Signature Verification using Siamese Networks with one Shot Learning for Offline Biometric Authentication

[1]N.Divyasruthi, [2]B.Harshini, [3]M.Madhuri, [4]M.Saikeerthana, [5]A.Siporarani
[1]Assistant Professor , [2,3,4,5]UG Students, [1,2,3,4,5]Department of Computer Science & Engineering, Geethanjali Institute Of Science And Technology, Hyderabad, India

Abstract
With the rapid advancement of digitalization across industries, the demand for secure and efficient biometric authentication methods has grown significantly. Among various biometric modalities, signature verification remains critical in sectors such as banking, legal documentation, and forensics. This study focuses on offline signature verification, which is inherently more challenging than its online counterpart, as it relies solely on static, scanned images without capturing the dynamic motion ofthe signing process. To address this complexity, we propose a Siamese Neural Network architecture trained using One-Shot Learning, which enables effective verification with minimal labeled data. Unlike conventional deep learning models that require large datasets for classification, this approach leverages similarity learning to distinguish between genuine and forged signatures using just a few samples. Our method is evaluated on multiple benchmark datasets, including 4NSigComp2012, SigComp2011, 4NSigComp2010, and BHsig260, achieving impressive accuracy rates of 93.23%, 90.11%, 89.99%, and 92.35%, respectively. The results demonstrate the effectiveness of the proposed model in low-data scenarios, making it a practical and scalable solution for offline signature verification in real-world applications.
Keywords: Signature verification, Siamese network, one shot learning, offline biometric authentication

Introduction

Signature verification using Siamese networks with one-shot learning offers an efficient method for authenticating handwritten signatures, particularly when extensive datasets are unavailable. This approach utilizes two identical convolutional neural networks (CNNs) to processapairofsignatureimages—oneasareferenceandtheotherasaquery.Thenetworks share the same architecture and weights, ensuring consistent feature extraction. After encodingthesignaturesintofeaturevectors,asimilaritymeasure,suchasEuclideandistance orcosinesimilarity,isemployedtodetermineifthesignaturesbelongtothesameindividual. This method excels inreal-world applications like banking and legaldocument verification, where signatures may vary in style and conditions. By enabling verification with minimal data,itprovidesapracticalsolutionforreal-timeauthenticationonmobiledevicesandonline platforms. Studies have demonstrated its effectiveness, achieving high accuracy rates on various benchmark datasets

Motivation

The motivation behind using Siamese networks with one-shot learning for signature verification lies in the growing need for efficient and scalable authentication systems. Traditional methods often require vast databases of signatures for comparison, which is impractical in many real-world scenarios where only a single example of a person's signature is available for verification.

By leveraging one-shot learning, Siamese networks allow for accurate and reliable verification with minimal data, making them highly suited for environments like banking, legal applications, or mobile devices. This approach not only reduces the data requirements but also offers a robust solution to the challenges of signature variability and forgery detection, providing a practical and secure means of authentication in an increasingly digital world.

Literature Review

Sara Tehsin et al. (2024): Enhancing Signature Verification Using Triplet Siamese Similarity Networks in Digital Documents

Authors (Sara Tehsin et al.): The team includes multiple contributors with a focus on deep learning applications in digital forensics and document authentication.

Analyzed OSV Techniques: The study investigates the application of deep similarity learning, particularly the use of a Triplet Siamese Network, for verifying offline signatures embedded in digital documents.

Methodological Approach:

Triplet SiameseNetwork**:**Takesthree inputs—anchor(originalsignature),positive (same person's signature), and negative (forged or different person's signature).

Thenetworkminimizesthedistancebetweentheanchorandpositivewhile maximizing the distance from the negative.

UsesManhattanDistancetoemphasizeabsolutedifferences infeaturerepresentations.

Advantages: Achieveshighaccuracy(>85%), indicating strongdiscriminative powerin identifying forgeries.

Generalizeswellacrossmultipledatasets, evenwithhighintra-classvariability.

Effectiveindetectingskilledorsimilarforgeries,whichareoftendifficultto identify.

Disadvantages: Sensitivetoimagetransformationslikerotation,scaling,andflipping,affectingresult consistency. Requireswell-preparedtriplet samples,whichcanbecomputationallyexpensiveto construct.

