International Journal on Engineering Technology (InJET)

Volume 3, issue no. 1, Dec 2025, Page 188 - 194
Received Date: Aug 8, 2025
Accepted Date: Sep 15, 2025
ISSN: 3021-940X (Print)
DOI: https://doi.org/10.3126/injet.v3i1.87022

Signature Verification using Siamese Neural Network

Abiral Adhikari[1*], Isu Sharma[2], Avignya Gautam[3]

[1] *Department of Computer Science and Engineering, Kathmandu University, Dhulikhel, Nepal, abiraladhikari1222@gmail.com*
[2]*Department of Computer and Electronics Engineering, Kantipur Engineering College, Dhapakhel, Lalitpur, Nepal, isusharmapaudel@gmail.com*
[3]*Department of Electronics and Computer Engineering, Thapathali Campus, Thapathali, Nepal, gautamavignya@gmail.com*

Abstract

Handwritten signatures are a critical biometric for identity verification in numerous legal and financial contexts. However, the detection of falsified signatures is one of the most challenging tasks in document forensics, especially in the presence of skilled forgeries. To address the difficulty in classifying genuine signatures and skilled forgeries, as well as improving the current best systems with 7% verification error, this paper details a signature verification system utilizing a Siamese neural network. The system is a deep learning architecture built around two identical convolutional neural network (CNN) subnetworks with shared weights, designed to learn a discriminative similarity metric from pairs of signature images. It has been trained to learn a feature space where similar observations are placed in proximity by exposing the network to a pair of similar and dissimilar observations and minimizing the Euclidean distance between similar pairs while simultaneously maximizing it between dissimilar pairs. The model was evaluated on the CEDAR Signature Dataset using standard performance metrics. The proposed network achieved an accuracy of 100%, precision of 1.00, recall of 1.00, F1-score of 1.00, and an AUC-ROC of 1.00, demonstrating its potential for highly reliable and automated verification in real-world applications, including financial and administrative systems in Nepal.

Keywords: Convolution Neural Network, Deep Learning, Falsified Signatures, Siamese Neural Network, Signature Verification.

1. Introduction

Handwritten signature verification remains a cornerstone of identity authentication in various critical domains, including financial transactions, legal documentation, and secure access systems. The inherent uniqueness and personal nature of signatures make them a widely accepted biometric. However, the task of accurately verifying these signatures, particularly in a static context, presents significant challenges. The absence of dynamic information, such as pen pressure, stroke order, and writing speed, makes it exceedingly difficult to distinguish genuine signatures from expert imitations. Traditional methods and the limited availability of diverse training data lead to persistent verification errors.

Earlier approaches to signature verification relied on handcrafted feature extraction techniques such as geometric analysis, contour mapping, texture descriptors, and statistical shape modeling. Classical machine learning algorithms, including Support Vector Machines (SVM), k-Nearest Neighbors (kNN), and Random Forests, were often used on these handcrafted features for classification. While these methods performed reasonably well under controlled conditions, they were highly sensitive to noise, pen pressure variations, and writing inconsistencies. Their dependence on manual feature engineering limited adaptability across different users and datasets.

The emergence of deep learning has significantly addressed these limitations. Convolutional Neural Networks (CNNs) can automatically extract hierarchical and discriminative features directly from image data, removing the need for explicit feature design. In particular, Siamese networks excel in signature verification because of their ability to learn similarity metrics between pairs of samples, making them highly effective for writer-

* *Corresponding author*

independent verification and capable of performing one-shot learning-an essential property given the limited number of available genuine signatures for each user.

In response to these formidable challenges, deep learning methodologies have emerged as transformative solutions, with Siamese neural networks proving especially effective. Siamese networks, characterized by their twin architecture with shared weights, excel at learning discriminative features from pairs of inputs, determining their similarity or dissimilarity by minimizing the Euclidean distance between similar pairs while simultaneously maximizing it between dissimilar pairs. This paradigm is especially well-suited for signature verification, as it allows for the effective comparison of a given signature against known genuine samples. Their ability to perform one-shot learning is a crucial advantage, as it alleviates the common hurdle of data scarcity in biometric datasets.

