SIGNATURE AUTHENTICATION VERIFICATION USING SIAMESE NEURAL NETWORK

[1]Vudduru.Bharathi, [2]P. Pranitha, [3]P. Chandana, [4]T. V. K. Tejaswini, [5]V. Heshma
[1]Associate Professor, [2,3,4,5]UG Student, [1,2,3,4,5]Department of Computer Science & Engineering (AI&ML),
Geethanjali Institute of Science And Technology, Nellore, India

Abstract
Signature authentication plays a crucial role in verifying the legitimacy of academic, legal, and business documents. It is a biometric technique used to authenticate individuals based on their unique signing patterns with advancements in machine learning, particularly in deep learning methods such as Convolutional Neural Networks (CNNs) and Siamese Networks have been employed to enhance the accuracy of both online and offline signature verification systems. There are mainly two types of signature verification: static and dynamic. Siamese Neural Networks (SNNs), a deep learning architecture designed for similarity detection. The SNN model analyzes pairs of signature images, extracting feature representations and computing similarity scores to distinguish between genuine and forged signatures. By integrating fewshot-learning, the system enhances feature extraction and improves verification accuracy. Siamese networks are effective for this task because they learn a similarity metric rather than classifying signatures directly
Keywords:

Introduction

A signature is a handwritten depiction of a person's name or mark used to authenticate identity and validate documents. It is one of the oldest and most widely accepted biometric traits. A signature reflects individual writing behavior, making it unique to each person. It is legally recognized and commonly used in banking, contracts, government forms, and more. Unlike other biometrics, signatures are non-intrusive and socially accepted. They require no specialized equipment to create and can be easily captured on paper. This simplicity makes signatures a convenient method of identity verification. Despite the rise of digital authentication, handwritten signatures remain relevant. Their continued use has encouraged research into automatic signature verification techniques. In today's digital age, preserving the reliability of handwritten signatures is essential for secure identity management.

SIGNATURE AUTHENTICATION

Signature authentication is the process of verifying whether a given signature genuinely belongs to the claimed individual. It plays a crucial role in confirming identity across various sectors, including finance, legal, and government services. This method ensures that signatures on documents are not forged or tampered with. Authentication can be performed manually by experts or automatically using biometric systems. With the advancement of technology, automated signature authentication has become more reliable and efficient. It is categorized into online and offline methods, with offline being more practical for scanned or paper-based documents. Offline Signature Verification (OSV) uses image processing and machine learning to validate static signature images. This approach is gaining attention due to its low infrastructure needs and broad applicability. Signature authentication remains vital for securing transactions and maintaining trust. In a digital world, it bridges the gap between traditional practices and modern security demands.

SIGNATURE AUTHENTICATION VERIFICATION

Signature authentication verification is a process used to confirm the identity of an individual by analyzing their handwritten signature. It ensures that a signature presented on a document genuinely belongs to the claimed person. This method is crucial in preventing fraud and maintaining the integrity of legal, financial, and official records. It is commonly employed in sectors like banking, government, and insurance. The verification can be performed through online or offline approaches. Online methods use real-time data such as pen pressure and motion, while offline methods rely on analyzing static images. Offline Signature Verification (OSV) is especially valuable for scanned or paper-based documents. Techniques like deep learning and pattern recognition are used to improve verification accuracy.

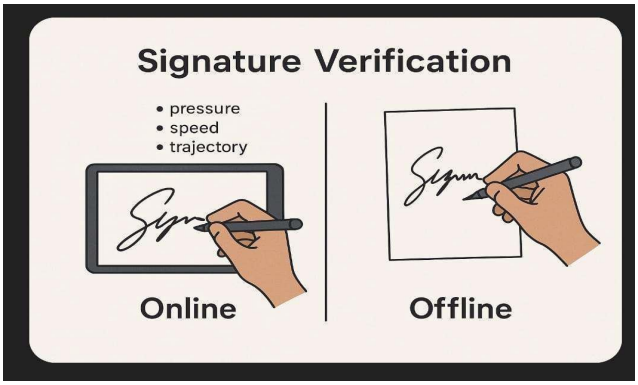

Fig 1: Signature Authentication Verification

TYPES OF SIGNSTURE AUTHENTICATION VERIFICATION SYSTEMS

It is the process used to confirm the identity of an individual by analyzing their handwritten signature. This method is crucial in preventing fraud and maintaining the integrity of legal, financial, and official records. The verification can be performed by two approaches. They are:

1) Static or Offline Signature Verification
2) 2) Dynamic or Online Signature Verification

This project aims to design and implement an advanced Signature Authentication and Verification System using a Siamese Neural Network (SNN), a deep learning architecture well-suited for tasks involving similarity measurement. Handwritten signatures remain a widely accepted form of identity verification across multiple sectors, including banking, legal documentation, and digital forensics. However, manual verification methods are often subjective, time-consuming, and prone to human error. To address these limitations, the proposed system leverages the power of deep learning to provide a robust and automated solution for signature verification. At the core of this system lies the Siamese Neural Network, which is specifically designed to compare pairs of inputs and determine their similarity. The model is composed of two identical Convolutional Neural Networks (CNNs) with shared weights. These CNNs are responsible for extracting feature representations from two input signature images. The outputs of the CNNs—feature vectors—are then passed to a distance function, such as Euclidean or cosine distance, to compute the similarity score between the two signatures.

Problem Statement

Handwritten signatures have long served as a cornerstone of identity verification across various sectors, including banking, legal documentation, and government services. However, the manual verification of these signatures is increasingly susceptible to human error, especially in the face of sophisticated forgery techniques. Skilled forgeries can closely mimic genuine signatures, making it challenging to distinguish between authentic and counterfeit documents. Traditional verification methods often rely on expert analysis, which is not only time- consuming but also subjective and inconsistent. This subjectivity can lead to discrepancies in the validation process, undermining the trust placed in signature-based authentication. Moreover, the rise of digital

documentation necessitates the development of automated systems capable of verifying signatures on scanned or digitally captured documents, where dynamic writing characteristics are absent.

Literature Review

[1] "Zheng, Lidong, Xingbiao Zhao, Shengjie Xu, Yuanyuan Ren, and Yuchen Zheng. "Learning discriminative representations by a Canonical Correlation Analysis-based Siamese Network for offline signature verification." Engineering Applications of Artificial Intelligence 139 (2025): 109640." The authors observed that distinguishing between genuine and forged signatures in offline verification tasks is challenging due to the subtle differences in writing behaviors. They proposed a writer-independent Canonical Correlation Analysis-based Siamese Network (CCASigNet) to learn discriminative representations between signature pairs. By training the model with three types of signature pairs—genuinegenuine, genuine-forged, and forged-forged—they effectively captured nuanced features distinguishing genuine signatures from forgeries. The network used CCA and classification-based losses, resulting in strong feature extraction capabilities. Experimental results across four benchmark datasets demonstrated that CCASigNet achieved state-of- the-art performance, outperforming existing verification systems. Additionally, the model showed excellent generalization and can be easily transferred to datasets with different language scripts. This approach provides an effective solution for writer-independent offline signature verification.

[2] "Xiao, Wanghui, and Hao Wu. "Learning features for offline handwritten signature verification using spatial transformer network." Scientific Reports 15, no. 1 (2025): 9453." The authors observed that offline signature verification is particularly challenging due to the difficulty in distinguishing subtle but crucial differences between genuine and expertly forged signatures. To address this, they proposed a two-stage Siamese network model with a spatial transformer network, which helped improve feature extraction by focusing on relevant handwriting details while ignoring irrelevant information. The use of the Focal loss function addressed the class imbalance between genuine and forged signatures, improving training effectiveness. Experimental results on four diverse handwritten signature datasets demonstrated that the proposed model outperformed existing state-of-the-art methods in verification accuracy. The approach showed strong generalization across different languages, highlighting its robustness. This model provides an efficient solution for offline signature verification tasks, with significant improvements in both accuracy and efficiency. Overall, the proposed system enhances document security and authentication reliability