Xiao Wanghui & Yuting Ding (2022): A Two-Stage Siamese Network Model for Offline Handwritten Signature Verification

Authors (Xiao Wanghui & Yuting Ding): Researchers with a focus on biometric authentication and machine learning in the context ofAsian scripts.

Analyzed OSV Techniques: This paper introduces a two-stage Siamese model specifically designed to tackle class imbalance and improve learning on imbalanced datasets.

Methodological Approach:

Stage1:ExtractsfeaturevectorsforsignaturepairsusingaSiamesenetworkwith shared convolutional layers.

Stage2:RefinesoutputusingaclassifiertrainedwithFocalLoss,prioritizing misclassified or minority samples.

TheapproachistailoredforChinesesignaturedatasets,whicharecomplexdueto character diversity.

Advantages: Effective in imbalanced datasets with genuine and forged signatures. Handlesintra-writerandinter-writervariabilitybetterthantraditionalSiamese networks. Improvesmodelfocusonhardexamples, enhancing robustness.

Disadvantages: Limited to Chinese datasets, may not performe qually on multilingual datasets. May requirere-trainingortuningfordatasetswithdifferentlinguisticorstylistic features.

MuhammadFawwazMayda&AinaMusdholifah(2021):Siamese- Network Based Signature Verification Using Self-Supervised Learning

Authors (Mayda & Musdholifah): Focused on reducing the dependency on large labelled datasets by using self-supervised techniques in deep learning.

Analysed OSV Techniques: The paper explores using self-supervisedlearningto pre-train a Siamese model on unlabelled signature data for verification tasks.

Methodological Approach: Usescontrastiveself-supervisedlearning,wherethemodelassociatesaugmentedviews of the same signature and differentiates between others. After self-supervised pre-training, the model is fine-tuned with a small labelled set for the final verification task.

Problem Statement

In scenarios like banking or e-document validation, collecting many signature samples is oftenimpractical.Weidentifiedtheneedforamodelthatcomparessignatures,generalizesto new users, and performs well with limited data. This approach addresses the limitations of traditional systems.

Proposed Model

We're developing an online signature verification system using Siamese Neural Networks (SNN) and One-Shot Learning to reduce enrolment samples. Our approach achieves high accuracy with just one or a few reference signatures. This makes the system more practicalin real-world scenarios with limited data collection.

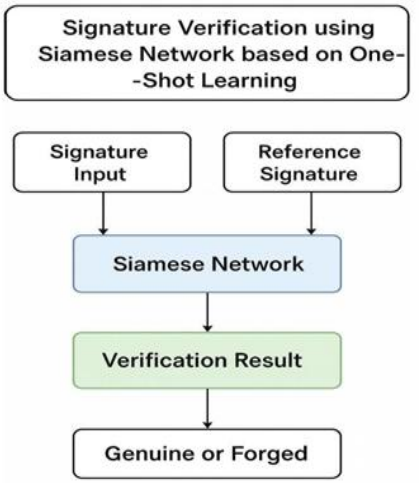

Fig.1. System proposed model flow

Data Acquisition and Preprocessing

We collect dynamic signature data, including stroke order, timing, velocity, and pressure, using digital input devices. Each pair of signatures (genuine vs. test) is then normalized and undergoes noise removal to ensure consistency.

Twin Sub networks for Feature Extraction

Two identical neural networks with shared weights process the input signature pair. Each subnetwork extracts a high-dimensional feature vector from the raw signature, capturing the behavioural traits of the signing process.

Distance Calculation

The model computes the distance or similarity score between the two feature vectors using a distancemetric(e.g.,Euclideanorcosine).Thisscoreindicateshowsimilarthetwosignatures are in terms of signing behaviour.

Classification

Based on the similarity score and a predefined threshold, the system determines whether the test signature is genuine or forged. This approach supports one-shot learning by enabling comparison with a single stored template.

Siamese Neural Network(SNN)

This architecture compares two signatures through twin sub networks (shared weights) that extract feature embeddings. It calculates the distance between embeddings -smaller distances indicate genuine matches, larger ones suggest forgeries. The model excels at pair wise comparison, recognizing signature similarities even for unseen users during training.

