

Handwritten Signature Verification Using Convolutional Neural Networks

D.V.S. Abhigna^{1*}, D. Srujana², D. Hema Varshini³, G. Niharika⁴, A. Vishnu Vardhan⁵

^{1,2,3,4}Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, India

⁵Dept of Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, India

*Corresponding Author: abhigna0512@gmail.com, Tel.:8465844980

DOI: <https://doi.org/10.26438/ijcse/v7i3.5559> | Available online at: www.ijcseonline.org

Accepted: 20/Mar/2019, Published: 31/Mar/2019

Abstract— The area of Handwritten Signature Verification has been extensively investigated in the most recent decades yet remains an open research issue in image recognition. The target of signature verification is to segregate if the given signature is genuine (delivered by the guaranteed individual), or a fraud (created by an impostor). These curves describe the general shape of the signature and ignore the slight details that vary from a genuine signature to another. The verification is based on the comparison of characteristic curves by dynamic programming, which is a very powerful method for curves comparison. Much progression has been proposed in the writing in the last 5-10 years, most remarkably the use of Convolutional Neural Networks (CNN) strategies to take in highlight portrayals from signature pictures. Convolutional Neural Networks are utilized to order pictures and perform object recognition in the images. In this paper, we present how the issue has been taken care of in the previous couple of decades, discuss the ongoing progressions in the field, and the potential headings for future research.

Keywords—Forgery, Handwritten Recognition, Image Processing, Neural Networks

I. INTRODUCTION

Signature verification is a system utilized by banks, insight organizations and prominent foundations to approve the character of a person. Signature verification is often used to compare signatures in bank offices and another branch capture. A picture of a signature is nourished into the signature verification software and contrasted with the signature image on document.

Signature verification is a sort of programming that looks at signatures and checks for legitimacy. This spares time and vitality and averts human blunder amid the signature validation procedure and brings down odds of extortion during the time spent verification. The product creates a certainty score against the signature to be checked. Excessively low of a certainty score implies the signature is doubtlessly a fabrication.

Signature verification programming has now turned out to be lightweight, quick, adaptable and increasingly dependable with different alternatives for capacity, numerous marks against one ID and an enormous database. It can naturally scan for a mark inside a picture or document.

In the field of signature verification there are many solutions proposed but all the solutions have more error rate. So, in this paper, the individual signature verification can be done

by creating a neural network i.e., A Convolution Neural Network.

A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning calculation which can take in an info picture, relegate significance (learnable loads and inclinations) to different viewpoints/questions in the picture and have the capacity to separate one from the other. The pre-preparing required in a ConvNet is much lower when contrasted with other characterization calculations. While in crude techniques channels are hand-designed, with enough preparing, ConvNets can get familiar with these channels/qualities.

The design of a ConvNet is comparable to that of the network example of Neurons in the Human Brain and was propelled by the association of the Visual Cortex. Singular neurons react to upgrades just in a limited area of the visual field known as the Receptive Field. An accumulation of such fields covers to cover the whole visual zone.

Rest of the paper is organized as follows, Section I contains the introduction of Handwritten Signature Verification, Section II contain the related work of Handwritten Signature Verification, Section III contain the some measures of Handwritten Signature Verification, Section IV contain the architecture and essential steps of Handwritten Signature Verification, section V explain the Handwritten Signature

Verification methodology with flow chart, Section VI describes results and discussion Handwritten Signature Verification, Section VII contain the recommendation of Handwritten Signature Verification and Section VIII concludes research work with future directions.

II. RELATED WORK

Title: Off-Line Persian Signature Identification and Verification Based on Image Registration and Fusion

Problem Statement: Offline Persian Signature Verification

Objective: A strategy for offline Persian signature distinguishing proof and check is recommended that is based on Image Registration, DWT (Discrete Wavelet Transform) and Picture Fusion. Preparing signatures of every individual are enlisted to conquer move and scale issue. To extract features, at first, DWT is used to access details of signature; at that point a few enrolled examples of every individual signatures are melded to produce reference example of individual's signatures. In the order stage, Euclidean separation between the test picture also, each example is utilized in various sub-groups. [1].

Title: Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries

Problem Statement: Handwritten Signature Verification using HMM.

Objective: This technique reports the commitment to signature check considering distinctive forgery types in an HMM framework. The tests have demonstrated that the mistake rates of the straightforward and forgery signatures are close. This mirrors the genuine applications in which the straightforward falsifications speak to the important deceitful case. What's more, the trials show promising outcomes in talented fabrication check by utilizing basic static and pseudo-dynamic highlights. [2].

