Journal of Engineering Issues and Solutions

Advancing Offline Signature Verification with Bidirectional Siamese Deep Learning: A Writer-Independent Approach

Surendra Basnet[1]*, Deeyo Ranjan Dongol[2], Surendra Shrestha[3]*

[1]Himalayan Institute of Science and Technology, Gwarko, Lalitpur, Nepal,
[1]Nepal Bank Limited, Dharmapath, Kathmandu, Nepal
[2]Aspire College, Biratnagar, Nepal
[3] Faculty of Science, Health and Technology, Nepal Open University, Lalitpur, Nepal, [3]Department of Electronics and Computer Engineering, Pulchowk Campus, IOE, TU, Lalitpur, Nepal
**Corresponding email: surendra.basnet@nepalbank.com.np, surendra@ioe.edu.np*
Submitted: April 13, 2025; Revised: June 15, 2025; Accepted: June 21, 2025

https://doi.org/10.3126/joeis.v4i1.81613

Abstract

Offline handwritten signature verification is critical for secure authentication in legal, financial, and administrative domains. Traditional systems struggle with intra-user variability and skilled forgeries, while writer-dependent approaches lack scalability. Unlike digital data validation, verifying physical signatures is a complex task due to variations in writing styles, intra-writer inconsistency, and skilled forgery attempts. This research introduces a writer-independent deep learning approach using a Bidirectional Recurrent Convolutional Siamese Network (BRCSN) to address these challenges. The proposed model combines convolutional neural networks (CNNs) to extract spatial features and bidirectional gated recurrent units (Bi-GRUs) to learn sequential stroke patterns, allowing the system to capture both local and global dependencies from static signature images. A triplet loss function is employed to optimize the network by minimizing the distance between genuine signature pairs and maximizing the distance between forged ones in the embedding space. The system is evaluated on benchmark multi-lingual signature datasets and achieves high classification accuracy, recall, and F1-score, while maintaining low false acceptance and rejection rates. Importantly, the BRCSN model performs consistently across diverse users without requiring writer-specific training, making it well-suited for real-time deployment in legal, financial, and administrative applications. Inference time is kept under 100 milliseconds, supporting practical use cases. By eliminating the need for retraining and leveraging spatial-temporal learning through BRCSN, this research contributes to the advancement of secure and scalable biometric systems capable of robust forgery detection.

Keywords: Offline Signature Verification, Writer-Independent Systems, Siamese Networks, Deep Learning, Forgery Detection

1. Introduction

Handwritten signatures continue to be a trusted and legally recognized method for personal authentication in banking, legal, and administrative sectors (Srihari et al., 2002). While the rise of digital transformation has introduced technologies such as digital signatures and biometric methods like facial or fingerprint recognition, paper-based signature verification remains necessary in many real-world scenarios, especially in regions lacking digital infrastructure.

However, unlike digital signature verification, offline (paper-based) handwritten signature verification is inherently more complex. This complexity arises due to intra-writer variability, inter-writer similarity, and the increasing prevalence of skilled forgeries (Chen & Zhang, 2020; Justino et al., 2001). Manual signature verification methods are time-consuming, error-prone, and difficult to scale (Dhillon & Bhatti, 2021).

Recent advances in machine learning and deep learning have enabled the development of automated signature verification systems. Traditional writer-dependent systems require retraining for every user, making them unsuitable for scalable deployment. Hence, there is growing interest in writer-independent systems capable of generalizing across unseen users (Patel & Thakur, 2019).

The Bidirectional Recurrent Convolutional Siamese Network (BRCSN) research introduces a deep learning framework for offline, writer-independent signature verification. The model captures both spatial and sequential features from static signature images and learns a discriminative embedding space using triplet loss (Singh et al., 2022; González-González et al., 2018).

2. Methodology

Offline signature verification systems typically comprise four key stages: image acquisition, preprocessing, feature extraction, and verification. In this research, a Bidirectional Recurrent Convolutional Siamese Network (BRCSN) is employed to enhance accuracy, generalization, and robustness. A high-level overview of the proposed system workflow is presented in Figure 1.

