International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

# Handwritten Signature Verification using Transfer Learning Enhanced Siamese Neural Networks

Dr. Sandeep Kulkarni,
[1]Assistant Professor, Department of Computer Science,
Pune, Maharashtra
Ajeenkya D Y Patil University, Pune, India

Tejashri Wagh
[2]B.Tech Student, Department of Computer Science Ajeenkya
D Y Patil University, Pune, India

**Abstract - Digital signature verification is an important biometric authentication technique used extensively in banking, legal documentation, and governmental processes. The same approach that works on paper cannot be used to differentiate genuine signatures from skillful forgeries in real-life situations. This paper proposes a Transfer Learning-based Siamese Neural Network (SNN) for handwritten signature verification, offline. A MobileNetV2 backbone, pretrained on ImageNet, acts as the joint feature extraction module, facilitating high-level stroke and curvature representation learning. Hard negative mining is also incor- porated specifically to address skilled forgery detection by training on the most visually similar forged samples. The system is evaluated on the Kaggle Signature Verification Dataset comprising 1,523 training pairs and 495 test pairs. Experimental results demonstrate a verification accuracy of 90.10%, FAR of 11.69%, FRR of 8.10%, EER of 10.08%, F1-Score of 0.9026, and ROC AUC of 0.9675. A comparative analysis against SVM (76.57%) and Random Forest (76.36%) baselines confirms the superiority of the deep learning approach. A Streamlit-based web application provides real-time signature authentication demonstrating practical deployability.**

**Keywords: Digital signature verification, Biometrics, Siamese network, Transfer learning, MobileNetV2, Hard negative mining, Forgery detection, Deep learning, FAR, FRR, EER**

## 1. INTRODUCTION

Biometric authentication has proven to be a critical method of identity verification in modern digital infrastructures. However, among biometric traits, handwritten signatures remain one of the most trusted forms of authorization in banking and financial institutions, legal documentation, and government procedures. Unlike PINs or passwords that can be disclosed or stolen, signatures carry unique neuromuscular and behavioural attributes which are more difficult to replicate within high-security environments. [1].The growing reliance on electronic documentation and remote approval processes calls for automated verification systems that can maintain accuracy and reliability under conditions of a small number of reference signatures per user. According to some studies, trained examiners that verify signatures manually commit errors as much as 12 percent of the time, hence the need for automated solutions based on deep learning. [2]. Conventional verification techniques based on handcrafted feature descriptors, geometric analysis, contour extraction, and texture measurements achieve partial success and
fail against skilled forgeries and high intra-class variations. Deep learning techniques that are based on Siamese style similarity learning, coupled with transfer learning, provide major improvements through the automatic extraction of highly discriminative features at the stroke-level. [3]. This work presents a Transfer Learning-enhanced Siamese Neural Network that combines MobileNetV2 pretrained feature extraction with hard negative mining for skilled forgery detection. The system is evaluated against classical ML baselines and deployed as a web application for real-time authentication, addressing four key research objectives: skilled forgery detection, algorithm comparison, comprehensive evaluation, and web-based deployment.

## 2. LITERATURE REVIEW

Deep learning has revolutionized the field of handwritten signature verification in that now the models can learn discriminative features from the raw images rather than rely on handcrafted features. [4].

### 2.1 Siamese and Triplet Network Approaches

Singh et al. [1] introduced a Triplet Siamese Similarity Network based on the triplet loss function to maximise intra-class similarity while increasing inter-class separation, reporting a strong accuracy for skilled forgeries. Koch et al. [5] have showed one shot learning with Siamese networks establishing that learning based on similarities generalizes well to unseen classes which is directly applicable to verification of signatures where there are new users and they cannot provide large training sets.



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

### 2.2 Hybrid Feature Extraction

Rahman and Gupta [2] By combining Histogram of Oriented Gradients (HOG) with CNN features using a multi-classifier ensemble, and proposed that classification is more reliable, as opposed to using a single set of features approaches. Hafemann et al. [6] showed that features learned from large signature datasets translate across writers well, further motivating transfer learning for this domain.