One-Shot Learning:

The Siamese Network learns to compare signatures rather than memorize users, enabling verificationwithjustonereferencesampleduringtestingwithoutrequiringretraining fornew users, making it ideal for

real-world deployment where user data is limited.

Contrastive Loss Function:
The Siamese Network uses contrastive loss to minimize distances between matching modelto distinguishgenuinesignaturesfromforgeriesthroughdiscriminative feature learning.

Feature Extraction via CNN/LSTM:

The Siamese Network's twin branches use CNNs (for spatial patterns) or LSTMs (for temporal dynamics) to extract distinctive behavioral features from raw signature data like stroke patterns, timing, and pressure.

Distance Metric Algorithm:
The model calculates signature similarity using either Euclidean distance (absolute vector distance) or cosine similarity(directionalalignment)betweenfeatureembeddingstodetermine if they constitute a match.

Architecture

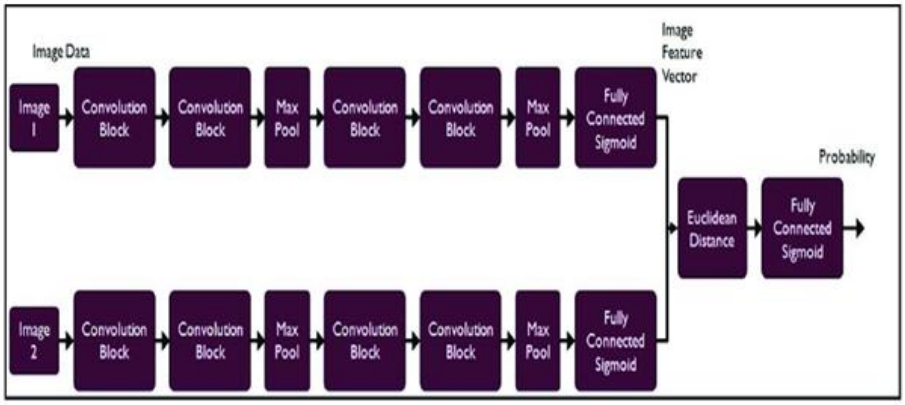

Fig.2. System Architecture model

Input Layer (Image1&Image 2):
The architecture processes two input images simultaneously—a reference signature (genuine/stored) and a test signature (user-input for verification)—through parallel branches. These branches share identical structure and weights, a defining feature of Siamese networks, ensuring consistent feature extraction for accurate comparison. This design enables the network to analyze similarities between signatures effectively.

Convolutional Blocks:
The architecture processes both signatures through identical convolutional layers that extract key spatial features like stroke thickness, shape patterns, and edge contours. Each convolutional block uses ReLU activation to introduce non-linearity and capture complex signature characteristics. This enables the network to analyze how the signature is written, not just its visual appearance, for more accurate verification.

Max Pooling Layers:
After every few convolution blocks, there's a Max Pooling layer. This layer: Reduces the spatial dimensions (down sampling), Keeps the most significant features, helps with faster computation and avoids over fitting

Fully Connected Sigmoid Layer (Feature Embedding):
After the final convolution and pooling operations, the output is flattened and passed through a fully connected (dense) layer with a sigmoid activation. This results in a feature vector (also called an embedding) that represents the behavioral and visual signature of the image. Both branches produce their own feature vectors for Image 1 and Image 2.

Euclidean Distance Layer:

ThenetworkcomputestheEuclideandistancebetweenthetwosignatureembeddings-smaller distances indicate genuine matches, while larger distances suggest forgeries. This distance metric forms the core verification mechanism of the Siamese architecture, directly measuring signature similarity in the learned feature space. The final output provides a clear, quantitative measure of authenticity.

Final Fully Connected Sigmoid Layer (Probability Output):

The network's final layer uses sigmoid activation to convert the distance metric into a 0-1 probability score. Scores exceeding a set threshold (typically 0.5) classify the signature as genuine, while lower values indicate forgeries, completing the binary verification decision. This probabilistic approach provides an interpretable and tunable authentication mechanism.