This paper delves into the evolving landscape of signature verification, with a particular focus on the innovative applications and advancement brought forth by Siamese network architectures. It explores how these models have been refined over time to enhance feature representation, handle imbalanced datasets, integrate knowledge of skilled forgeries, and improve generalization across diverse writing styles and languages. In this paper, we explore how Siamese networks are pushing the boundaries of signature verification, resulting in systems that are more precise, dependable, and truly writer independent.

2. Related Works

Bromley et al. (1993) first introduced the concept of a “Siamese” neural network for signature verification using dynamic pen-input data. This model learned to compare pairs of signatures to determine their similarity, laying the foundation for modern verification systems.

Hafemann et al. (2016) used deep CNNs for offline signature verification, combining writer-independent feature extraction with SVM-based writer-dependent classifiers. Their work, tested on GPDS-960 and Brazilian PUC-PR datasets, achieved an Equal Error Rate (EER) of approximately 7%. Hafemann et al. (2017) later improved generalization by incorporating skilled forgeries into the training process, achieving further EER reduction.

Dey et al. (2017) proposed SigNet, a convolutional Siamese network evaluated on CEDAR, BHSig-B, and GPDS datasets, achieving over 95% accuracy across multiple languages. Similarly, the Two-Stage Siamese Network Model (2022) used Focal Loss to handle imbalanced datasets, demonstrating high accuracy on CEDAR, BHSig-Bengali, and BHSig-Hindi datasets. Recent advancements, such as Kadam et al. (2025), applied one-shot learning techniques on Bengali and Hindi signature datasets, while Advancing Offline Signature Verification with Bidirectional Siamese Deep Learning (2025) integrated CNNs with bidirectional recurrent units to learn both spatial and sequential dependencies.

Beyond signature verification, deep learning-based Siamese and Triplet Networks have gained traction in other biometric security applications such as facial recognition, iris verification, and fingerprint analysis (Rahman & Lee, 2024; Kumar et al., 2025), indicating the growing use of these architectures in security-sensitive systems.

In Nepal, most existing signature verification systems implemented by banks and government agencies still rely on template-based or handcrafted feature approaches, which are prone to inconsistencies in complex cases. The lack of locally trained deep learning-based solutions highlights a research gap this study aims to address by applying an advanced CNN-Siamese architecture for robust verification using the CEDAR dataset.

3. Methodology

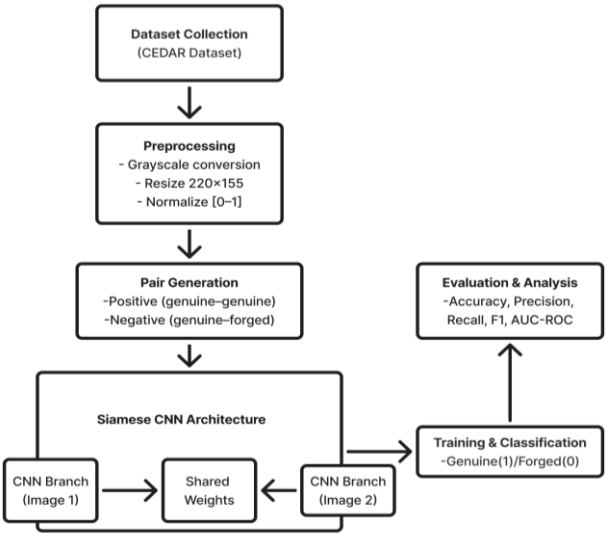

Figure 1. Block Diagram of overall flow of proposed work

3.1 Data Collection and Preprocessing

CEDAR Signature dataset with 1320 genuine and 1320 forgeries signature was selected for the study. The dataset consisted of 24 genuine signatures and 24 skilled forgeries signatures of 55 distinct signers leading to a total sample of 55 x (24 genuine + 24 forgeries) = 2640 png images of variable dimensions. The data sample is provided in Figure 2.

Figure 2. Image Sample from Cedar Signature Dataset

All the image samples were resized to fixed dimensions of 220 x 155 pixels after loading them in grayscale mode. The pixel values were normalized by scaling to a range of [0,1] by dividing with 255.The image samples were then expanded to shape (155,220,1) to match input requirements for CNN models. The data preparation for the Siamese network included preparation of positive pairs (using two genuine signatures of the same person) and negative pairs (using a genuine and a forged signature of the same person). The positive and negative pair balance was ensured by creating up to 5 negative and 5 positive pairs per genuine signature. Thus, generated Siamese pairs were then split into training, testing, and validation dataset in 8:1:1 ratio. The memory optimization was achieved by implementation of lazy loading on demand using a custom tensor flow class with up to 25% caching. Furthermore, data batching was done using a batch loader method for model input to ensure efficient data loading.