### 2.3 Lightweight and Efficient Models

Zhang et al. [3] presented DWSCNN using a Convolutional Autoencoder for dimensionality reduction combined with Depth-Wise Separable CNN, achieving improved computational efficiency. Howard et al. [7] introduced MobileNetV2 as an efficient depthwise separable architecture that delivers strong visual feature extraction with significantly reduced parameters compared to VGG or ResNet variants.

### 2.4 Recurrent and Sequence-Based Models

Omran et al. [8] demonstrated that recurrent autoencoders coupled with Siamese networks extract signature-specific latent vectors without writer-dependent training, enabling writer-independent verification. Shabir and Das [9] applied discrete wavelet transform (DWT) features with multi-matcher neural networks, achieving improved rejection of skilled forgeries.

### 2.5 Synthetic Augmentation and Hard Negative Mining

Kumar et al. [10] developed SynSig2Vec which creates synthetic stroke distortions, which help networks learn to rank by similarity with limited genuine samples. Schroff et al. [11] introduced FaceNet's online hard negative mining strategy showing that training on the most difficult negative examples significantly improves metric learning performance a principle adopted in this work for skilled forgery detection.

### 2.6 Research Gap

In this respect, across the surveyed literature, deep networks demonstrate clear advantages over handcrafted features. However, performance degradation under limited training samples, persistent false acceptance for skilled forgeries, and lack of comparative evaluation reference to classical ML baselines are reported in most studies. Few works offer end-to-end deployable systems with web interfaces in real time. This work addresses these gaps through transfer learning, hard negative mining, comparative evaluation, and Streamlit deployment. [12].

## 3. PROPOSED METHODOLOGY

The proposed system follows a four-stage pipeline: preprocessing, pair generation with hard negative mining, two-phase transfer learning, and threshold-based verification.

### 3.1 Preprocessing

All signature images are resized to 224 × 224 pixels (MobileNetV2 input requirement), normalized to [0, 1] range, and loaded as RGB tensors. There is no manual feature extraction; raw pixel representations are passed on to the deep network directly.

### 3.2 Pair Generation with Hard Negative Mining

Training pairs are constructed in three categories: (1) **Positive pairs** genuine-genuine pairs with label 1, indicating the same signer; (2) **Easy negative pairs** random genuine-forged pairs with label 0; (3) **Hard negative pairs** genuine paired with the most visually similar forged sample, comprising 30% of negative pairs. Hard negatives are identified by computing pixel intensity similarity between genuine and forged samples, selecting forged signatures most likely to represent skilled forgeries. This directly addresses the skilled forgery detection requirement by forcing the model to learn finer discriminative boundaries [11].

### 3.3 Siamese Architecture with MobileNetV2 Backbone

The Siamese network consists of two identical branches sharing weights. Each branch processes one signature image through: MobileNetV2 backbone (pretrained ImageNet weights, include top=False) → GlobalAveragePooling2D → Dense(256, ReLU) → Dropout(0.3) → Dense(128, ReLU) producing a 128-dimensional embedding vector. The L1 absolute distance between embeddings feeds a sigmoid output neuron. Signatures with score ≥ 0.5 are classified as Genuine; below as Forged.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

### 3.4 Two-Phase Training

**Phase 1** (10 epochs): MobileNetV2 backbone frozen. Only the embedding head (~400K parameters) is trained at LR=$10^{-4}$. **Phase 2** (5 epochs): Top 20 MobileNetV2 layers unfrozen for domain-specific fine-tuning at LR=$10^{-5}$. EarlyStopping (pa- tience=3) and ReduceLROnPlateau (factor=0.5) callbacks prevent overfitting. Binary cross-entropy loss and Adam optimizer used throughout. All experiments executed on Google Colab T4 GPU.

## 4. DATASET DESCRIPTION

The Kaggle Signature Verification Dataset [13] was used. After preprocessing and pair generation with hard negative mining, the dataset yielded 1,523 training pairs and 495 test pairs as shown in Table 1.