[3] "Babu, Kancharagunta Kishan, Srikanth Lukka, Palliyana Shabarish, Aviresh Laxman Sai, Bandi Sai Varshini Goud, and Ganji Yeshwanth. "Online Signature Verification Using Deep Learning." In 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), pp. 1196-1201. IEEE, 2025." The authors observed that while online signature verification (OSV)systems are critical for secure authentication, they face challenges in providing real- time responsiveness and reliable performance, especially as new users are added to the database. The authors proposed integrating a CNN-based Siamese network with a ReactJS- based web interface, enabling efficient signature upload and storage. The model effectively extracts spatial features from signatures, comparing them for similarity to determine authenticity. By continuously training the model, the system can handle both real and forged signatures, improving over time. The combination of signature preprocessing, feature extraction, and classification models ensures robustness and accuracy in identity verification. The proposed system offers a reliable solution for secure online transactions and digital applications. This approach minimizes manual effort and enhances the security of signature-based authentication systems.

[4] "Gutub, Adnan, Sahar Altalhi, and Budur Ghazwani. "Offline Efficient Signature Authentication Using Octave Convolution Neural Network." Arabian Journal for Science and Engineering (2025): 1-16." The authors observed that offline signature verification is particularly challenging due to the difficulty in distinguishing between genuine and skillfully forged signatures, especially given the limited features available in offline

systems. They proposed the use of Octave Convolution (OctConv), which outperformed traditional Convolutional Neural Networks (CNN) in terms of accuracy. By comparing OctConv with several baseline CNN models, the authors demonstrated that OctConv achieved superior results across multiple signature datasets, including CEDAR, UTSig, BHSig260-Hindi, and BHSig260- Bengali. The proposed model showed competitive performance against state- of-the-art methods, including CNN and capsule networks. The study highlights the effectiveness of OctConv in overcoming the limitations of traditional CNNs and improving verification accuracy. The approach provides a promising solution for enhancing signature verification systems, especially for cybersecurity applications. The results demonstrate that OctConv is well-suited for distinguishing genuine signatures from forgeries.

[5] "Abinesh, G., V. Kavitha, and Prajith J V. "Signature Verification Using Deep Learning and CNN." International Journal of Innovative Science and Research Technology 10, no. 3 (2025): 374-381." The authors observed that traditional signature verification methods struggle with intra-class variability, reducing their reliability in distinguishing between genuine and forged signatures. They demonstrated that CNN-based models can extract spatial features more effectively, enabling robust feature learning. The use of a Siamese network with contrastive or triplet loss improved verification accuracy by focusing on pairwise similarity. The model generalized well to unseen data, indicating strong adaptability across different users and datasets. Experimental results showed that this deep learning approach outperformed traditional methods in accuracy, precision, recall, and F1- score. The system also reduced manual effort in forensic analysis. Overall, the approach presents a significant advancement in automated and reliable signature authentication.

