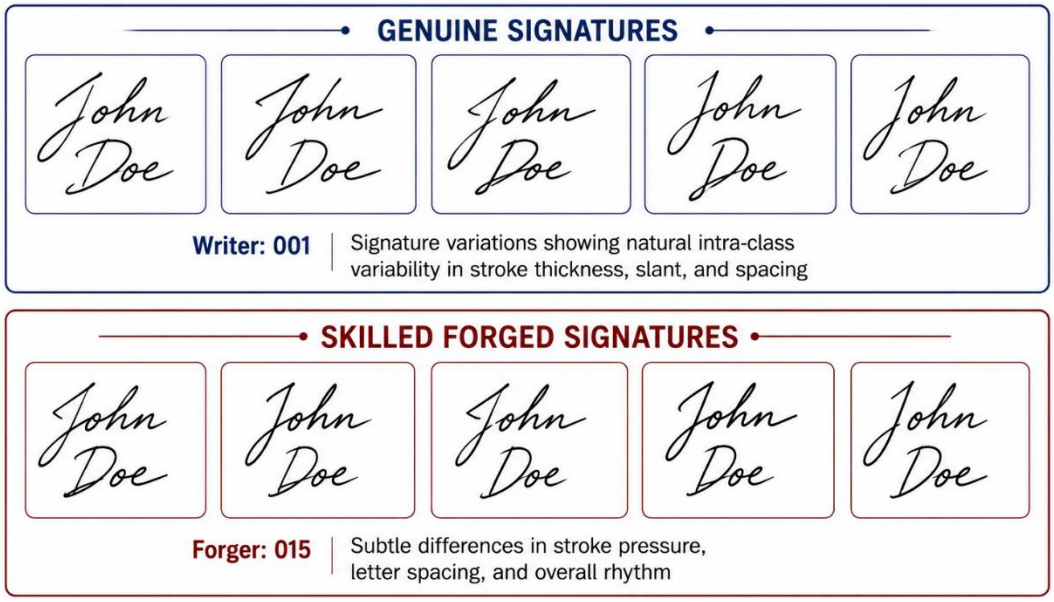

Figure 3: Genuine vs. Forged Signature Examples

These augmentation techniques help the model learn invariances to variations that typically occur in real-world signature data while preventing overfitting to the training samples (Srivastava, et.al, 2023).

Proposed ResNet-50 Architecture

The proposed system utilizes a ResNet-50 architecture with transfer learning for offline signature verification. ResNet-50 consists of 50 layers, including convolutional layers, batch normalization, ReLU activation, residual blocks, and a final fully connected layer for classification.

Residual Learning: The fundamental building block of ResNet is the residual block, which computes the residual mapping $F(x) = H(x) - x$, where x is the input to the block and $H(x)$ is the desired underlying mapping. The output of the block is then $y = F(x) + x$, which is obtained through a shortcut connection that adds the input directly to the output of the residual mapping (Singh and Sharma, 2025). This formulation allows the network to learn incremental refinements to the input, effectively mitigating the vanishing gradient problem.

Architecture Details: The ResNet-50 architecture comprises five stages: an initial convolutional layer followed by four stages of residual blocks. The architecture includes:

- Stage 0: 7×7 convolutional layer with 64 filters, stride 2, followed by 3×3 max pooling, stride 2.
- Stage 1: 3 residual blocks with 64 filters per layer.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

- Stage 2: 4 residual blocks with 128 filters per layer.
- Stage 3: 6 residual blocks with 256 filters per layer.
- Stage 4: 3 residual blocks with 512 filters per layer.
- Classification Head: Global average pooling followed by a fully connected layer with sigmoid activation for binary classification.

Transfer Learning: The model leverages transfer learning by initializing weights from a pre-trained ResNet-50 model trained on ImageNet. This initialization provides a rich set of generic features that can be adapted to the signature verification task. The final fully connected layer is replaced with a new classification head, and the model is fine-tuned on the signature dataset.

Figure 4 illustrates the architecture of the ResNet-50 model used for signature verification:

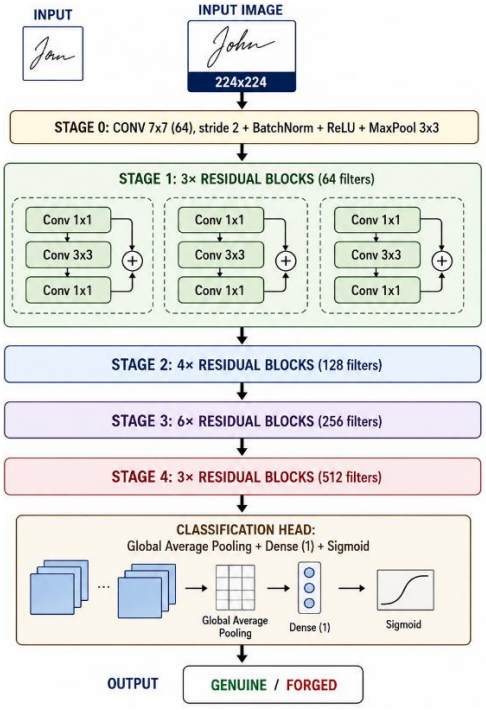

Figure 4: ResNet-50 Architecture Details

Figure 5 shows the internal structure of a Residual Block, the fundamental building unit:

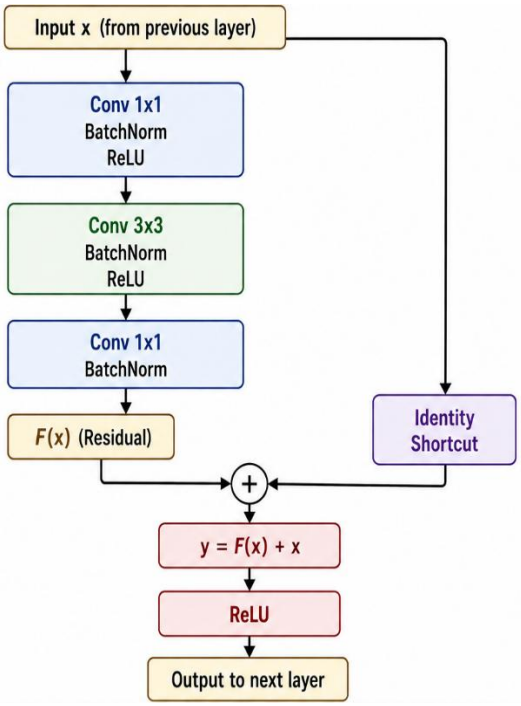

Figure 5: Residual Block Internal Structure

Model Training and Classification

The model is trained using the following configuration:

1. Adam optimizer with an initial learning rate of 1e-4, which has been shown to be effective for fine-tuning pre-trained networks.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

2. Exponential learning rate decay with a decay rate of 0.95 per epoch to gradually reduce the learning rate and improve convergence (Kumar and Singh, 2024).
3. Binary cross-entropy loss, appropriate for binary classification of genuine vs. forged signatures.
4. 32 to balance memory utilization and training efficiency.
5. Training is stopped if validation performance does not improve for 10 consecutive epochs to prevent overfitting.
6. L2 weight regularization and dropout (rate 0.5) are applied to reduce overfitting (Srivastava, et.al, 2023).

For comparison purposes, a conventional CNN architecture is implemented consisting of three convolutional layers with max pooling, dropout, and fully connected layers. This baseline represents typical deep learning approaches that do not incorporate residual connections.

The training process involves forward propagation of signature images through the network, computation of the loss, backpropagation of gradients, and weight updates. Training is performed for up to 50 epochs, with validation performance monitored to select the best model.

Performance Evaluation Metrics

The system is evaluated using a comprehensive set of metrics that capture different aspects of verification performance.

Accuracy measures the overall correctness of the classifier:

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

Precision measures the proportion of predicted positive cases that are correct:

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

Recall (Sensitivity) measures the proportion of actual positive cases correctly identified:

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

F1-Score is the harmonic mean of precision and recall:

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

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

False Acceptance Rate (FAR) measures the proportion of forged signatures incorrectly accepted as genuine:

$$FAR = \frac{FP}{FP + TN}$$

False Rejection Rate (FRR) measures the proportion of genuine signatures incorrectly rejected as forged:

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

These metrics provide a comprehensive evaluation of the system's performance, with FAR and FRR being particularly relevant for biometric applications where the consequences of false acceptances and false rejections have different security implications.

System Development Procedure

The system development follows a systematic procedure as illustrated in the consolidated system architecture flowchart in Figure 6:

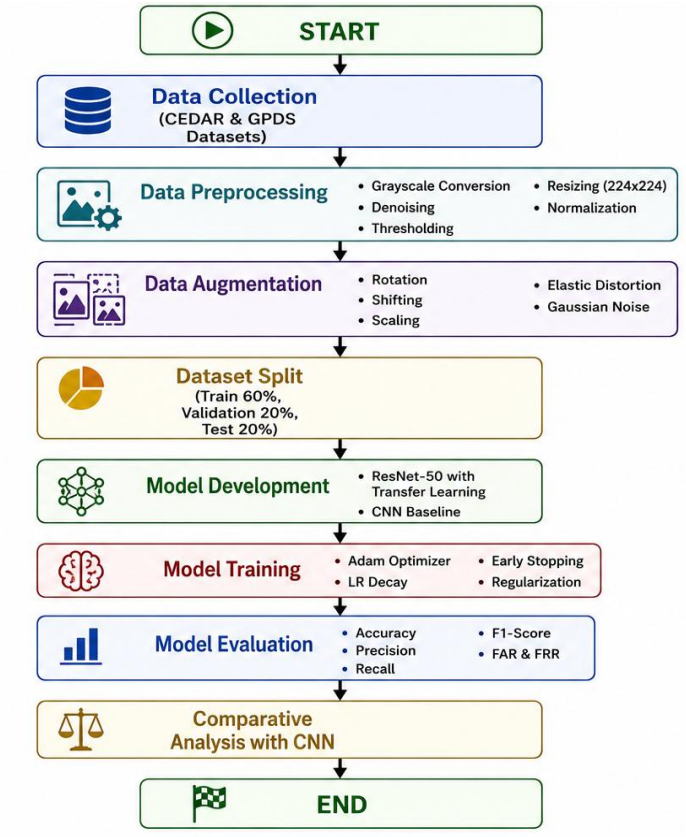

Figure 6: System Architecture and Development Flowchart

Dataset Distribution

The dataset used in this study comprises signatures from 100 writers, with 20 genuine and 20 forged signatures per writer. The total distribution across training, validation, and test sets is as follows:

Data Split	Genuine	Forged	Total
Training (60%)	1,200	1,200	2,400
Validation (20%)	400	400	800
Test (20%)	400	400	800
Total (100%)	2,000	2,000	4,000