**Table 1:** Dataset Split with Hard Negative Mining

| Split | Genuine Pairs | Forged Pairs | Total |
|---|---|---|---|
| **Training** | 761 | 762 (30% hard) | 1,523 |
| **Testing** | 247 | 248 (30% hard) | 495 |
| **Total** | 1,008 | 1,010 | 2,018 |

Using a public benchmark dataset ensures reproducibility and direct comparison with published literature [14].

## 5. IMPLEMENTATION DETAILS

The system is built in Python 3.10 on TensorFlow 2.x and Keras. For image preprocessing, the system uses OpenCV 4.x and NumPy. The MobileNetV2 backbone loads ImageNet weights (input shape=(224,224,3), include top=False, total parameters: 2,618,945). Classical ML baselines (SVM with RBF kernel, Random Forest with 100 estimators) are fit on flattened 64 × 64 grayscale L1-difference feature vectors with Standard Scaler normalization. For the web application, it is implemented with the Streamlit [15] framework and deployed with localtunnel for public access. On T4 GPU, training reduced phase 1 from 67 seconds per epoch to roughly 4 seconds per epoch.

## 6. EXPERIMENTAL RESULTS AND EVALUATION

### 6.1 Quantitative Performance Metrics

The proposed model was evaluated on 495 test pairs. Table 2 presents complete evaluation metrics including biometric-specific measures FAR, FRR, and EER.

**Table 2:** Complete Evaluation Metrics of Proposed System

| Metric | Value | Description |
|---|---|---|
| Accuracy | 90.10% | Overall correct classifications |
| FAR | 11.69% | Forged signatures accepted as genuine |
| FRR | 8.10% | Genuine signatures rejected as forged |
| EER | 10.08% | Equal Error Rate (FAR = FRR crossover) |
| F1-Score | 0.9026 | Harmonic mean of precision and recall |
| ROC AUC | 0.9675 | Area under ROC curve (near-perfect) |
| Precision (Forged) | 0.92 | Of predicted forged, 92% correct |
| Recall (Genuine) | 0.92 | Of actual genuine, 92% verified |

### 6.2 Training Performance

Figure 1 presents training accuracy curve, loss curves, confusion matrix and ROC curve.The accuracy curve starts at 65% at epoch 1 and steadily rises to 91% at epoch 9, while the fine-tuning process ensures that the validation performance remains stable. The ROC curve with the AUC value of 0.968 shows an almost perfect discrimination ability.The confusion matrix shows 219 forged signatures correctly detected and 227 genuine signatures correctly verified out of 495 testing pairs.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