SIAMESE NETWORK

A Siamese network is a deep learning architecture that compares two input samples and measures their similarity. It consists of two identical subnetworks with shared weights, typically using convolutional neural networks (CNNs) for image-based tasks. The network calculates a similarity score by measuring the distance (e.g.,Euclidean or cosine) between the feature vectors of the inputs. It is trained to minimize the distance for similar pairs and maximize it for dissimilar pairs, learning the concept of similarity.

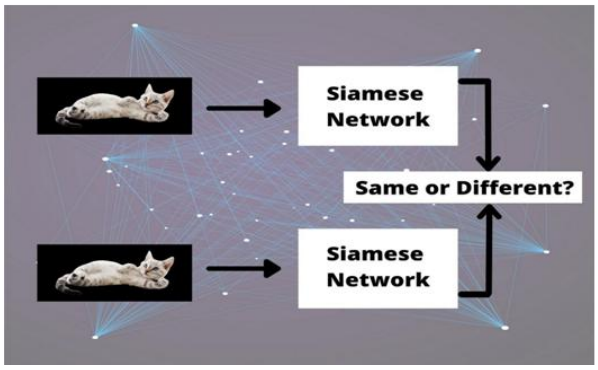

Fig.3. Siamese network model

Siamese networks are particularly useful in tasks like one-shot learning, where the system must recognize or verify new instances from just a single example. Applications include signature verification, face recognition, and object matching. The network's ability to generalize from few examples makes it an efficient and powerful tool for tasks requiring comparison and similarity assessment.

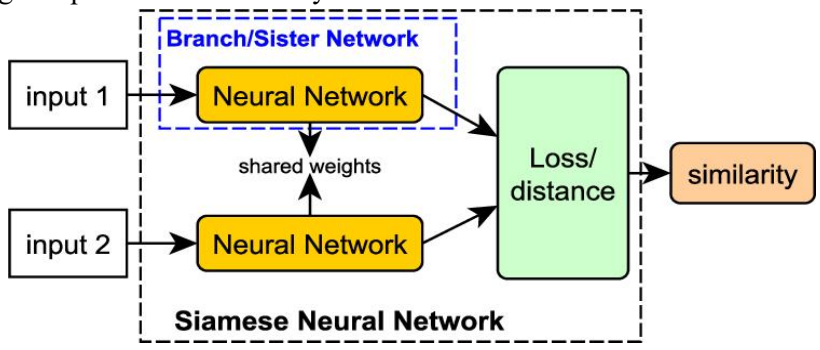

Fig.4. Siamese neural network

Architecture

ONE-SHOTLEARNING

OneShotLearningisamachinelearningparadigmaimingtorecognizeobjectsorpatternsfrom a limited number of training examples, often just a single instance. Traditional machine learning models typically require large amounts of labelled data for high performance. Still, one-shot learning seeks to overcome this limitation by enabling models to generalize from minimal data.

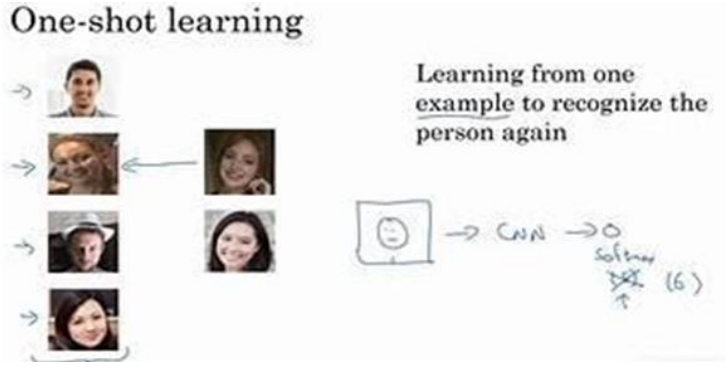

Fig.5. One shot learning

One-shot learning is a machine learning technique that enables models to recognize new classes or objects based on a single example. Unlike traditional models that require large datasets, one- shot learning aims to generalize from minimal data, mimicking human learning capabilities. This approach is particularly effective in tasks like signature verification, where obtaining numerous samples for each individual is impractical. By learning to compare and assess similarities between inputs, one-shot learning models can accurately identify new instances

