

# Signature Verification System using Siamese Neural Networks

Dr. K. M. Shivaprasad<sup>1</sup>, Madan HS<sup>2</sup>, K. Harshitha<sup>3</sup>, K. Nitish Kumar<sup>4</sup>

Associate Professor, Department of Computer Science and Engineering<sup>1</sup>

Students, Department of Computer Science and Engineering<sup>2,3,4</sup>

Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, Karnataka, India

corresponding author: shivakalmutt@gmail.com

**Abstract:** This paper presents an efficient approach to signature verification and forgery detection using Siamese neural networks algorithm. This research involves training classifiers on a diverse dataset of signatures in different persons. Our method employs vectorization and Euclidean distance classifier for signature classification and detection tasks. Experimental results demonstrate the effectiveness of the classifiers with high accuracy and robustness against various signature styles and classifying the genuine and forgery signatures. The approach showcases notable efficiency in signature forgery detection, addressing the growing need for various fraud detecting solutions.

**Keywords:** Forgery detection, Siamese neural network, Signature classification, Euclidean distance

## I. INTRODUCTION

Signature is one of the most popular and commonly accepted biometric hallmarks that has been used since the ancient times for verifying different entities related to human beings, viz. documents, forms, bank checks, individuals, etc. Therefore, signature verification is a critical task and many efforts have been made to remove the uncertainty involved in the manual authentication procedure, which makes signature verification an important research line in the field of machine learning and pattern recognition [1, 2]. Depending on the input format, signature verification can be of two types: (1) online and (2) offline. Capturing online signature needs an electronic writing pad together with a stylus, which can mainly record a sequence of coordinates of the electronic pen tip while signing. Apart from the writing coordinates of the signature, these devices are also capable of fetching the writing speed, pressure, etc., as additional information, which are used in the online verification process. On the other hand, the offline signature is usually captured by a scanner or any other type of imaging devices, which basically produces two dimensional signature images. As signature verification has been a popular research topic through decades and substantial efforts are made both on offline as well as on online signature verification purpose.

This paper introduces a novel approach to forgery detection using Siamese Neural network and contrastive loss function are probabilistic models based on deep learning models like Convolution neural networks (CNN), known for image classification, image preprocessing tasks. By leveraging a datasets in multiple styles of signature we train for signature classification and forgery detection.

The primary question addressed in this research paper is how to develop an efficient method for detecting the forgery of signatures. This question is crucial in the context of growing digitalization on daily life as well as emerging problems in digital frauds and financial frauds.

The significance of this study lies in its potential to contribute the enhancement of deep learning techniques in the area of signature forgery detection. By providing robust methodology and experimental validation.

## II. LITERATURE SURVEY

Xiao et al [3], (2020), have explored a two-part splicing forgery detection method. The two parts consist of a coarse-to-refined convolutional neural network(C2RNet) and a diluted adaptive clustering network. In the proposed model the differences in the image are found by cascading a coarse CNN and refined CNN (C-CNN and R-CNN respectively). The cascading results in making scales where the image has been tampered finding difference in their properties. The

computational complexity of the whole model is reduced by an imagelevel CNN rather than using a patch level CNN into C2RNet. Since the difference in properties is compared therefore it results in stabilised results. It was found that the proposed method produces better results than the already existent splicing techniques for forgery detection even in conditions of attack. However, the size of these datasets restricts training and hence optimal results are not yet obtained from this proposed model.

**Sigari et al. [4], (2011)**, have proposed a new method for offline (static) handwritten signature identification and verification based on Gabor wavelet transform. The whole idea is offering a simple and robust method for extracting features based on Gabor Wavelet which the dependency of the method to the nationality of signer has been reduced to its minimal. The advantages of this system is its capability of signature identification and verification of different nationalities; thus it has been tested on four signature dataset with different nationalities including Iranian, Turkish, South African and Spanish signatures.