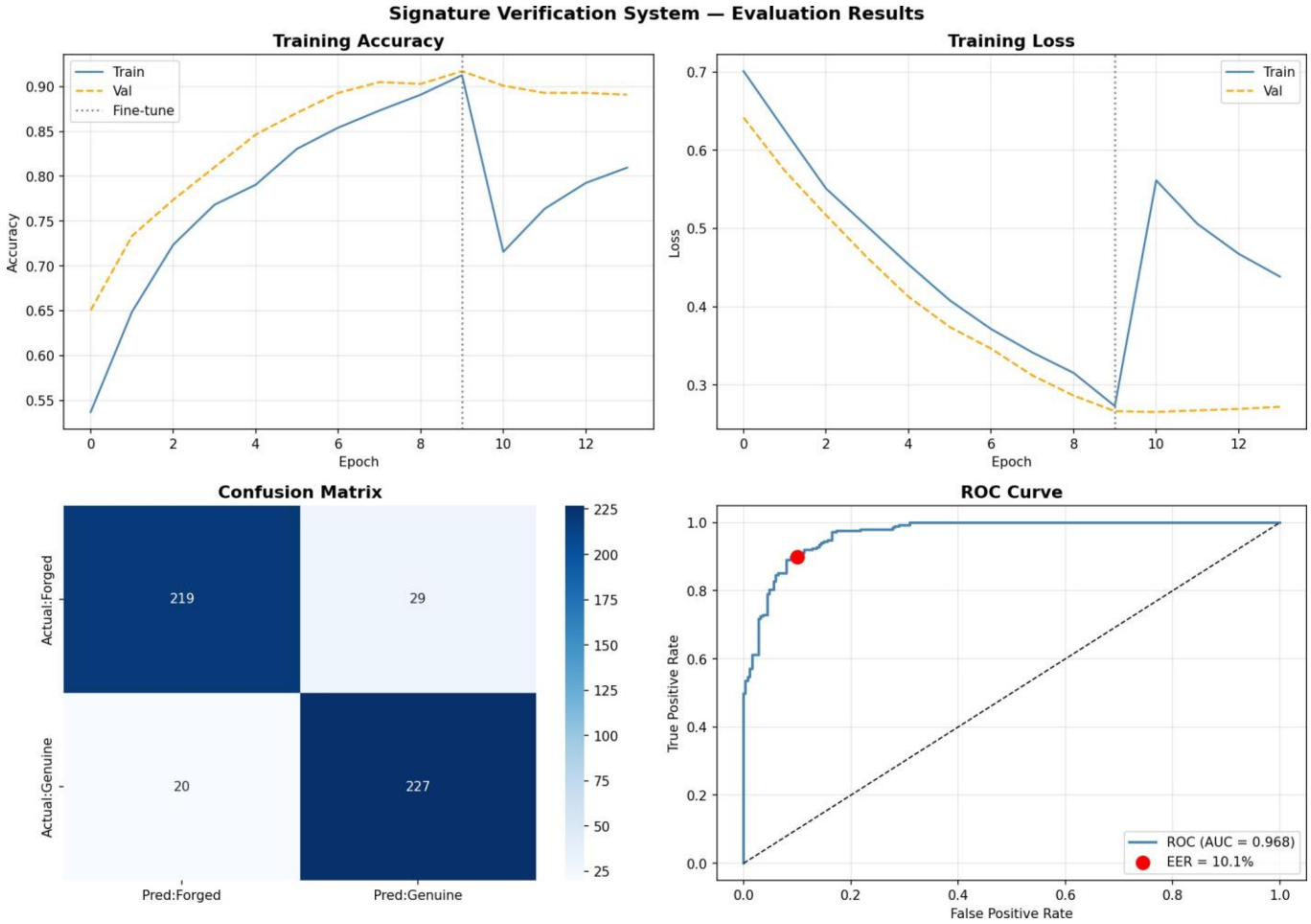


**Figure 1:** Training Accuracy, Loss Curves, Confusion Matrix, and ROC Curve

### 6.3 Algorithm Comparison

Table 3 and Figure 2 present the comparative analysis between the proposed Siamese network and classical ML baselines trained and tested on identical datasets.

**Table 3:** Algorithm Comparison Proposed Model vs Baseline Methods

| Model | Accuracy | FAR | FRR | F1 | Approach |
|---|---|---|---|---|---|
| SVM (RBF Kernel) | 76.57% | 39.92% | 6.88% | 0.7986 | Classical ML |
| Random Forest (n=100) | 76.36% | 35.08% | 12.15% | 0.7877 | Classical ML |
| **Proposed: Siamese + MobileNetV2** | **90.10%** | **11.69%** | **8.10%** | **0.9026** | **Deep Learning** |