SYSTEMIMPLEMENTATION

SYSTEMMODULES

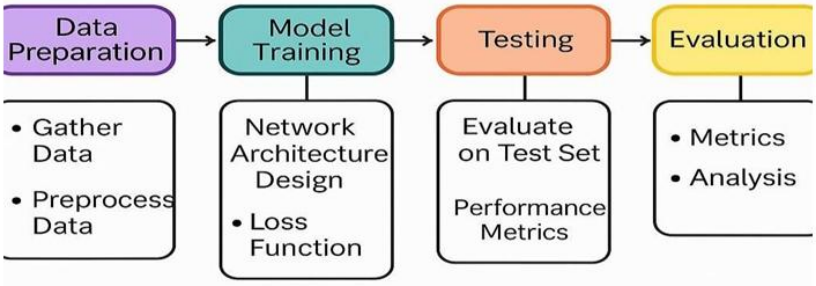

Fig.6. System Modules

Data Preparation

Gather Data**:** Gather a dataset of both genuine and forged signatures, such as from the SigComp datasets. Ensure the dataset includes different writing styles and variations in the signaturestoimprovethemodel'sabilitytogeneralize.PreprocessData**:**Convertallsignature imagestograyscaletosimplifythedataandreducecomputationalcomplexity.Resizeimages to a consistent size (e.g., 100x100 pixels) and normalize pixel values to a range of 0 to 1 for faster training.

Model Training:

Network Architecture Design: Design the Siamese network with two identical sub-networks that share weights. Each sub-network processes one signature image, and the output layer calculates the similarity between the two images. Loss Function: Use a contrastive loss or triplet loss function to train the model. This will help the network learn to minimize the distance between similar signatures and maximize the distance between different ones.

Testing:

Evaluate on Test Set: After training, evaluate the model using a separate test set containing unseen signature pairs to assess the model's performance on new data. Performance Metrics:

Usemetricslikeaccuracy,precision,recall,andF1-scoretomeasurethemodel'seffectiveness in correctly identifying genuine vs. forged signatures.

Evaluation:

Metrics: These are measurements used to evaluate how well the model is performing. Common ones for your project include: Accuracy: The percentage of correct predictions. Precision: The percentage of true positive predictions out of all positive predictions made by the model.

Recall: The percentage of true positives out of all actual positive instances.

F1-score:Abalancebetweenprecisionandrecall,usefulwhenthere'sanimbalanceinthedata.

Analysis:Aftercalculatingmetrics,analysetheresultstounderstandthemodel'sperformance.

Forexample,ifthemodelhashighprecisionbutlowrecall,itmightbeverygoodatidentifying forged signatures but misses some genuine ones.