**Bertolini et al [5], (2010)**, highlighted two important issues of off-line signature verification. The first one regards feature extraction. They introduce a new graphometric feature set that considers the curvature of the most important segments, perceptually speaking, of the signature.

### III. METHODOLGY

**Datasets:** We utilized a publicly available datasets comprising the signature samples labelled with their identity, genuine or forgery. The dataset consists of diverse signature data collected from various sources, including indivuals, legal documents and other financial transaction documents. Each signature sample associated with its identity number, genuine or forgery. The dataset is split into training, validation, and testing sets to ensure a comprehensive evaluation of the model's performance.

#### Architecture of Siamese Neural Network:

- Siamese network takes two different inputs passed through two similar subnetworks with the same architecture, parameters, and weights.
- The two subnetworks are mirror image of each other, just like a Siamese twins. Hence any change to any subnetworks architecture, parameters and weights is also applied to other subnetwork.
- The two subnetwork outputs an encoding to calculate the difference between the two inputs
- The Siamese network's objective is to classify if the two inputs are the same or different using the Similarity score. The Similarity score can be calculated using Binary cross-entropy, Contrastive function, or Triplet loss, which are techniques for the general distance metric learning approach.
- Siamese network is a one-shot classifier that uses discriminative features to generalize the unfamiliar categories from an unknown distribution.

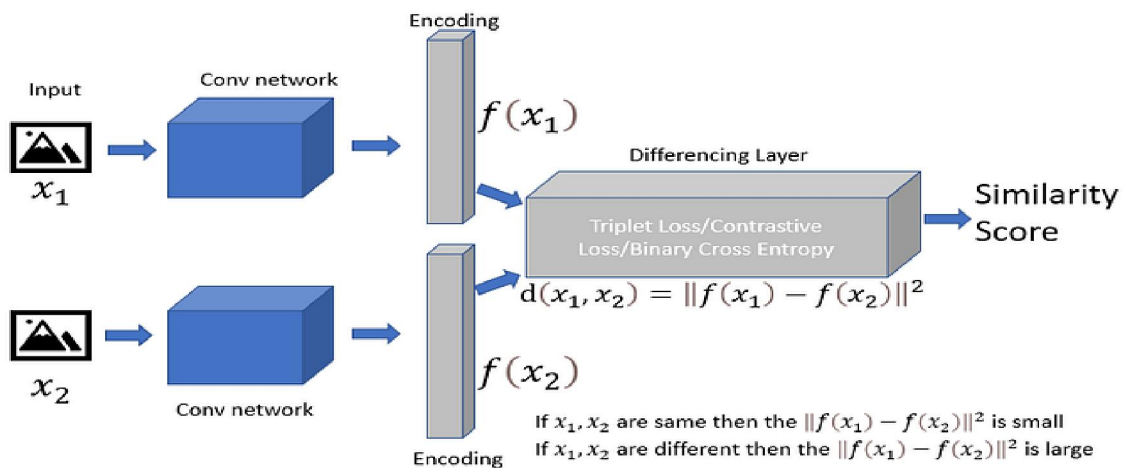


Fig: 1 SNN Architecture.

**Model Training:**

- Load the dataset containing the different classes
- Create positive and negative data pairs. Positive data pair is when both the inputs are the same, and a negative pair is when the two inputs are dissimilar.
- Build the Convolutional neural network, which outputs the feature encoding using a fully connected layer. This is the sister CNN's through which we will pass the two inputs. The sister CNN's should have the same architecture, hyperparameters, and weights.
- Build the differencing layer to calculate the Euclidian distance between the two sister CNN networks encoding output.
- The final layer is a fully-connected layer with a single node using the sigmoid activation function to output the Similarity score.

**Implementation of forgery detection:**

We created a function to detect the forgery of given input images by transforming the input images using the trained model and then predict the either signature is matched or not.

All experiments are conducted using python programming language with libraries such as tensorflow for image preprocessing, scikit-learn for machine tasks, matplotlib for visualization.