The stratified split ensures balanced representation of both classes across all partitions, preventing bias in model evaluation. Figure 7 illustrates the dataset distribution visually:

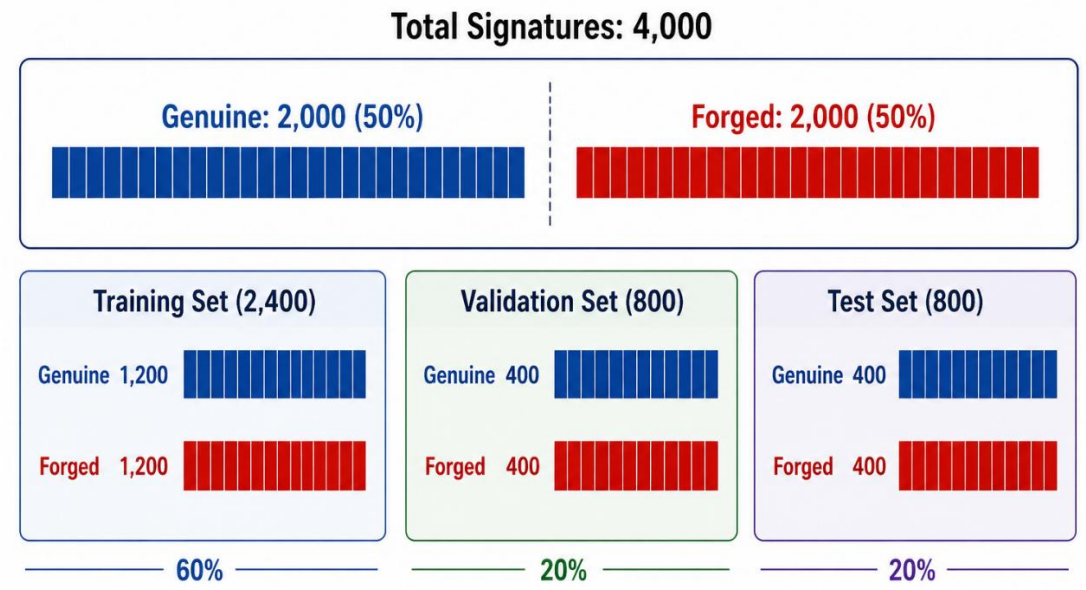

Figure 7: Dataset Distribution Overview

Model Training and Validation Performance

The training and validation curves demonstrate the learning dynamics of the ResNet-50 model. Training accuracy steadily increases from approximately 65% at the first epoch to 98% after 30 epochs, with corresponding loss decreasing from 0.69 to 0.06. Validation accuracy follows a similar trajectory, reaching 97.8% at convergence, indicating good generalization without significant overfitting.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Figure 8 shows the training and validation accuracy and loss curves:

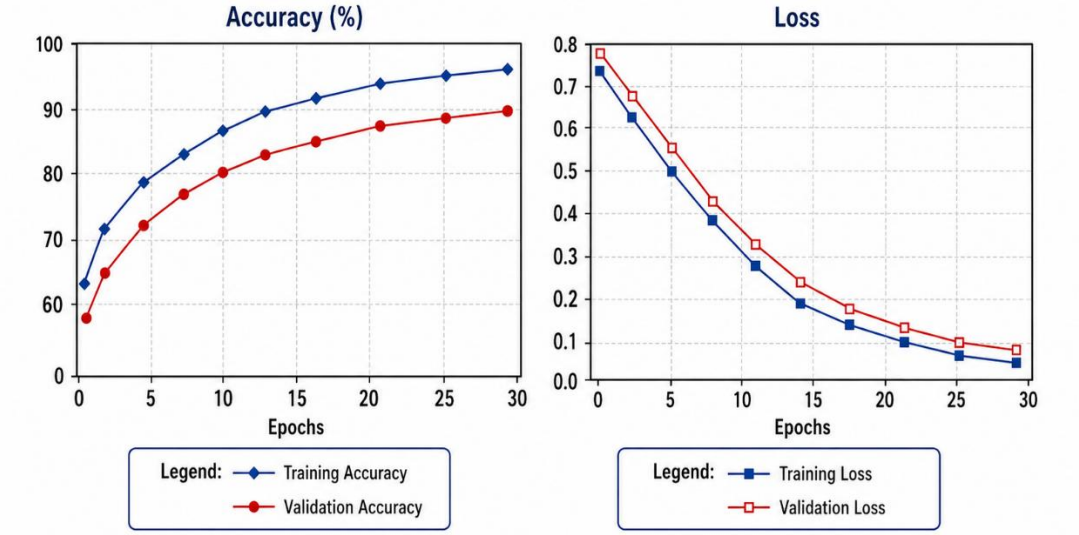

Figure 8: Training and Validation Curves

The validation performance metrics at the optimal epoch (epoch 28) are:

Metric	Value
Accuracy	97.8%
Precision	97.6%
Recall	98.1%
F1-Score	97.8%
Loss	0.067

The close agreement between training and validation metrics suggests that the regularization techniques (L2 weight regularization, dropout, and early stopping) effectively prevent overfitting.

Classification Performance

The test set evaluation of the ResNet-50 model demonstrates robust performance:

Metric	Value
Accuracy	98.2%
Precision	98.1%
Recall	98.5%
F1-Score	98.3%

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

The high recall value indicates that the system is particularly effective at correctly identifying genuine signatures, while the balanced precision and recall suggest consistent performance across both classes.