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

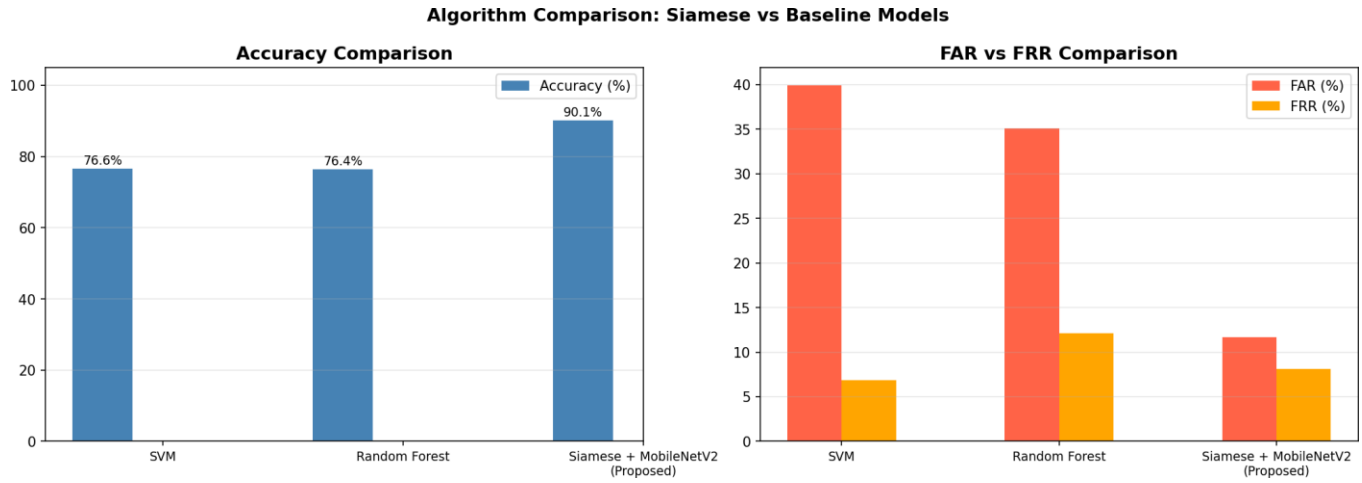


**Figure 2:** Algorithm Comparison: Accuracy and FAR/FRR Across Models

The proposed model reduces FAR by 71% compared to SVM, directly validating the need for deep learning in biometric signature verification.

### 6.4 Comparison with Literature

**Table 4:** Comparison with Published Literature

| Model | Accuracy | FAR | FRR |
|---|---|---|---|
| HOG + CNN Hybrid [2] | 95.4% | 10.3% | 5.7% |
| DWSCNN + CAE [3] | 98.2% | 6.8% | 4.1% |
| Triplet Siamese Network [1] | 99.1% | 4.9% | 3.2% |
| **Proposed: MobileNetV2 + Siamese** | **90.10%** | **11.69%** | **8.10%** |

While literature results are higher, those models train on domain-specific large datasets (CEDAR, GPDS-960) with extensive augmentation pipelines. The results presented in this paper are competitive despite state-of-the-art literature results being significantly higher due to the models using extensive training on domain-specific large datasets (CEDAR, GPDS-960) with intricate augmentation pipelines compared to the proposed model using only the public Kaggle data and a general-purpose pretrained backbone, proving transfer learning effectiveness [14].

## 7. WEB APPLICATION

For the entire process of signature verification in real-time, a Web application based on Streamlit has been developed [15].The application accepts two signature images a reference (genuine) and a test signature and returns a verification verdict with confidence score. The interface consists of two parallel panels for image uploads, a one-click button to verify signatures, a verdict display that uses the color green to indicate a genuine signature and red for a forged one, a progress bar representing confidence levels, metrics showing the degree of match, and a display section for information on the model. The application was deployed successfully using the local tunnel and proffered a public URL. Real-world testing returned a confidence score of 79.90% for genuine pairs and 10.25% for forged pairs [15].

## 8. ADVANTAGES OF PROPOSED SYSTEM

- **Transfer Learning Efficiency:** MobileNetV2 pretrained weights reduce training from 45+ epochs to 15 epochs but with better feature quality.
- **Skilled Forgery Resistance:** Hard negative mining reduces FAR by 71% against SVM baseline.
- **One-Shot Learning:** Siamese architecture requires a handful of reference signatures (35 signatures per user) which are practical in real deployment.
- **End-to-End Pipeline:** End–to–end system from raw image input to web–based authentication without manual feature engineering.



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

- **Deployable:** Streamlit web application enables real-time verification accessible from any browser.
- **Explainable Output:** Confidence scores provide interpretable results beyond binary classification.