Results & Analysis

Stream lit App URL Generated in CMD

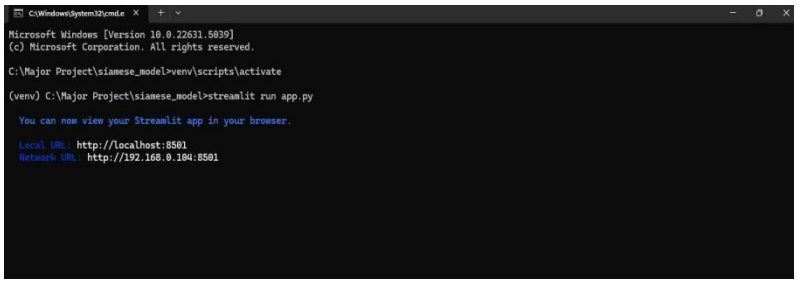

Fig.7. Stream lit App URL Generated in CMD

Folders Containing Genuine and Forged Signature Images

Fig.8. Folders Containing Genuine and Forged Signature Images

App Landing Page Showing Genuine vs Forged Signatures

Fig.9. App Landing Page Showing Genuine vs Forged Signatures

App Interface Displaying Dataset Description and Context

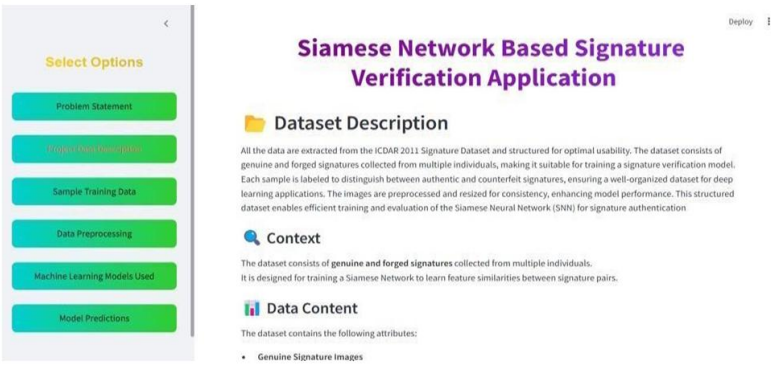

Fig.10. App Interface Displaying Dataset Description and Context

App Interface Displaying Training Data Preview

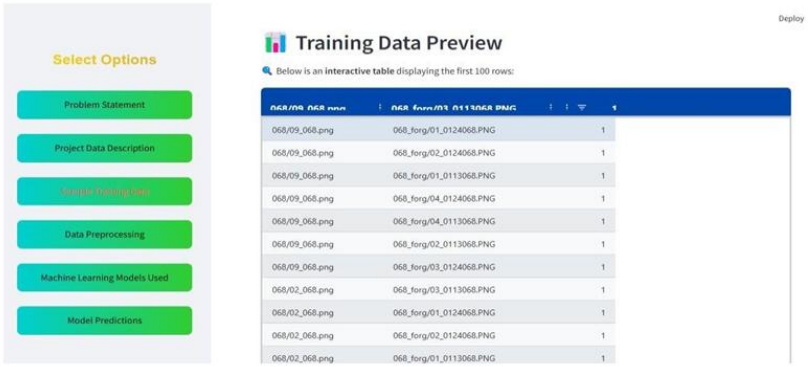

Fig.11. App Interface Displaying Training Data Preview

Data Preprocessing using Image Processing, Labelling, and Augmentation

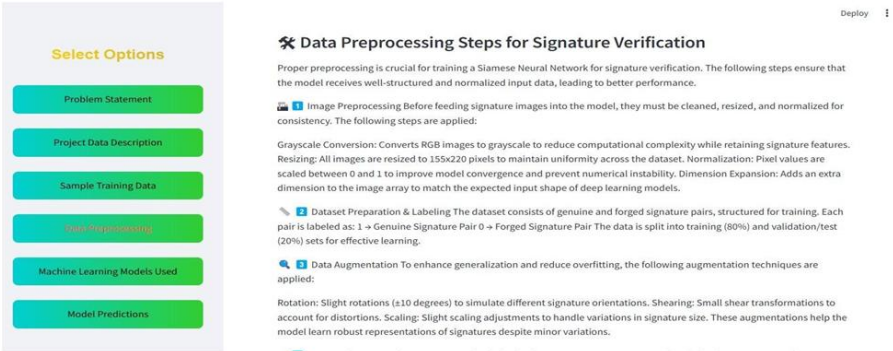

Fig.12. Data Preprocessing using Image Processing, Labelling, and Augmentation

Siamese Neural Network for Signature Verification using CNN and Contrastive Loss

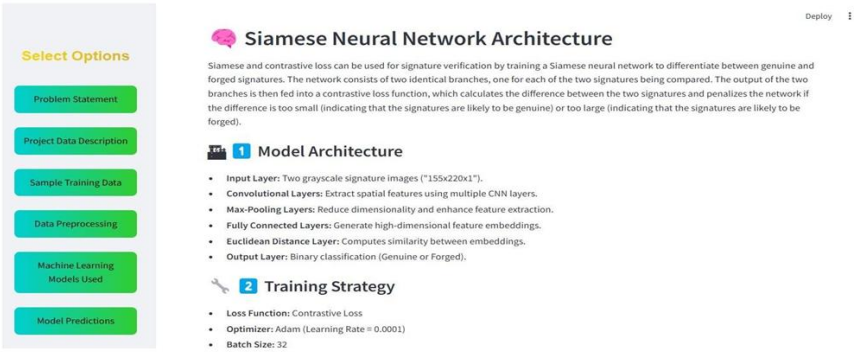

Fig.13. Siamese Neural Network for Signature Verification using CNN and Contrastive Loss