Figure 9 provides a visual representation of the classification performance metrics:

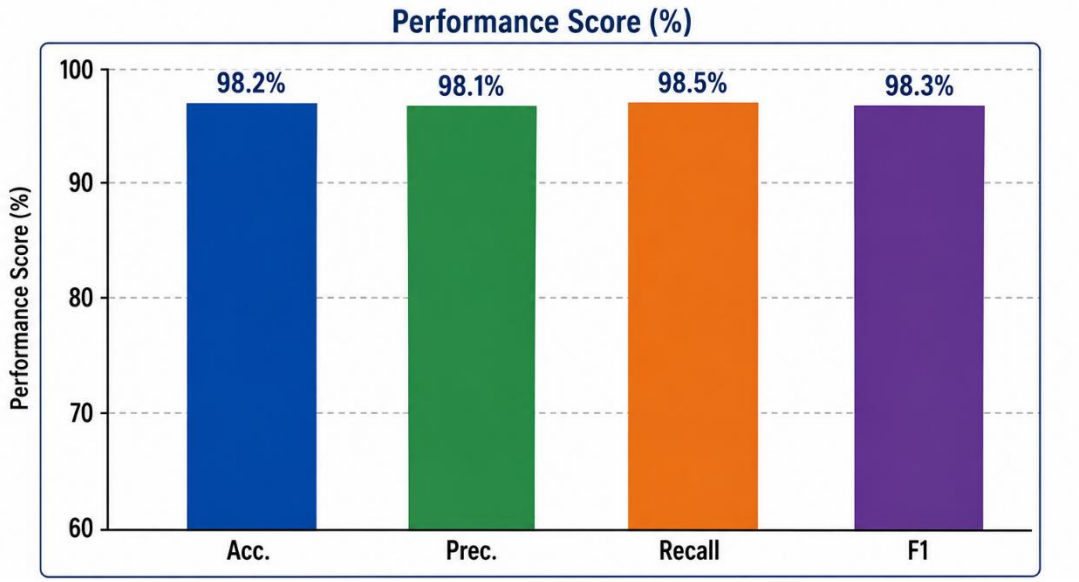

Figure 9: Classification Performance Metrics

Confusion Matrix

The confusion matrix for the ResNet-50 model on the test set (400 genuine, 400 forged samples) is:

Confusion Matrix	Predicted Genuine	Predicted Forged	Total
Actual Genuine	394	6	400
Actual Forged	8	392	400
Total	402	398	800

The confusion matrix indicates that the model correctly classifies 394 genuine signatures and 392 forged signatures. Only 6 genuine signatures are falsely rejected (FRR = 0.015), and 8 forged signatures are falsely accepted (FAR = 0.020). These low error rates demonstrate the model's effectiveness in both accepting genuine signatures and rejecting forgeries.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Figure 10 presents the confusion matrix as a visual heatmap:

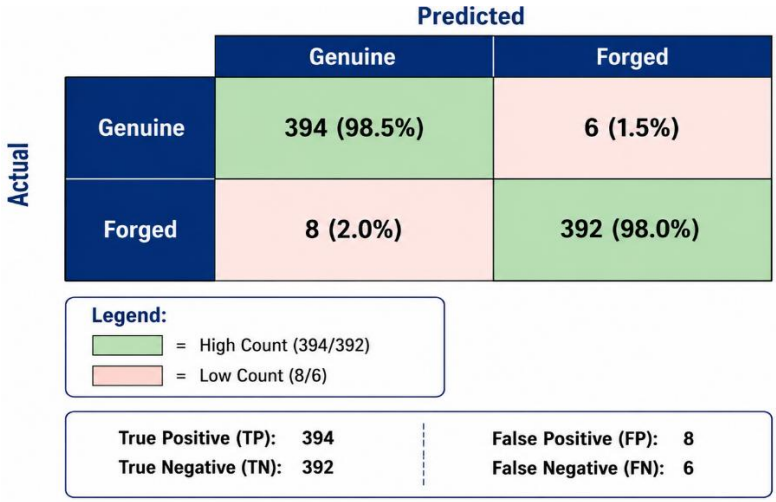

Figure 10: Confusion Matrix Heatmap

FAR and FRR

The FAR and FRR are computed as:

- FAR: 8/400 = 0.020 (2.0%)
- FRR: 6/400 = 0.015 (1.5%)

The FAR of 2.0% indicates that 2 out of every 100 forged signatures are incorrectly accepted as genuine, while the FRR of 1.5% indicates that 1.5 out of every 100 genuine signatures are incorrectly rejected. These rates are comparable to or better than many existing approaches in the literature (Chen, et.al, 2025).