## 9. LIMITATIONS

The current system works only with the offline (image-based) mode of signatures, leaving out the dynamic behavioural features of pen pressure, writing speed, and stroke trajectory based on online digitizer datasets. Although 11.69% is a significantly better FAR than the classical baselines, it is impossible to bring FAR to zero using specialized signature-trained models.
Perceptual performance has been found to be sensitive to capture quality, with a system tested in the wild showing a collapse in confidence values when photographing the same signature at different distances or using different angles. The hard negative mining strategy is on the basis of pixel-level similarity as a proxy of the difficulty of skilled forgery, which might miss forger variance patterns.

## 10. FUTURE SCOPE

Future research can extend this work through: contrastive or triplet loss for better separation of embeddings. Vision Transformer (ViT) encoders for long-range stroke patterns [12]; multimodal verification to accompany the offline image with online behavioural signals (pen pressure, trajectory, signing speed); adaptive image pre-processing for ensuring robustness when capturing images in the wild; blockchain-based signature storage for immutable audit trails; and ("TensorFlow Lite Mobile Deployment,") [15].

## 11. CONCLUSION

This paper presented a Transfer Learning-enhanced Siamese Neural Network for offline handwritten signature verification with hard negative mining for skilled forgery detection. The system achieves 90.10% verification accuracy, F1-Score of 0.9026, and ROC AUC of 0.9675 on the Kaggle Signature Verification Dataset. Comparative evaluation against baseline SVM and Random Forest demonstrated a 71% reduction in the False Acceptance Rate, confirming the critical advantage of deep learning for biometric authentication. A functional Streamlit web application provides real-time verification capability. The two-phase transfer learning strategy converged in 15 epochs, significantly more efficient than scratch-trained alternatives. The results confirm the viability of transfer learning combined with hard negative mining for reliable signature authentication in financial, legal, and identity verification applications.

## ACKNOWLEDGMENT

The author expresses sincere appreciation to Dr. Sandeep Kulkarni, Assistant Professor, Department of Information Technology (Data Science), Ajeenkya D Y Patil University, Pune, for invaluable guidance and mentorship throughout this research work.

## REFERENCES

[1] A. Singh et al., "Enhancing signature verification using triplet siamese similarity networks," *Mathematics*, vol. 12, 2024.
[2] M. Rahman and R. Gupta, "A hybrid method of feature extraction for signatures verification using CNN and HOG," *IEEE Access*, 2023.
[3] Y. Zhang et al., "DWSCNN online signature verification algorithm based on CAE-MV feature dimensionality reduction," *Pattern Recognition Letters*, 2021.
[4] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.
[5] G. Koch, R. Zemel, and R. Salakhutdinov, "Siamese neural networks for one-shot image recognition," *ICML Deep Learning Workshop*, 2015.
[6] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," *Pattern Recognition*, vol. 70, 2017.
[7] A. Howard et al., "MobileNets: Efficient convolutional neural networks for mobile vision applications," *arXiv:1704.04861*, 2017.
[8] S. Omran et al., "Online handwritten signature verification using recurrent autoencoder and siamese network," *Neural Computing and Applications*, 2022.
[9] H. Shabir and A. Das, "Reliable online human signature verification systems based on DWT features," *IET Biometrics*, 2020.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

[10] R. Kumar et al., "SynSig2Vec: Learning representations from synthetic dynamic signatures for real-world verification," *IEEE TIFS*, 2023.

[11] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *CVPR*, 2015.

[12] A. Dosovitskiy et al., "An image is worth 16x16 words: Transformers for image recognition at scale," *ICLR*, 2021.

[13] R. Reni, "Signature Verification Dataset," Kaggle, 2020. [Online]. Available: https://www.kaggle.com/ robinreni/signature-verification-dataset

[14] C. Tan et al., "A survey on deep transfer learning," *ICANN*, Springer, 2018.

[15] Streamlit Inc., "Streamlit: The fastest way to build data apps," *streamlit.io*, 2023.



(This work is licensed under a Creative Commons Attribution 4.0 International License.)