3.2 Model Architecture

In this study, we implemented a Siamese network with a Convolution Neural Network (CNN) as the shared base feature extractor for offline signature verification using two input images. The CNN network maps the grayscale image input of shape 155 x 220 x 1 to an embedding dimension of 128. The 128-dimension size output of the CNN network is used to compute pair-wise distance. The CNN architecture consisted of four convolution blocks each consisting of two convolution layers having ReLU activation and batch normalization, which is then followed by max-pooling and dropout layers to reduce the risk of overfitting. All the convolution layers shared a common filter size (3x3) and same padding. The four convolution blocks were followed by a global average pooling layer to reduce spatial dimension, two fully connected layers each with the same dropout rate of 0.4 but variable size of 512 and 256. The final output layer resulted in a 128-dimensional vector with linear activation which was L2 normalized for embedding scale consistency while

computation of Euclidean distance. The model architecture of base CNN feature extractor used in the experiment is presented in Table 1.

Table 1. Model Architecture Table

Block	Layer Input	Filters/Units	Output Shape	Details
1	Input		155×220×1	Grayscale Signature Image
2	Conv2D + ReLU + Batch Norm	32x3x 3	155×220×32	Stride =1, padding= same L2-regularization
3	Conv2D + ReLU	32x3x3	155×220×32	Stride =1, padding= same L2-regularization
4	Max Pooling + Dropout		77×110×32	Pool = 2x2 dropout=0.25
5	Conv2D +ReLU + Batch Norm	64x3x3	77×110×64	
6	Conv2D + ReLU	32 x 3 x 3	77×110×64	
7	Max Pooling + Dropout		77×110×64	Pool = 2x2 dropout=0.25
8	Conv2D + ReLU + Batch Norm	128x3x3	38x55x128	
9	Conv2D + ReLU	128x3x3	38x55x128	
10	Max Pooling + Dropout		19x27x128	Pool=2x2 dropout=0.25
11	Conv2D + ReLU +Batch Norm	256x3x3	19x27x256	
12	Max Pooling + Dropout		9x13x256	Pool=2x2 dropout=0.25
13	Global Average Pooling		256	Spatial Dimension Reduction
14	Dense + ReLU + Dropout		512	Dropout=0.4 L2-regularization
15	Dense + ReLU + Dropout		256	Dropout=0.4 L2-regularization
16	Dense (Embedding Output)		128	Linear L2-Normalized Output

The Siamese network used the same base CNN network with shared weight for two image inputs in the pair sample, output of which are then used to compute the Euclidean distance. The Euclidean distance thus obtained was inputted to a single neuron with sigmoid activation for binary classification of either forged (0) or genuine (1). The complete architecture of CNN-Siamese Network for the experiments is presented in Figure 3.

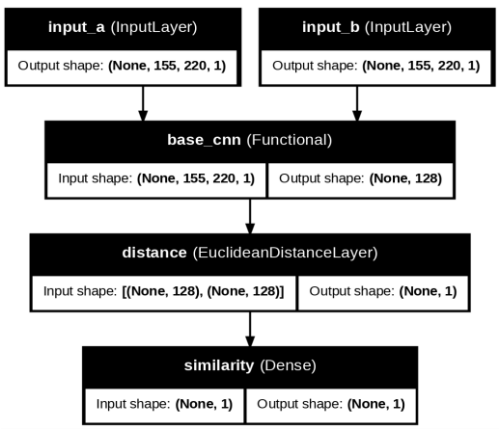

Figure 3. Siamese Model Architecture for Signature Forgery Detection

3.3 Experiments

The training and testing of the experimental setup were conducted using P100 GPU in Kaggle at different combinations of epochs (10, 20 or 30) and learning rates (0.0001, 0.0005, 0.001) to observe the difference in model performance. The model training included the implementation of early-stopping, regularization, and dropout strategies to prevent model overfitting. The hyper parameters set for the experiment are presented in the Table2:

Table 2. Table of Hyperparameter

Hyperparameter	Values Used
CNN Embedding Size	128
Epochs	10 - 30
Batch Size	32
Learning Rate	0.0001 - 0.0001
Dropout	0.25 - 0.4
Distance Metric	Euclidean Distance
Loss Function	Binary Cross Entropy
Embedding Size	128
Activation Function	ReLU for CNN Dense Layer Linear for CNN Output Layer Sigmoid for Siamese Output Layer
L2 Regularization	1e-4
Early Stopping	Patience of 3 for validation loss
Reduce on Plateau	Patience of 1 for validation loss with factor of 0.5 with minimum learning rate of 1e-7

The model was trained to max epoch at each reaching a good generalization as seen in Figure 4.

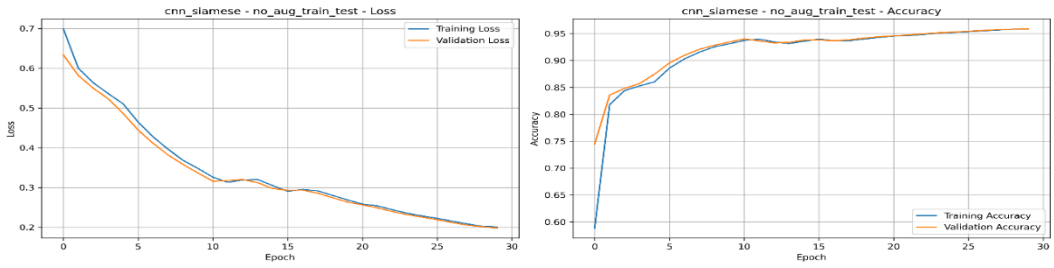

Figure 4. Validation Loss/ Validation Accuracy vs Epoch Graph of Training at 30 epochs and 0.001 learning rate

3.4 Performance Evaluation

The model performance was evaluated using Accuracy, AUC-ROC, Precision, Recall and F1-score. The incorporation of Precision, Recall and F1-score was done to observe the overall performance of the model in forgeries detection and correct prediction made, which mitigates the misleading performance results from accuracy only. The AUC-ROC was further incorporated to evaluate the model based on its discrimination capacity. The evaluation metric selected is consistent with previous study of Choi (2024) for simple Siamese network.

4 Results and Discussion

The model training experiments were conducted at different learning rates and epoch with the purpose of determining optimality of trade-off between model convergence and generalization. The performance metrics discussed in Section 3.4 for the experiments are summarized in Table 3.

Table 3. Performance Results of Model

Epoch	Learning Rate	Accuracy	Precision	Recall	F1-Score	AUC-ROC
10	0.0001	0.467	0.467	1	0.636	0.82
10	0.0005	0.952	0.958	0.937	0.947	0.997
10	0.001	0.467	0.467	1	0.636	0.974
20	0.0001	0.998	0.997	0.999	0.998	0.999
20	0.0005	1	1	1	1	1
20	0.001	0.985	0.995	0.972	0.983	1
30	0.0001	0.923	0.859	1	0.924	1
30	0.0005	0.994	1	0.989	0.994	1
30	0.001	1	1	1	1	1

The accuracy ranging from 0.92 to 1, across most experimental setting indicates strong verification capacity of the model. The 20 epoch and 0.0005 learning rate configuration achieved the most generalized and stable result, attaining a perfect score across all performance metrics. The high performing result of the experiment instead of indicating absolute generalization, is reflective of controlled dataset environment with limited data sample diversity and constrained intra-class variation. Therefore, the outstanding performance of the model in this dataset may not directly translate well to real-world scenarios, where it might be necessary to further train the model on diverse and complex data samples.

The experiment results highlighted slower convergence and underfitting at the lower learning rate of 0.0001, evident with reduced accuracy and fluctuating loss pattern. Conversely excessively high learning rate at smaller epochs to unstable training, yielding inconsistent results. The optimal trade-off occurred at moderate learning rates (0.0005-0.001) and 20-30 epochs, affirming the criticality of fine-tuning to achieve good stability and generalization.