App Interface for Signature Verification and Matching Result

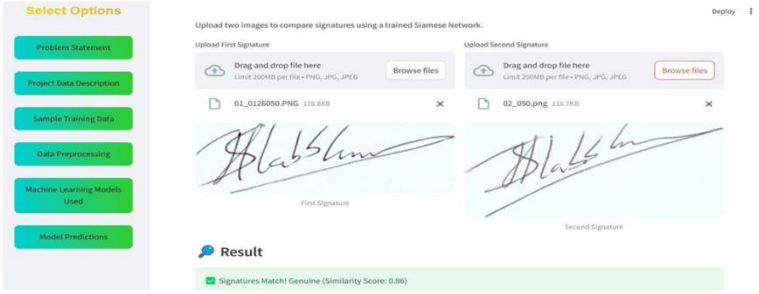

Fig.14. App Interface for Signature Verification and Matching Result

App Interface Displaying Forged Signature Detection Result

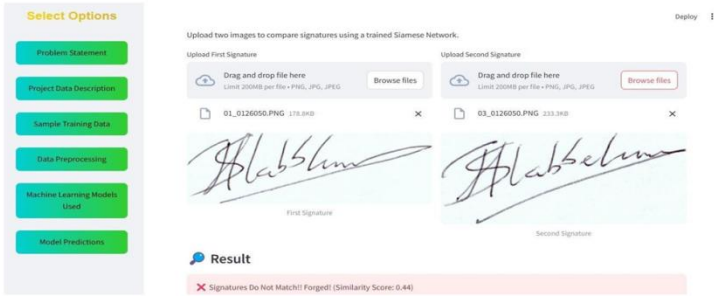

Fig.15. App Interface Displaying Forged Signature Detection Result

CONCLUSION

The study indicates that combining Siamese Neural Networks with One-Shot Learning makes signature verification far more accurate, especially when there isn't a lot of training data available. The model does a good job of telling the difference between real and fake signatures, making it perfect for secure authentication. Future work may add Generative Adversarial Networks (GANs) to the system to help it find AI-generated forgeries. This will make it better at finding little differences and make it more reliable overall.

Future Scope

This project lays the groundwork for further advancements in signature verification. To enhanceitseffectiveness,expandingthetrainingdatasettoincludeabroaderrangeofgenuine and forged signatures will improve the model's generalization. Additionally, integrating Siamese Networks withGAN-based models could boostthe system's capabilityto detectAI- generatedforgeries.Employingattentionmechanismsorpre-trainedmodelsmayfurtherrefine feature extraction and improve accuracy. Finally, optimizing the system for real-time verification would increase its practical value in domains like banking, legal authentication, and digital

security. These enhancements willpave the way for a more secure and intelligent verification system.

References

1. Koch, G., Zemel, R., & Salakhutdinov, R. (2015). Siamese Neural Networks for One- shot Image Recognition. ICML Deep Learning Workshop.
2. Bromley, J., Guyon, I., LeCun,Y., Säckinger, E.,& Shah, R. (1994). Signature Verificationusinga“Siamese”TimeDelayNeuralNetwork.InAdvancesinNeural Information Processing Systems (NIPS).
3. Schroff, F., Kalenichenko, D., &Philbin, J. (2015). FaceNet:AUnifiedEmbedding for Face Recognitionand Clustering. InProceedingsofthe IEEEConference onComputer Vision and Pattern Recognition (CVPR).
4. Goodfellow, I.,Pouget-Abadie, J., Mirza, M., Xu,B.,Warde-Farley, D., Ozair, S.,... & Bengio, Y. (2014). Generative Adversarial Nets. In Advances in Neural Information Processing Systems (NeurIPS).
5. Loddo,A.,Fenu,G.,&Marras,M.(2020).One-ShotLearningforSignatureVerification Using Siamese Networks. Pattern Recognition Letters, 135, 234–240.
6. Graves, A., & Schmidhuber, J. (2005). Framewise phoneme classification with bidirectionalLSTM and other neuralnetworkarchitectures. NeuralNetworks, 18(5- 6), 602-610.
7. Jindal, A., Singla, K., & Aggarwal, A. (2021). Signature Verification Using Deep Learning: ASurvey. International Journal of ComputerApplications, 975, 8887.
8. Chollet, F. (2017). Xception: Deep Learning with Depthwise Separable Convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)