

SIGNATURE FORGERY RECOGNITION

¹Shriganesh Bhandari, ²Satyam Shukla, ³Omkar Koyande

¹Student, Computer Engineering, ²Student, Computer Engineering, ³Student, Computer Engineering

¹Prof. Sruthi Jadhav,

¹VPPCOE, Mumbai, India

Abstract: Signatures are one of the most important techniques for biometric authentication. There are two kinds of signature nowadays, offline (static) and dynamic (online). There are greater distinctive characteristics of offline signatures, but there are less distinctive characteristics of offline signatures. Offline signatures are also harder to check. Furthermore, the most significant downside of offline signatures is that even the most talented signer does not sign the same way. This is called Intra-personal variability. Both checking the offline signatures is a difficult problem for researchers. In this research, we proposed an offline signature verification approach based on the Deep Learning to prevent signature fraud by malicious individuals.

Index Terms – Offline Signature Recognition, Siamese Neural Network, , Contrastive loss, Euclidean Distance.

1) INTRODUCTION

Signature is a socially accepted and extensively used for identification of an Individual. It has an assumption that signature changes slowly and is virtually impossible to forge without detection. Increasing identification requirements and security paradigm shift have placed biometrics and particularly signature detection and verification at the center of much attention. The term biometrics refers to individual recognition based on a person's distinguishing characteristics. It has an advantage over token-based approach of not being lost over knowledge-based approach of not being forgotten. Handwritten signatures are recognized to be one of the most common techniques in establishing the identity of an individual. A good signature verification system has wide range of applications in diverse fields which include access control system, electronic fund transfer, bank operation, document analysis, etc.

Main Features of a Signature:

1. Global Features: These are extracted from the whole signature, including block codes, Wavelet and Fourier transforms. They can be extracted easily and are tough to noise. However they only deliver limited information for signature verification.
2. Local Features: These are calculated to describe geometrical characteristics such as location, tangent rack, and curving. Local features provide affluent features of writing shapes and are powerful for cultivated writers. Having said however extraction of consistent local features is still a hard problem.

Different kind of Forgeries:

The objective of signature verification system is to discriminate between two signature classes, the genuine and fake signatures. There are 3 different kinds of forgeries we generally see

1. Random Forgery: In these kinds of forgeries the person has no idea of a person's name or the style of signature.
2. Simple Forgery: These kinds of forgeries simply include imitating someone else's signature with only decent knowledge of its local features.
3. Skilled Forgeries: This is generally signed by a person who has access to a genuine signature.

2) OBJECTIVES

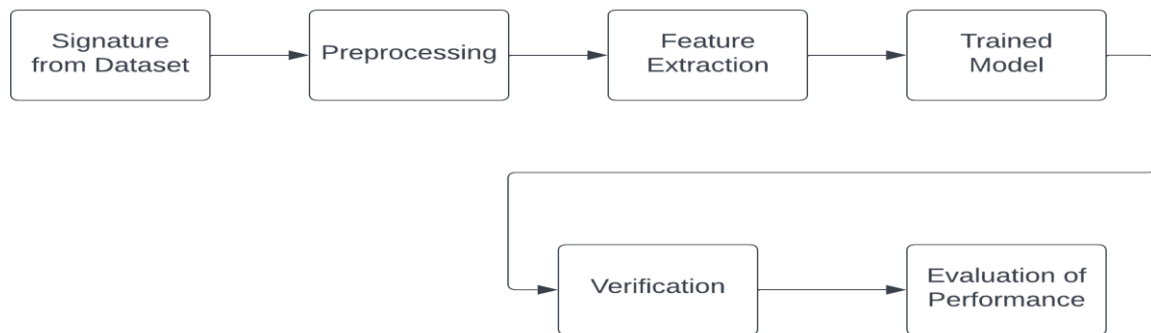
1. To develop signature recognition & verification system by artificial neural network.
2. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures.
3. To accurately characterize each user's signature, thus offering good verification and recognition performance.
4. To reduce the time required for Signature verification and recognition.
5. To maintain the Security in various financial domain such as banking, Insurance, etc.