WORKFLOW OF THE SYSTEM

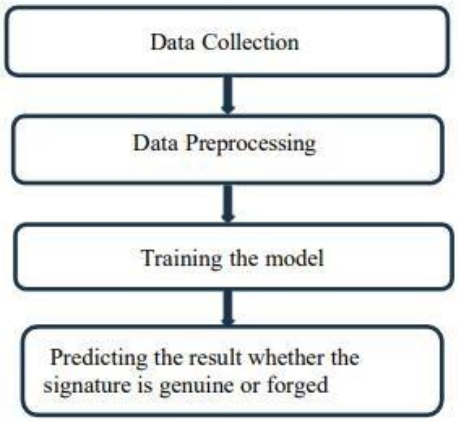

Fig 7: Workflow of the system

The process begins with Data Collection, where historical signatures samples are collected from various individuals. The dataset includes both genuine and forged signatures to ensure balanced learning. A large and diverse dataset improves the model's ability to generalize. Proper labeling of each sample is crucial for supervised learning. Following this, the Pre-Processing stage involves the raw signature data is cleaned and prepared for analysis. This may involve resizing images, converting them to grayscale, and removing noise. Normalization and feature extraction techniques are also applied. Preprocessing ensures the model receives consistent and high-quality input. The preprocessed data is used to train the model. The model learns to recognize distinguishing features between genuine and forged signatures. Siamese network is used for training the model leveraging pairs of signature images (genuine and forged). The network learns to compare the similarities between two signatures, producing a similarity score. During training, the model minimizes a contrastive loss function, ensuring that genuine signature pairs are closer in feature space while forged signatures are farther apart. The network is trained iteratively, with evaluation metrics like accuracy and precision used to

assess performance. Once trained, the model is tested with new signature inputs. It analyzes the input and predicts whether the signature is genuine or forged. The prediction is based on the patterns and features learned during training. This step ensures real-time and accurate verification of signatures

Results & Analysis

EVALUATION METRICS

Evaluation metrics are essential tools used to assess the performance and accuracy of machine learning models and algorithms. These metrics provide quantitative measures that enable researchers and practitioners to evaluate the effectiveness of their methods and make informed decisions about model selection and optimization. Moreover, the choice of evaluation metrics depends on the nature of the problem being addressed and the desired outcome. By utilizing a combination of evaluation metrics, practitioners can gain comprehensive insights into the overall performance of their models and make informed decisions regarding their deployment and optimization strategies. These Evaluation metrics play a crucial role in not only validating the performance of machine learning models but also in comparing different models and algorithms. They help in identifying the strengths and weaknesses of a model, guiding the refinement process for better outcomes. Common evaluation metrics include Mean Absolute Error (MAE), Mean Squared Error (MSE), accuracy, and execution time. Each metric serves a specific purpose in evaluating different aspects of model performance, such as prediction accuracy, error magnitude, and computational efficiency.

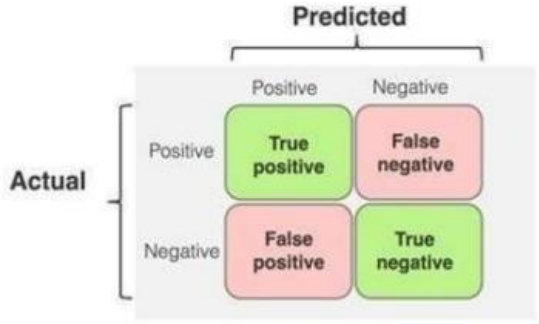

Fig 10 Performance Metrics

Accuracy– The mean amount of accurate predictions is used to characterize the accuracy measure. This isn't quite as strong, though, given the imbalanced sample.

$$= \frac{+}{+ + +} \quad (1)$$

Precision, also known as positive predictive value, gauges the capacity of a model to pinpoint the right examples for every class. For multi-class classification with unbalanced datasets, this is a powerful matrix.

$$= \frac{}{+} \quad (2)$$

RESULT COMPARISION

Model	Accuracy (%)	Precision (%)
Siamese Network	96.5	95.2
Random Forest	91.3	89.4
Hidden Markov Model (HMM)	89.8	87.6
Support Vector Machine (SVM)	93.1	91.7

Table 1: Performance Comparision of Various Algorithms.

The performance comparison of various algorithms for signature verification reveals that the Siamese Network stands out with an impressive accuracy of 96.5% and precision of 95.2%. This suggests that the Siamese Network is highly effective in distinguishing between genuine and forged signatures. In comparison, other algorithms such as Random Forest, Hidden Markov Model (HMM), and Support Vector Machine (SVM) also perform well, but with slightly lower accuracy and precision rates. For instance, SVM achieves an accuracy of 93.1% and precision of 91.7%, while Random Forest and HMM trail behind with accuracy rates of 91.3% and 89.8%, respectively.