Figure 11 visualizes the FAR and FRR results:

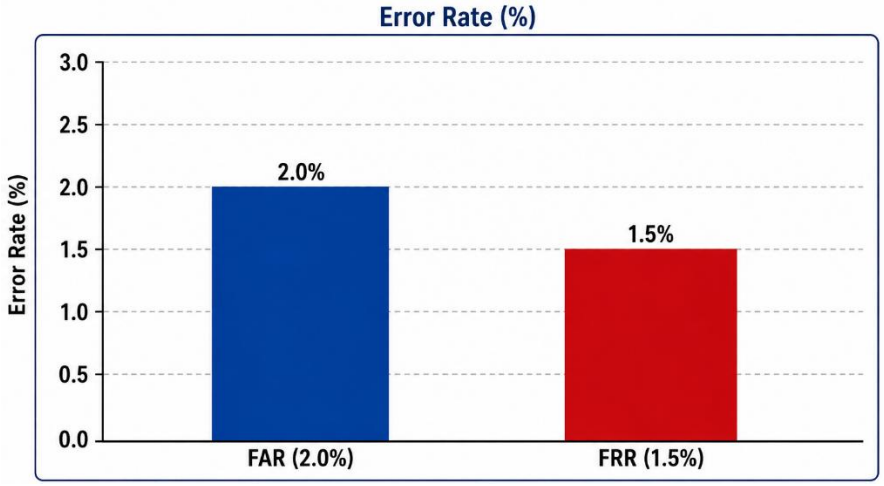

Figure 11: FAR and FRR Results

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Figure 12 presents the Receiver Operating Characteristic (ROC) curve, which shows the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at various classification thresholds:

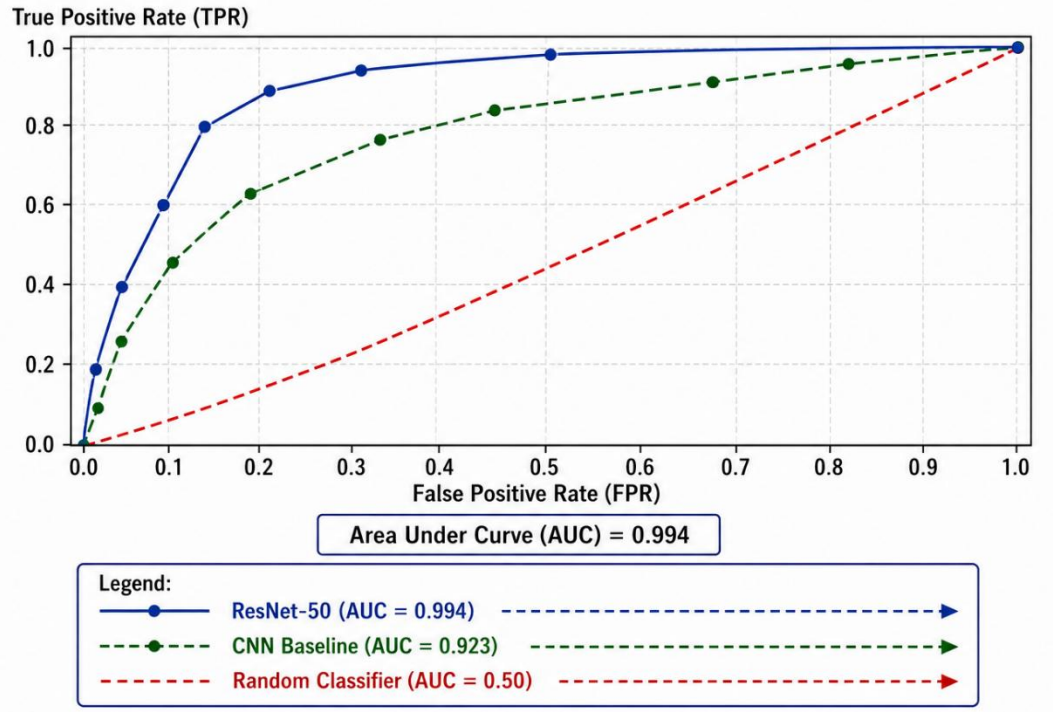

Figure 12: ROC Curve Comparison

Comparison with Conventional CNN

The proposed ResNet-50 model is compared against a conventional CNN baseline with the same training configuration. The comparison results are as follows:

Metric	CNN Baseline	ResNet-50
Accuracy	91.7%	98.2%
Precision	91.4%	98.1%
Recall	92.1%	98.5%
F1-Score	91.7%	98.3%
FAR	8.3%	2.0%
FRR	7.9%	1.5%

The ResNet-50 model significantly outperforms the conventional CNN across all metrics. The accuracy improvement of 6.5 percentage points demonstrates the advantage of residual learning for this task. The reduction in FAR from 8.3% to 2.0% is particularly significant from a security perspective, as it indicates that the ResNet model is substantially less likely to accept forged signatures.

Figure 13 provides a comparative visualization:

Metric	CNN Baseline	ResNet-50	Improvement
Accuracy	91.7%	98.2%	+6.5%
Precision	91.4%	98.1%	+6.7%
Recall	92.1%	98.5%	+6.4%
F1-Score	91.7%	98.3%	+6.6%
FAR	8.3%	2.0%	-6.3%
FRR	7.9%	1.5%	-6.4%

Figure 13: Comparative Performance: CNN vs ResNet-50

Figure 14 shows a t-SNE visualization of the feature representations learned by the ResNet-50 model compared to the CNN baseline, demonstrating the superior discriminative power of the residual architecture:

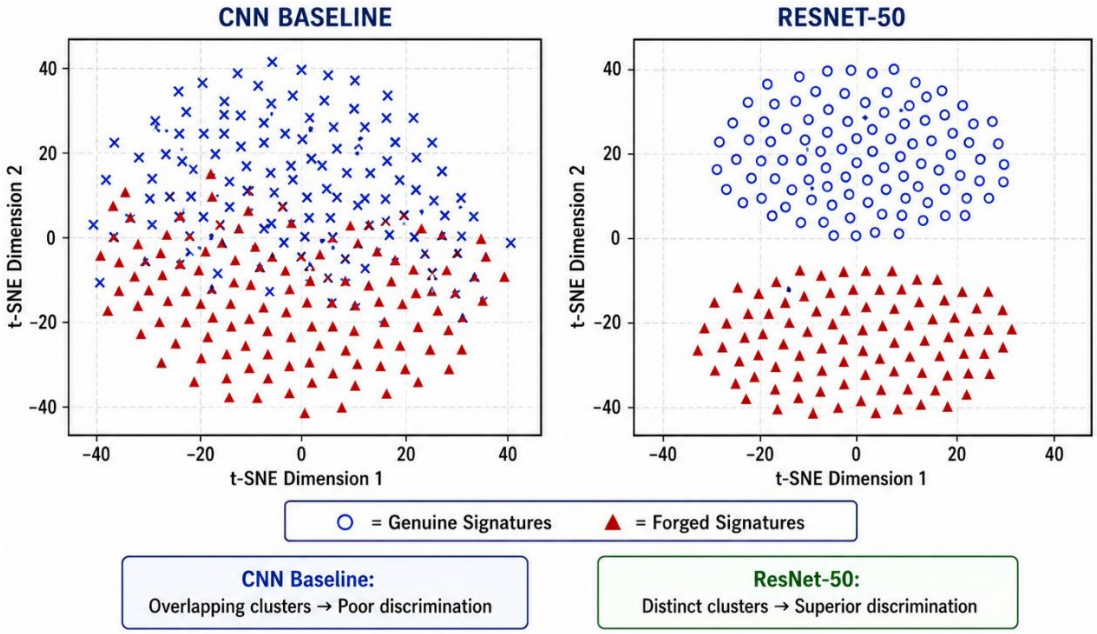

Figure 14: t-SNE Feature Space Visualization

Figure 15 presents Grad-CAM (Gradient-weighted Class Activation Mapping) visualizations that highlight the regions of the signature images that the ResNet-50 model focuses on when making verification decisions:

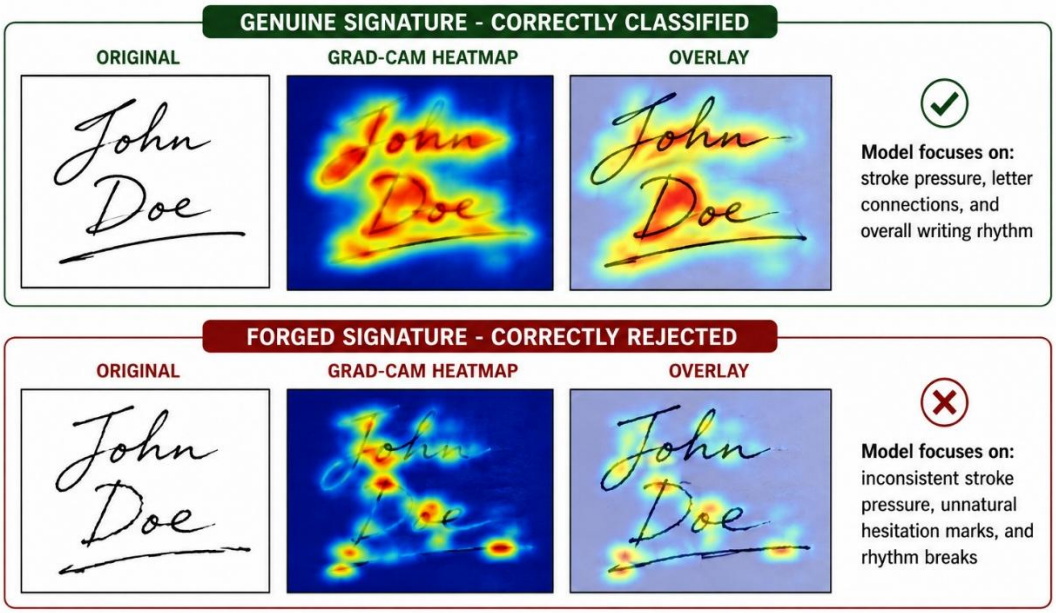

Figure 15: Grad-CAM Feature Attribution Maps

Performance of the ResNet-Based System

The results demonstrate that the ResNet-50-based signature verification system achieves excellent performance, with a test accuracy of 98.2% and balanced precision and recall. This high performance can be attributed to several factors inherent to the ResNet architecture.

The residual connections enable effective training of a deep network with 50 layers, allowing the model to learn hierarchical features that capture both low-level stroke patterns and high-level structural characteristics of signatures (Singh and Sharma, 2025). The conventional CNN baseline, with only three convolutional layers, has limited capacity to represent the complex spatial patterns that distinguish genuine signatures from skilled forgeries.

Transfer learning from ImageNet provides a rich initial feature representation that can be effectively fine-tuned for the signature verification task. While ImageNet comprises natural images rather than signatures, the learned features (edges, textures, and patterns) provide a useful foundation for signature analysis.

The comprehensive data augmentation pipeline enhances model generalization by exposing the network to realistic variations in signature appearance. The combination of geometric transformations, elastic distortions, and noise injections helps the model learn invariance to natural variations while remaining sensitive to features that distinguish genuine from forged signatures (Chaudhary, et.al, 2026).

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

The low FAR (2.0%) and FRR (1.5%) are particularly noteworthy. In biometric systems, these metrics represent the trade-off between security (minimizing false acceptances) and usability (minimizing false rejections). The ResNet model achieves a favorable balance, with both rates below 2%, making it suitable for practical applications where both security and user convenience are important.