3) EXISTING SYSTEM

Handwritten Offline Signature reputation based on biometrics, as proposed by Gulzar A. Laghari, can reliably distinguish between an imposter and a legitimate person. Biometrics is the study of an individual's behavioral and physiological characteristics. Shashi Kumar D R and K B Raja The paper proposes an offline signature verification system that combines grid and global capabilities with a neural network (SVFGNN). Signature verification function units are created by combining global and grid capabilities. Ankit Arora, Aakanksha S Chooshey Awesome characteristics (set of sections, percentage coefficient, projection, and center of gravity) were analyzed independently in the study, and the outcomes of each element were discussed. It shows how to understand offline signatures using DWT and Angular features (DOSVAF). To extract the functions, the signature is scaled and the blocks are subjected to DWT (Discrete Wavelet Rework). Nilesh Y. offered signature reputation using the Propagation Neural community once more. A fully image-based returned propagation neural network with an invariant central second and certain global residencies is suggested. Neural Networks were proposed by Odeh. It demonstrates how to utilize an MLP neural network to do offline signature verification and authenticity using four picture processing functions: eccentricity, skewness, kurtosis, and orientation. Mujahed Jarad, Nijad Al-Najdawi, and Sara Tedmori aided.

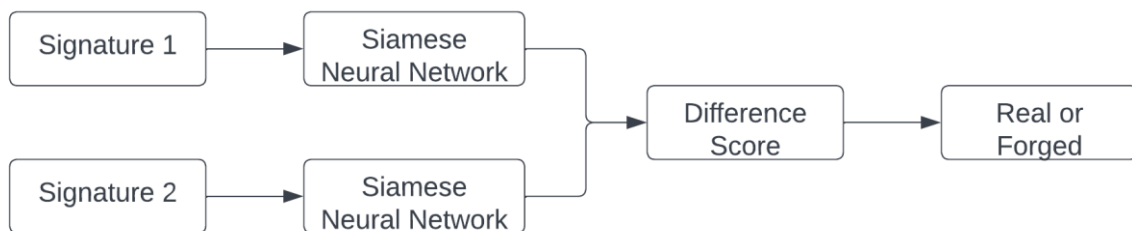
4) PROPOSED SYSTEM

1. Block Diagram



1.1 Block Diagram of the System

2. Proposed Model

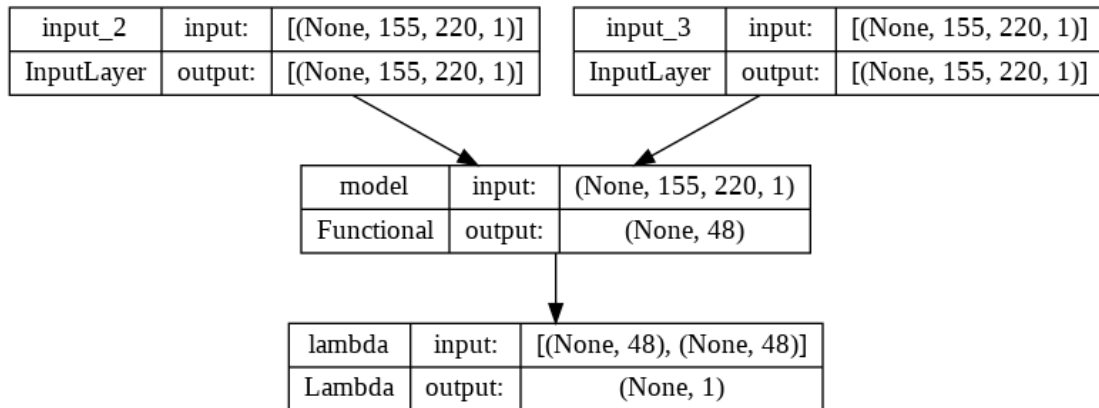


1.2 Architecture of the Signature Verification System

3. Siamese Neural Network

A Siamese neural network is a type of community architecture made up of two or more equal subnetworks. here The two CNNs are set up in the same way, with the same parameters and weights. The updating of parameters is mirrored across subnetworks. This framework has been successfully applied to dimensionality discounting and verification in weakly supervised metrics. Those subnetworks are connected at the top by a loss characteristic that computes a similarity metric based on the Euclidean distance between the characteristic representation on each facet of the Siamese community. The contrastive loss is one such loss function that is commonly used in the Siamese community.