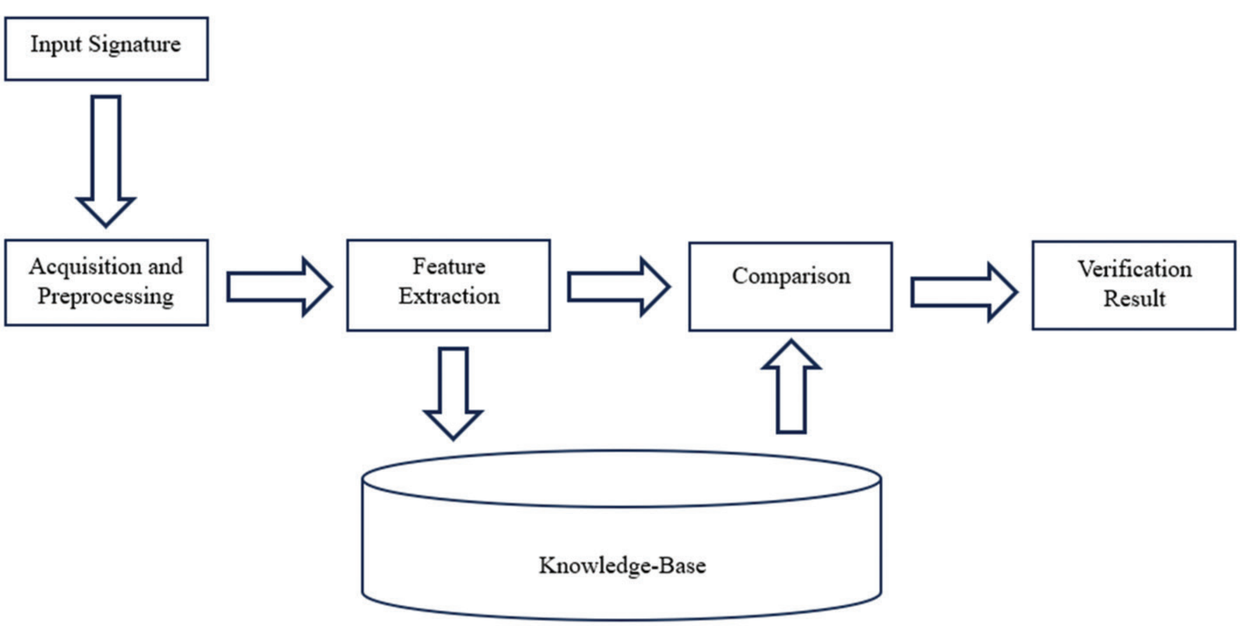

Figure 1: Signature Verification Flow Diagram

This study utilizes two publicly available benchmark datasets: CEDAR (English signatures) and BHSig260 (Bengali and Hindi signatures). These datasets consist of genuine and forged offline handwritten signatures representing diverse scripts and writing styles. Prior to model training, all images were resized, binarized for contrast enhancement, and normalized to ensure uniform input format. The data was divided into 70% for training, 15% for validation, and 15% for testing, maintaining a balanced distribution across classes.

Each input image is passed through convolutional layers for spatial feature extraction, followed by bidirectional GRU layers to capture forward and backward temporal dependencies. The Siamese network structure consists of three identical branches processing anchor, positive, and negative samples. Embeddings are normalized using L2 and optimized using triplet loss.