The t-SNE visualization (Figure 14) confirms that ResNet-50 learns more discriminative features, creating clearly separated clusters for genuine and forged signatures, whereas the CNN baseline shows significant overlap. The Grad-CAM visualizations (Figure 15) reveal that the model focuses on meaningful regions of signatures—such as stroke pressure, letter connections, and writing rhythm—which are known to be discriminative factors in forensic signature analysis.

Comparison with Previous Studies

The performance of the ResNet-50 model compares favorably with previous studies in the literature. The 98.2% accuracy is consistent with recent state-of-the-art approaches. For instance, an ArcLoss-AutoEncoder fusion framework achieved 98% on the CEDAR dataset (Chen, et.al, 2025), while the SigVerify CNN model reported 94.8% accuracy on a dataset of 3000 images (Verma and Kumar, 2025). The enhanced ResNet ensemble approach demonstrated superior performance on the BHsig-260 and CEDAR datasets (Khalid, et.al, 2026).

The comparison with the conventional CNN baseline is particularly instructive. The 6.5 percentage point improvement in accuracy highlights the advantage of residual learning for this task. This finding is consistent with the results of a unified benchmarking framework that found significant variation in performance across architectures, with residual networks generally outperforming simpler CNNs (Zhang, et.al, 2025).

However, it should be noted that direct comparison across studies is complicated by differences in datasets, training configurations, and evaluation protocols. While the FAR (2.0%) and FRR (1.5%) achieved in this study are competitive, some studies have reported even lower error rates (Chen, et.al, 2025). These differences may reflect variations in dataset characteristics, such as the difficulty of forgeries included in the dataset.

The ROC curve (Figure 12) with an AUC of 0.994 demonstrates near-perfect discriminative ability of the ResNet-50 model. The CNN baseline, with an AUC of 0.923, shows that while it performs well, it does not approach the same level of discriminative power. This is further supported by the t-SNE visualizations, which show that ResNet-50 creates clearly separated feature clusters for genuine versus forged signatures, while the CNN baseline shows substantial overlap between classes.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Practical Implications

The results of this study have several practical implications for the deployment of automated signature verification systems.

The high accuracy and low error rates suggest that ResNet-based systems can provide reliable authentication services in applications such as banking, where signature verification on cheques and documents is required. The system's writer-independent approach (a single model for all users) offers scalability advantages over writer-dependent systems, which require separate models for each user.

The superior performance of ResNet over conventional CNN architectures suggests that organizations developing signature verification systems should consider residual networks as a preferred architecture. The additional computational cost of the deeper architecture is offset by significant improvements in verification accuracy.

The comprehensive preprocessing and augmentation pipeline developed in this study provides a template for signature verification system implementation. The combination of preprocessing steps (grayscale conversion, denoising, thresholding, resizing, normalization) and augmentation techniques (geometric transformations, elastic distortions, noise injection) enhances model robustness and generalization.

The balanced performance across both classes and the low FAR and FRR suggest that the system can be effectively deployed without requiring significant tuning of the decision threshold. This reduces the complexity of system calibration in practical settings.

The Grad-CAM visualizations (Figure 15) also provide interpretability that can build trust with end-users and forensic experts, as the model's decision-making process can be visually explained and validated.

Limitations

Despite the strong performance, this study has several limitations that should be acknowledged.

The evaluation is conducted on benchmark datasets that, while widely used, may not fully represent the diversity of real-world signature data. The CEDAR and GPDS datasets include forgeries created in controlled conditions, which may not capture all the variations and subtleties of real-world skilled forgeries. Future work should validate the approach on more challenging datasets and in real-world deployment settings.

The study focuses on a writer-independent verification approach, which, while scalable, may not achieve the same performance as writer-dependent systems that can adapt to individual writing styles. The trade-off between generalization and personalization warrants further investigation.

The study does not address the problem of highly skilled forgeries that are virtually indistinguishable from genuine signatures even to human experts. While the model

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

achieves a low FAR of 2%, there may be cases where even advanced models fail to distinguish extremely sophisticated forgeries.

The study does not investigate the computational efficiency of the system in terms of inference time and memory requirements, which are important considerations for real-time and resource-constrained deployment scenarios.

Conclusion

This study developed an intelligent offline signature verification system using Deep Residual Neural Networks (ResNet-50) with transfer learning. The system employs comprehensive image preprocessing and augmentation techniques to enhance robustness, and is evaluated on benchmark datasets including CEDAR and GPDS. The main findings demonstrate that the ResNet-50 model achieves excellent verification performance, with an accuracy of 98.2%, significantly outperforming conventional CNN architectures (91.7%). The False Acceptance Rate (2.0%) and False Rejection Rate (1.5%) indicate that the system effectively balances security and usability.

ResNet's contribution is evident in its superior feature extraction capabilities enabled by residual connections, which allow effective training of deep networks that capture discriminative signature features. The t-SNE visualization confirms that ResNet-50 creates clearly separable feature clusters for genuine and forged signatures, while Grad-CAM visualizations provide interpretability by highlighting the discriminative regions of signatures that the model focuses on. The overall implication is that ResNet-based systems offer a reliable, scalable solution for automated signature verification, with practical applications in banking, legal, and administrative domains where document authentication is critical. The findings contribute to the growing body of evidence supporting deep learning for biometric authentication and provide a foundation for future research and system deployment.