4. Model



1.3 Model of The Siamese Network

Here the model structure takes 2 images. After that, image processing in CNN layers for feature vector. The vectors in the respective zones show the areas or signature features that are learned by the network for distinguishing between these two signatures. The feature vector is then compared by the Euclidean distance formula.

5. Layers of the Model

```

base_network.summary()

Model: "model"
-----
Layer (type)                Output Shape                Param #
-----
input_1 (InputLayer)        [(None, 155, 220, 1)]      0
conv2d_22 (Conv2D)          (None, 155, 220, 64)       320
max_pooling2d (MaxPooling2D) (None, 77, 110, 64)        0
dropout (Dropout)           (None, 77, 110, 64)        0
conv2d_23 (Conv2D)          (None, 77, 110, 64)       16448
max_pooling2d_1 (MaxPooling2D) (None, 38, 55, 64)        0
dropout_1 (Dropout)         (None, 38, 55, 64)        0
global_average_pooling2d (GlobalAveragePooling2D) (None, 64)                 0
dense (Dense)                (None, 48)                 3120
-----
Total params: 19,888
Trainable params: 19,888
Non-trainable params: 0
  
```

1.4 Layers of the Model

Convolutional Layer: Convolution is the first layer to extract features from an input image. Convolution preserves the relationship between pixels by learning image features using small squares of input data. It is a mathematical operation that takes two inputs such as image matrix and a filter or kernel.

Pooling Layer: Pooling layers section would reduce the number of parameters when the images are too large. Spatial pooling is also called subsampling or down sampling which reduces the dimensionality of each map but retains important information. Spatial pooling can be of different types:

- Max Pooling
- Average Pooling
- Sum Pooling

Max pooling takes the largest element from the rectified feature map. Taking the largest element could also take the average pooling. Sum of all elements in the feature map call as sum pooling.

Dropout Layer: The Dropout layer randomly sets input units to 0 with a frequency of rate at each step during training time, which helps prevent overfitting. Inputs not set to 0 are scaled up by $1/(1 - \text{rate})$ such that the sum over all inputs is unchanged.

Dense Layer: The Dense layers are the ones that are mostly used for the output layers. The activation used is the ‘Softmax’ which gives a probability for each class and they sum up totally to 1. The model will make it’s prediction based on the class with highest probability.

6. Metrics Used

Adaptive Estimation is a method for optimizing the gradient descent algorithm. When dealing with a large amount of data, the approach is truly green. It uses less memory and is more efficient. It’s essentially a combination of the ‘gradient descent with momentum’ and the ‘RMSP’ algorithms.

The Contrastive Loss feature is the version’s loss function. Its goal is to reduce dimensionality by learning an invariant mapping that generates high-to-low-dimensional area maps that switch similar input vectors to adjacent locations on the output manifold and different vectors to distant locations.

$$(1 - Y) \frac{1}{2} (D_W)^2 + (Y) \frac{1}{2} \{ \max(0, m - D_W) \}^2$$

1.5 Formula of Contrastive Loss

Euclidean The shortest distance between two points is represented by distance. This distance metric is used by most machine learning algorithms, including K-Means, to quantify the similarity of observations. learning rate: $1e-6$.

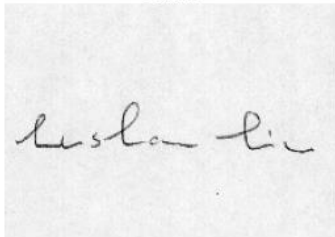
$$\sqrt{\{G_W(X_1) - G_W(X_2)\}^2}$$

1.6 Formula of Euclidean Distance

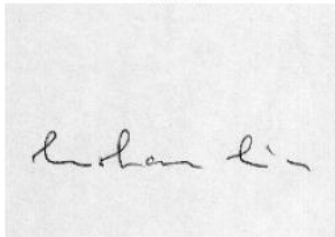
5) TEST CASES

```
[ ] predict_score()
```