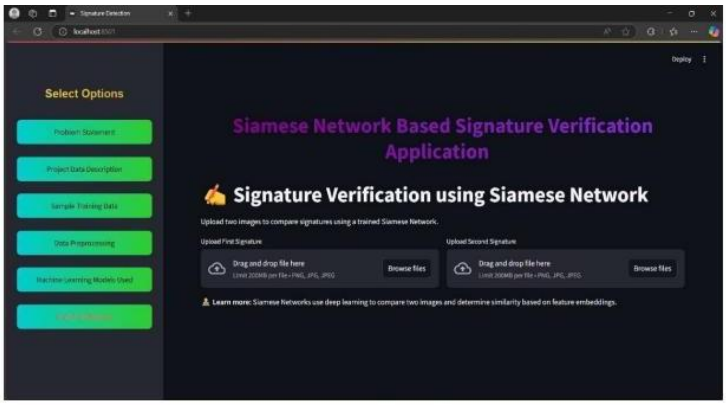

Fig 7.2.1: Home Page

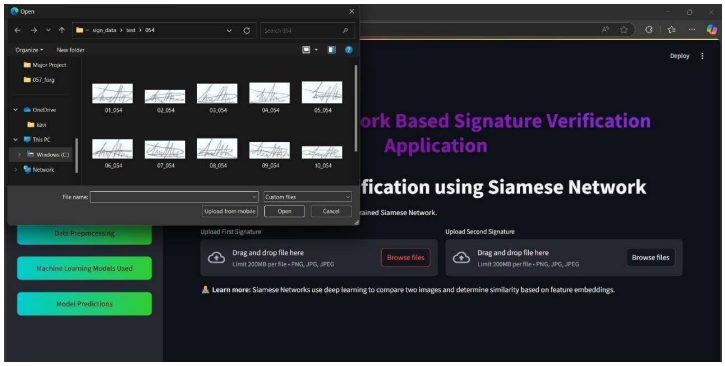

Fig 7.2.2: Uploading Signature Images

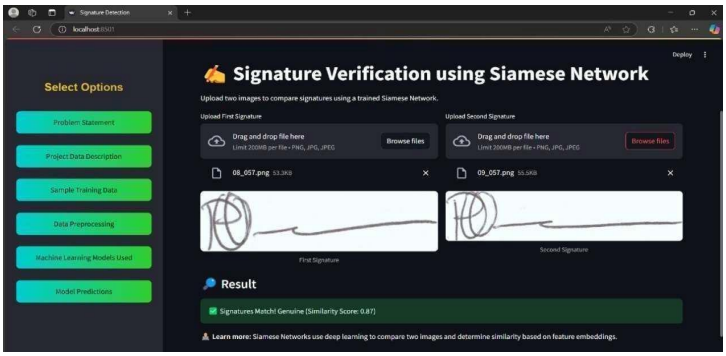

Fig 7.2.3: Signature Authenticated

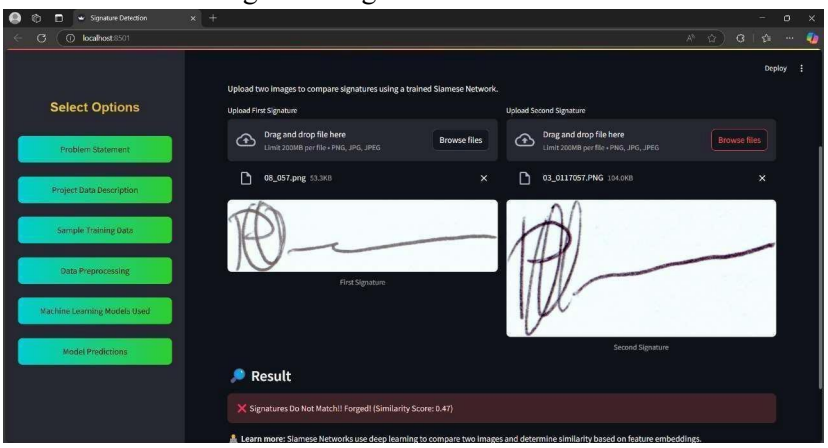

Fig 7.2.4: Signature not Authenticated

Conclusion

Signature authentication using Siamese Networks provides a reliable and accurate method for verifying handwritten signatures. By leveraging deep metric learning, the system effectively distinguishes between genuine and forged signatures, even with limited training data. It enhances security by reducing false acceptance and false rejection rates, making it suitable for applications like banking and identity verification. The model's scalability ensures efficient authentication for large datasets without frequent retraining. Additionally, it supports both online (dynamic) and offline (static) signature verification. The system's computational efficiency makes real-time authentication feasible.

Future Scope

The results show that the Siamese Network is an effective approach for verifying signatures with high accuracy. However, 100% efficiency is not yet achieved. Therefore, future work can focus on enhancing the performance by exploring advanced deep learning techniques such as transformer-based models or attention mechanisms to better capture subtle signature features. Additionally, incorporating unsupervised learning can help in identifying hidden patterns in unlabeled signature data, further improving the system’s generalization. By extending the system to generate visual explanations or attention maps, users can also gain a clearer understanding of which parts of the signature contributed most to the verification decision. Future advancements, such as hybrid models (CNN-RNN) or transformer-based architectures, can further enhance its robustness against sophisticated forgeries.

References

1. Zheng, Lidong, Xingbiao Zhao, Shengjie Xu, Yuanyuan Ren, and Yuchen Zheng."Learning discriminative representations by a Canonical Correlation Analysis-based Siamese Network for offline signature verification." Engineering Applications of Artificial Intelligence 139 (2025): 109640.