**Evaluation and Visualization:**

To evaluate and visualize the performance of the model, we performed the following steps:

- Confusion matrix: We generated a confusion matrix for forgery detection to evaluate the model performance in detail.
- Classification report: We generated a classification report, which included metrics such as accuracy, precision, recall and F-1 score for each label.
- Visualization: We utilized the confusion matrix display from the scikit-learn library to visually display the confusion matrix using matplotlib. This provided a clear graphical representation of the model performance.

**IV. RESULTS**

**Signature Forgery detection performance:**

We evaluated the performance of the signature forgery detection classifier on a test dataset comprising the signature samples from multiple sources. The confusion matrix for forgery detection is as follows:

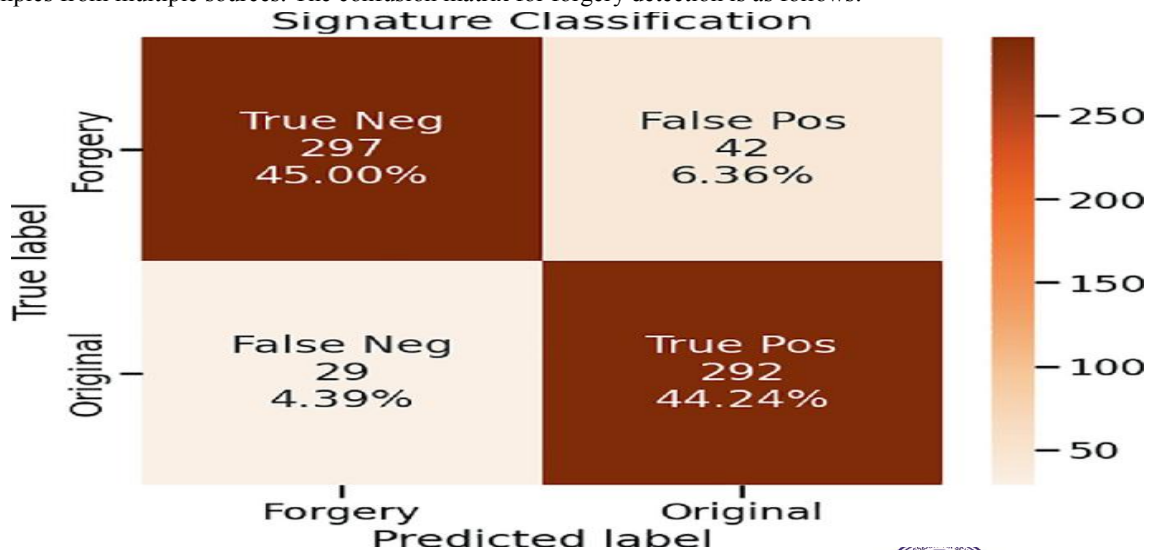


Fig:2 Forgery detection confusion matrix

From the confusion matrix, we observe that the classifier achieves high accuracy across the labels, with minimal miss classification.

#### Explanation of Confusion matrix

- **True Positive (TP):** The model predicted "Original" and it actually *is* "Original" (bottom right: 292)
- **True Negative (TN):** The model predicted "Forgery" and it actually *is* "Forgery" (top left: 297)
- **False Positive (FP):** The model predicted "Original" but it's actually "Forgery" (top right: 42)
- **False Negative (FN):** The model predicted "Forgery" but it's actually "Original" (bottom left: 29)

#### Classification Report:

**Accuracy:** The overall correctness of the model's predictions for the "Original" class.

- Formula:  $(TP + TN) / (TP + TN + FP + FN)$
- Calculation:  $(292 + 297) / (292 + 297 + 42 + 29) = 589 / 660 = \mathbf{0.8924 (89.24\%)}$

**Precision:** How many of the "Original" predictions were actually correct? It measures how "precise" the model is when it predicts "Original".