Genuine

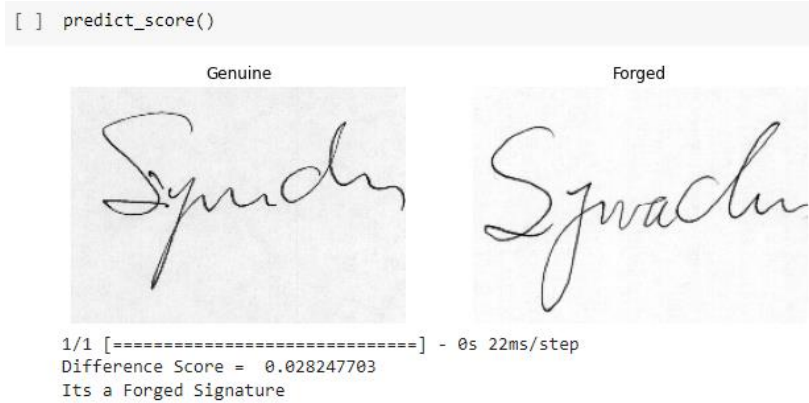


Genuine



1/1 [=====] - 0s 17ms/step
 Difference Score = 0.0053223437
 Its a Genuine Signature

1.7 Test Case 1



1.8 Test Case 2

6) Results

We have trained the model by using a dataset which consist of English signatures of the forged and original which are labeled and present in their respective folders. We trained the model for 2 epochs and the model thus generated loss function of 0.499 and an accuracy of 0.9560. As shown in the test cases, we were correctly able to predict if a signature is genuine or forged.

7) CONCLUSION

Signature Identification and verification deals with the problem of identifying and verifying signature samples from a set of samples available to us. The task of static signature verification is a difficult vision problem within the field of biometrics because signature for an individual may change depending on the psychological factors of the person. Through this project, I am trying to develop a deep learning model for offline handwritten signatures recognition which can extract high-level representations. Most of the models work well in the field only if the system can extract or create the right feature vector for a given Image. However, the task is equally difficult. Thus, we use a different kind of model in which we tend to extract high level representation of the model and thereby optimizing the feature vector required. In our project we conclusively demonstrated how we can optimize feature vector and improve upon the accuracy of the overall task. Accurate Signature verification models have a wide range of applications ranging from banking to online transactions access control systems etc.

8) REFERENCES

- [1] Neural network based offline signature recognition and verification system. Research Journal of Engineering Sciences (Shikha, P., & Shailja S)
- [2] Offline Signature Recognition and Forgery Detection using Deep Learning (Jivesh Poddara, Vinanti Parikha, Santosh Kumar Bharti)
- [3] SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification (Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Lladós, Umapada Pal)
- [4] Ciresan, Dan; Meier, Ueli; Gambardella, Luca; Schmidhuber, Jürgen (2010). "Deep big simple neural nets for handwritten digit recognition". *Neural Computation*. 22 (12): 3207–3220. arXiv:1003.0358. doi:10.1162/NECO_a_00052. PMID 20858131.
- [5] Krizhevsky, Alex; Sutskever, Ilya; Hinton, Geoffrey E. (2017-05-24). "ImageNet classification with deep convolutional neural networks" (PDF). *Communications of the ACM*. 60 (6): 84–90. doi:10.1145/3065386. ISSN 0001-0782.
- [6] LeCun, Yann. "LeNet-5, convolutional neural networks". Retrieved 16 November 2013.
- [7] Researchgate, www.researchgate.net/publication/304625369_Siganture_Verification
- [8] Shiwani Sthapak, Minal Khopade, Chetana Kashid,, Artificial Neural Network based signature, recognition and verification, *International Journal of Emerging Technology and Advanced. Engineering*, August 2013.
- [9] Offline Signature Recognition and Forgery Detection using Deep Learning, [Offline_Signature_Recognition_and_Forgery_Detection_using_Deep_Learning - ScienceDirect](http://Offline_Signature_Recognition_and_Forgery_Detection_using_Deep_Learning_-_ScienceDirect)