2. Xiao, Wanghui, and Hao Wu. "Learning features for offline handwritten signature verification using spatial transformer network." Scientific Reports 15, no. 1 (2025): 9453.
3. Babu, Kancharagunta Kishan, Srikanth Lukka, Palliyana Shabarish, Aviresh Laxman Sai, Bandi Sai Varshini Goud, and Ganji Yeshwanth. "Online Signature Verification Using Deep Learning." In 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), pp. 1196-1201. IEEE, 2025.
4. Gutub, Adnan, Sahar Altalhi, and Budur Ghazwani. "Offline Efficient Signature Authentication Using Octave Convolution Neural Network." Arabian Journal for Science and Engineering (2025): 1-16.
5. Abinesh, G., V. Kavitha, and Prajith J V. "Signature Verification Using Deep Learning and CNN." International Journal of Innovative Science and Research Technology 10, no. 3 (2025): 374-381.
6. Tehsin, Sara, Ali Hassan, Farhan Riaz, Inzamam Mashood Nasir, Norma Latif Fitriyani, and Muhammad Syafrudin. "Enhancing Signature Verification Using Triplet Siamese Similarity Networks in Digital Documents." Mathematics 12, no. 17 (2024): 2757.
7. Jain, Arihant, and Ashish Kumar. "Siamese Network For Signature Verification On Various Distributions of Data." In 2024 3rd International Conference for Advancement in Technology (ICONAT), pp. 1-10. IEEE, 2024.
8. Reddy, M. Sowmya, A. Anagha Lakshmi, G. Siddarth Reddy, B. Koustubha Madhavi, Bhawani Sankar Panigrahi, and V. Mohan. "Signature Forgery Detection using Siamese- Convolutional Neural Network." In 2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU), pp. 1-5. IEEE 2024
9. Xiao, Wanghui. "Offline Handwritten Signature Verification using Siamese Network Model." In 2024 6th International Conference on Electronic Engineering and Informatics (EEI), pp. 1536-1539. IEEE, 2024.
10. Catugas, Marevil E., Christelle Joyce M. Cerezo, Raymund M. Dioses, and Khatalyn E. Mata. "Enhancement of Siamese Neural Network for Improved Signature Fraud Detection".