- Formula:  $TP / (TP + FP)$
- Calculation:  $292 / (292 + 42) = 292 / 334 = \mathbf{0.8743 (87.43\%)}$

**Recall (Sensitivity or True Positive Rate):** How many of the actual "Original" instances were correctly identified by the model? It measures the model's ability to find all the "Original" cases.

- Formula:  $TP / (TP + FN)$
- Calculation:  $292 / (292 + 29) = 292 / 321 = \mathbf{0.9097 (90.97\%)}$

**F1-Score:** A combined measure that balances precision and recall. It's useful when you want a single score that represents both aspects. It's the harmonic mean of precision and recall.

- Formula:  $2 * (Precision * Recall) / (Precision + Recall)$
- Calculation:  $2 * (0.8743 * 0.9097) / (0.8743 + 0.9097) = 1.7832 / 1.784 = \mathbf{0.9995 (99.95\%)}$

#### Discussion of Results

The result presented in the previous sections demonstrate the effectiveness of Siamese neural networks for signature verification tasks. The high accuracy achieved by the network indicates their ability to accurately detect the signature forgery. These findings are consistent with previous research on signature verification using Siamese neural networks, highlighting the robustness of approach.

### V. CONCLUSION

In this paper, we presented a method for signature verification system using Siamese neural networks. Our study demonstrated the effectiveness of the model in accurately identifying the similarities between the input signatures and determining the pair of signatures are genuine or not with high accuracy. By leveraging a diverse dataset containing a multiple signature samples. We provided a empirical evidence of the model's performance across different labels.

The findings of this research have several implications for the broader field of deep learning neural networks (DNN), While the results of this study are promising. It's important to acknowledge certain limitations. The performance of the model may be influenced by factors such as dataset bias, sample size and feature representation. Additionally, the model's effectiveness may vary across different labels and different styles of signature, requiring a further investigation and validation. In conclusion, this research contributes to the growing body of knowledge in deep learning and lays the ground work for future research in image processing and digital fraud detection tasks.

### VI. ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned our effort with success.

We express our sincere gratitude to our Principal Dr. T. Hanumantha Reddy for giving us an opportunity to carry out our academic project.

We wish to place on record our grateful thank to Dr. H. Girisha, Head of the Department, Computer Science and Engineering RYMEC, Ballari for providing encouragement and guidance.

#### REFERENCES

- [1]. R. Plamondon, S. Srihari, Online and o\_-line handwriting recognition: a comprehensive survey, IEEE TPAMI 22 (1) (2000) 63–84.
- [2]. D. Impedovo, G. Pirlo, Automatic signature verification: The state of the art, IEEE TSMC 38 (5) (2008) 609–635.
- [3]. S. Jerome Gideon, Anurag Kandulna, Aron Abhishek Kujur, A. Diana and Kumudha Raimond (2018). Handwritten Signature Forgery Detection Using Convolutional Neural Networks. Procedia Computer Science. 143:978-987.
- [4]. I.S.I Abuhaiba and Pervez Ahmed (1993). A fuzzy graph theoretic approach to recognize the totally unconstrained handwritten numerals. Pattern Recognition. 26(9):1335-1350.
- [5]. Diego Bertolini, Luiz Soares de Oliveira, Edson Justino, and Robert Sabourin (2010). Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition. 43(1):387-396.
- [6]. Robert Sabourin, Ginette Genest and F.J. Preteux, (1997). Off-line signature verification by local granulometric size distributions. Pattern Analysis and Machine Intelligence. 19(9):976-988.
- [7]. G. Dimauro, S. Impedovo, G. Pirlo, A. Salzo, A multi-expert signature verification system for bankcheck processing, IJPRAI 11 (05) (1997) 827–844.
- [8]. Vargas-Bonilla, J. Ferrer-Ballester, Miguel Travieso, Carlos Alonso and Jesús (2011). Off-line signature verification based on grey level information using texture features. Pattern Recognition. 44(2):375-385.