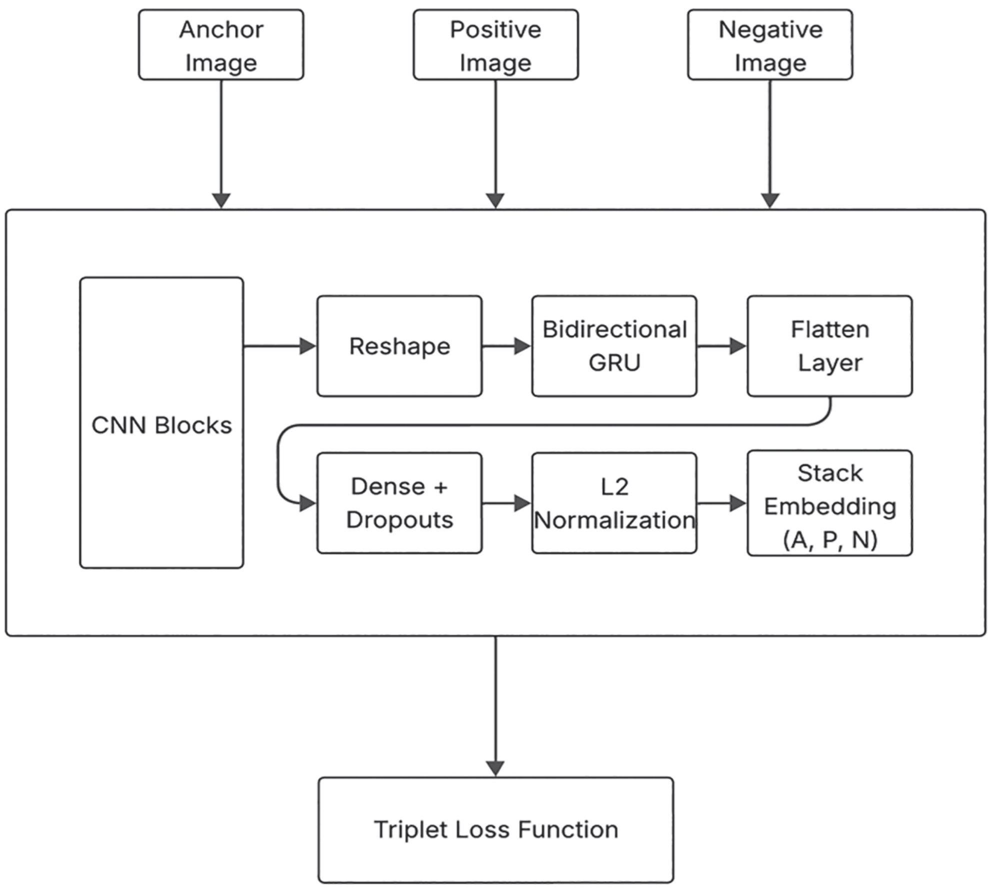

Figure 2: BRCSN Architecture Model

The model is trained using a triplet loss function:

$$L = \max(||f(a) - f(p)||^2 - ||f(a) - f(n)||^2 + \alpha, 0)$$

where a = anchor, p = positive, n = negative, and α = margin. The Adam optimizer with a learning rate of 0.0001 is used for backpropagation.

Table 1: BRCSN Model Hypermeter

Parameter	Value
Batch Size	64
Epochs	25
Input Resolution	150×400 pixels

Performance is evaluated using Accuracy, Precision, Recall, F1-score, AUC, FAR (False Acceptance Rate), and FRR (False Rejection Rate).

3. Results and Discussion

The proposed BRCSN model significantly outperforms the baseline Convolutional Siamese Network (CSN) across all metrics, as shown in Table 2:

Table 2: Performance comparison between BRCSN and CSN

Metric	BRCSN	CSN
Accuracy (%)	90.0	61.0
Precision	0.88	0.66
Recall	0.93	0.48
F1-Score	0.90	0.55
AUC-ROC	0.97	0.72

The model achieved an F1-score of 0.90, with a recall of 93.4% in detecting skilled forgeries. The FAR was under 2%, while FRR remained below 8%, demonstrating a balanced security-usability trade-off. The system performed consistently across different scripts and writing styles, indicating strong generalization.

4. Conclusions

This study presented a novel Bidirectional Recurrent Convolutional Siamese Network (BRCSN) for offline, writer-independent signature verification, addressing critical limitations of existing systems. The BRCSN model's hybrid architecture combines convolutional layers for spatial feature extraction with bidirectional recurrent units for temporal pattern analysis, enabling a comprehensive and discriminative representation of handwritten signatures. Trained with a triplet loss function, the model effectively learns to distinguish genuine signatures from skilled forgeries, outperforming conventional CNN and LSTM-based approaches. Notably, the model generalizes well across multiple scripts - English, Bengali, and Hindi - without requiring writer-specific retraining, thus offering a scalable and adaptable solution. With inference times under 100 milliseconds, the BRCSN model demonstrates practical viability for real-time deployment in domains such as banking, legal documentation, and biometric authentication systems. These results mark a significant advancement in offline signature verification and offer a strong foundation for future improvements in privacy-aware and distributed learning environments.

References

Chen, X., & Zhang, W. (2020). Fuzzy logic-based writer independent offline signature verification. IEEE Transactions on Cybernetics, 50(9), 3983–3992.

Dhillon, G. S., & Bhatti, S. (2021). Writer independent signature verification using CNN-LSTM hybrid architecture. Journal of Image and Vision Computing, 33(2), 88–96.

González-González, J., Ferrer, M. A., & Morales, A. (2018). Off-line signature verification using recurrent neural networks and transfer learning. IEEE Transactions on Information Forensics and Security, 13(7), 1756–1767.

Justino, E. J. R., Bortolozzi, F., & Sabourin, R. (2001). Off-line signature verification using HMM for random, simple, and skilled forgeries. In Proceedings of the International Conference on Document Analysis and Recognition (pp. 450–453).

Patel, D., & Thakur, A. (2019). Performance analysis of writer dependent and independent signature verification systems using deep learning. International Journal of Intelligent Systems and Applications, 11(1), 59–66.

Singh, A., Kaushik, R., & Mehta, P. (2022). Offline signature verification using Siamese networks with contrastive loss. Pattern Recognition Letters, 45(3), 109–120.

Srihari, S. N., Cha, S. H., Arora, H., & Lee, S. (2002). Individuality of handwriting. Journal of Forensic Sciences, 47(4), 856–872.