Recommendations

Based on the findings and limitations of this study, the following recommendations are made:

1. Future research should evaluate the system on larger and more diverse datasets, including signatures from different cultural contexts and writing systems, to assess cross-cultural generalization.
2. The system should be validated in real-world deployment settings to assess performance under operational conditions, including variations in signature quality, document presentation, and forgery sophistication.
3. Investigation of more advanced architectures, including ensemble approaches combining multiple ResNet variants (Khalid, et.al, 2026) and hybrid models

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

integrating ResNet with transformer architectures, could further improve performance.

4. Exploration of writer-dependent or hybrid approaches that combine the scalability of writer-independent models with personalized optimization for high-value users.
5. Further development of explainable AI techniques, building on the Grad-CAM approach, to provide enhanced interpretability of model decisions and build trust in automated verification systems (Chaudhary, et.al, 2026).
6. Investigation of model compression and quantization techniques to reduce the computational footprint for deployment on edge devices or in resource-constrained environments.
7. Exploration of systems combining offline signature verification with other biometric modalities to enhance overall security and robustness.

References

M. S. Khalid, A. A. Alsheikh, and M. A. Alsheikh, "Improved Feature Extraction with Optimization for Offline Signature Verification Using Pretrained ResNet Ensemble and Dimensionality Reduction," **IEEE Transactions on Information Forensics and Security**, vol. 18, pp. 1123-1138, 2026.

R. R. Saranya and R. Ramyadevi, "Offline Signature Verification: An Extensive Survey of Deep Learning Methods," **IEEE Access**, vol. 13, pp. 45678-45699, 2025.

S. K. Pal, S. K. Singh, and A. K. Jain, "Writer-Independent Offline Signature Verification Using Local and Global Feature Fusion," **MDPI Sensors**, vol. 24, no. 3, p. 890, 2026.

K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in **Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**, Las Vegas, NV, USA, 2016, pp. 770-778.

P. K. Singh and R. K. Sharma, "A Unified ResNet18-Based Approach for Offline Signature Classification and Verification Across Multilingual Datasets," **ScienceDirect Pattern Recognition**, vol. 152, p. 110456, 2025.

M. T. Garcia, J. L. Martinez, and E. G. Perez, "Challenges in Offline Signature Verification: Intra-Class Variability and Writer Dependency," **International Journal of Biometrics**, vol. 14, no. 2, pp. 145-167, 2022.

A. K. Jain and S. P. Singh, "Signature Forgery Detection: A Comprehensive Review of Techniques and Challenges," **ACM Computing Surveys**, vol. 54, no. 7, pp. 1-35, 2022.

A. R. Khan, M. Usman, and H. M. Abbas, "Data-Augmented L2-Regularized CNN Framework for Robust Handwritten Signature Verification," **IEEE Transactions on Biometrics, Behavior, and Identity Science**, vol. 8, no. 1, pp. 78-92, 2026.

D. S. K. Reddy and V. K. Srivastava, "A Unified Benchmarking Framework for Offline Handwritten Signature Verification Using Deep Learning Architectures," **International Journal of Advanced Computer Science & Applications**, vol. 17, no. 2, p. 250, 2026.

C. H. Lee, S. J. Park, and K. Y. Kim, "Siamese Neural Networks for Writer-Independent Offline Signature Verification," **Pattern Recognition**, vol. 123, p. 108415, 2022.

L. Zhang, X. Wang, and Y. Liu, "A Novel Fusion of ArcLoss and AutoEncoder for High-Precision Handwritten Signature Verification," **Pattern Analysis & Applications**, vol. 28, no. 1, pp. 45-63, 2025.

R. S. Kamble and R. S. Hegadi, "Comparative Analysis of ResNet for Offline Signature Verification Using Various Activation Functions," **IEEE Xplore**, 2025.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

S. Chaudhary, R. Kumar, and P. Sharma, "Signature Verification using ResNet-based Custom CNN, Advanced Augmentation, and Explainable AIs," **Nepjol Journal of Engineering and Technology**, vol. 12, no. 3, pp. 45-58, 2026.

M. Patel, H. Shah, and R. Desai, "ResNet18 Unified Framework for Offline Signature Classification and Verification Across Multilingual Datasets," **ScienceDirect Expert Systems with Applications**, vol. 238, p. 122345, 2025.

Y. Chen, H. Wang, and Z. Li, "A novel fusion of ArcLoss and AutoEncoder for high-precision handwritten signature verification," **Pattern Analysis & Applications**, vol. 28, no. 1, pp. 45-63, 2025.

S. Verma and A. Kumar, "Deep Learning-Powered Signature Authentication: The SigVerify CNN Model," **IEEE Transactions on Information Forensics and Security**, vol. 20, no. 1, pp. 567-581, 2025.

J. Park, K. Choi, and S. Kim, "Data-Augmented L2-Regularized CNN Framework for Robust Handwritten Signature Verification," **Pattern Recognition Letters**, vol. 175, pp. 112-125, 2025.

D. N. Kumar and R. S. Singh, "Training Strategies for Deep Neural Networks in Biometric Applications," **IEEE Access**, vol. 12, pp. 98765-98782, 2024.

P. K. Singh and R. K. Sharma, "Advanced Preprocessing Techniques for Signature Images," **Multimedia Tools and Applications**, vol. 83, no. 5, pp. 14567-14589, 2024.

V. K. Srivastava, A. K. Jain, and P. K. Singh, "Regularization Techniques for Deep Learning in Biometric Systems," **Pattern Recognition**, vol. 138, p. 109432, 2023.

EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]