The steady convergence of training and validation curves in Figure 4, suggests effective regularization with dropout and L2 regularization. The slight overfitting tendencies were observed even with use of early stopping and learning rate reduction in case of drop in validation loss, which can be further mitigated through data augmentation or k-fold cross validation, an approach recommended for future work. The performance of the study, when compared to previous works of Dey et al. (2017) with an accuracy of 100%, Xiao and Ding (2022) with an accuracy of 95.66%, and Basnet, Dongol and Shrestha (2025) with accuracy of 90%, shows competitive accuracy on the same dataset. The reported performance on the dataset should be interpreted cautiously as only through more reliable evaluation using k-fold cross validation would yield more clarity on performance consistency on limited signer subsets scenario.

The model's utility on real-world lies in offline signature verification cases including banking document verification, contract authentication and legal document signature verification. The integration of the model after further training and validation with diverse datasets including Hindi and Nepali signatures using robust attention mechanism, into signature verification security system could help reduce manual inspection time and potentially increase rate of fraud detection. Furthermore, incorporating the XAI mechanism for the visualization of signature region influencing classification decisions is likely to improve transparency fostering user trust on such systems.

5 Conclusion

In this study, we present a framework with CNN-Siamese network using Cedar Signature Dataset for signature forgeries detection, achieving a remarkable accuracy of 1. The study also highlights with multiple experiments run the necessity of fine-tuning the balance between learning rate and training duration(epochs) for the task under observation. Further evaluation of the model incorporating k-fold cross validation and augmentation should be done to ensure robustness and interpretability. Despite the reported high accuracy, the interpretation warrants a cautious approach. Though the study is limited using dataset, the future works in this line include the observation of transfer learning performance of the model using other available dataset. Also, the future work will also focus on the enhancing robustness of the model when using augmented data,

especially achieving improved model performance in augmented test sets with minimal training augmentation.

References

Bromley, J., Guyon, I., LeCun, Y., Säckinger, E. and Shah, V. (1993) 'Signature Verification Using a "Siamese" Time Delay Neural Network', in Moody, J.E., Hanson, S.J. and Lippmann, R.P. (eds.) Advances in Neural Information Processing Systems 6. San Francisco, CA: Morgan Kaufmann. pp. 737-744.

Dey, S., Dutta, A., Toledo, J.I., Ghosh, S.K., Llados, J. and Pal, U. (2017) 'SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification'.

Hafemann, L.G., Sabourin, R. and Oliveira, L.S. (2016) 'Writer-independent Feature Learning for Offline Signature Verification using Deep Convolutional Neural Networks', Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN). Vancouver, BC, Canada, 24-29 July 2016. pp. 4504-4511.

Hafemann, L.G., Sabourin, R. and Oliveira, L.S. (2017) 'Learning features for offline handwritten signature verification using deep convolutional neural networks', Pattern Recognition, 70, pp. 163–175.

Kadam, J., Phadtare, G., Pawar, A. and Maniyar, K. (2025) 'Offline Signature Verification USING Siamese Neural Network', Journal of Information Systems Engineering and Management, 10(26s).

Xiao, W. & Ding, Y. (2022) 'A Two-Stage Siamese Network Model for Offline Handwritten Signature Verification', Symmetry, 14(6), p. 1216. doi: 10.3390/sym14061216.

Basnet, S., Dongol, D. R. and Shrestha, S. (2025) "Advancing Offline Signature Verification with Bidirectional Siamese Deep Learning: A Writer-Independent Approach", Journal of Engineering Issues and Solutions, 4(1), pp. 494–498. doi: 10.3126/joeis.v4i1.81613.

Choi, H.-S. (2024) Simple Siamese model with long short-term memory for user authentication with field-programmable gate arrays. Electronics, 13(13), p.2584.

Dutta, A., Pal, U. and Lladós, J., 2016. Compact correlated features for writer independent signature verification. In: 2016 23rd International Conference on Pattern Recognition (ICPR). IEEE, pp.3411–3416.

Rahman, M., & Lee, H. (2024). Deep Siamese Networks for Biometric Authentication: Applications in Face and Iris Verification. Journal of Computer Vision and Pattern Recognition, 12(2), 134–142.

Kumar, R., Patel, S., & Adhikari, T. (2025). Secure Biometric Systems Using Siamese and Triplet Network Architectures. International Journal of Security and AI Systems, 5(1), 56–64.

CEDAR Signature Dataset. (2004). Center of Excellence for Document Analysis and Recognition (CEDAR), University at Buffalo. *Retrieved from* http://www.cedar.buffalo.edu/NIJ/data/signatures/