Title: Offline Signature Verification Using Pixel Matching Technique

Problem Statement: Signature Verification using Pixel Matching Technique

Objective: The proposed method is utilizing an offline signature verification and Pixel Matching Technique procedure. PMT (Pixel Matching Technique) is utilized to check the signature of the client with the example signature which is put away in the database. The proposed framework is isolated into two noteworthy stages. I. Pre-preparing, II. Confirmation

In the pre-handling there are 3 stages for refining the image. The means are Capturing Signature, Noise & Colour Removal and Adjusting properties such as Rotation(angular) and resizing

Going to the verification process, based on the percentage matched, if the rate crosses the limit esteem, at that point the signature is a genuine one else it represents to an extortion one. [3].

Title: Off-Line Handwritten Signature Identification Using Rotated Complex Wavelet Filters

Problem Statement: Signature Verification using Rotated complex wavelet filters.

Objective: In this paper, another strategy for written by hand signature recognizable proof dependent on pivoted complex wavelet channels is proposed. We have proposed to utilize the Rotated Complex Wavelet channels (RCWF) and Double Tree Complex Wavelet Transform (DTCWT) together to determine signature highlight extraction, which catches data in twelve distinct ways. In recognizable proof stage, Canberra remove measure is utilized. The proposed strategy is contrasted and Discrete Wavelet Transform (DWT). [4].

Title: Of-line signature verification by the tracking of feature and stroke positions.

Problem Statement: Offline signature verification by tracking feature and stroke positions.

Objective: In this paper, two strategies are proposed to follow the varieties. Given the set of preparing mark tests, the first strategy estimates the positional varieties of the one-dimensional projection profiles of the mark designs; and the second strategy decides the varieties in relative stroke positions in the two-measurement signature designs. The insights on these varieties are resolved from the preparation set. Given a signature to be verified, the positional removals are resolved, the validity is chosen dependent on the measurements of the preparation tests. For the motivation behind correlation, two existing strategies proposed by different analysts were executed and tried on the equivalent database. [5].

III. METHODOLOGY

In a CNN, the highlights encouraged into the last linear classifier are altogether gained from the dataset. A CNN comprises of number of layers, beginning at the raw picture pixels, which each play out a basic calculation and feed the outcome to the following layer, with the outcome being encouraged to a linear classifier. The layers' calculations depend on number of parameters which are found out through the procedure of backpropagation, in which for every parameter, the slope of the characterization loss concerning that parameter is processed and the parameter is refreshed with the objective of limiting the misfortune work. Precisely how this updated is done and what the misfortune work is are tunable hyperparameters of the system.

The design of a CNN decides what number of layers it has, what every one of these layers is doing, and how the layers

are associated with one another. Picking a good architecture is pivotal to successful learning with a CNN. For our important preparing tasks, we utilized the VGG-16 CNN architecture. This system contains an aggregate of 16 layers with learnable parameters.

These layers are of following types,

- 1) Fully connected Layer
- 2) SoftMax Nonlinearity
- 3) Convolution Layer
- 4) Dropout Layer
- 5) Max pooling Layer
- 6) Rectified Linear Unit Nonlinearity

Fully Connected Layer:

Fully connected layers apply transformation to their inputs. In a fully-connected layer, every output depends on every input according to the weight matrix W , a learnable parameter.

SoftMax Nonlinearity:

It has no learnable parameters. The SoftMax nonlinearity appears in the final layer of the neural network and computes final class scores that will be fed into the loss function or outputted during testing. Using SoftMax to compute class scores is an attractive option because of its ease of interpretation.

Convolution Layer:

Convolutional layers process an input picture by sliding various little filters over each conceivable district and yielding the dot product of the channel what's more, the picture at every region. They are like fully connected layers, yet with limitations on which input neurons are associated with which yields. Results are just associated with contributions of a little region, what not loads for each channel are integrated as opposed to being permitted to be adapted freely. The learnable parameters for a convolutional layer are the loads of each channel furthermore, one predisposition esteem for each channel. Convolutional layers loan themselves normally to comprehension of pictures, in which we frequently need to extricate includes by taking a gander at little regions of a picture, where we couldn't care less precisely where in the picture the component is. For instance, a face is yet a face in any case of where in the picture it is. Our design utilizes 3x3 channels, with more channels utilized per layer as the system gets deeper.

Dropout Layer:

Dropout layers are a non-deterministic nonlinearity utilized in numerous advanced neural systems. A dropout layer takes in various information sources and for each input sets it to 0 with probability p and leaves it unaltered with likelihood $(1-p)$. During test time, dropout layers rather act deterministically and increase all info esteems by $(1-p)$, the

normal incentive by which they were duplicated during training. The dropout esteem p is a tunable hyperparameter for the system. Dropout can be deciphered as a type of regularization, as utilizing dropout amid preparing powers the system to have numerous methods for figuring a right outcome instead of only one. This shields the system from depending too vigorously on any single association.

Max Pooling Layer:

Max pooling layers decrease the size of a picture by consolidating 2x2 areas of the contribution to a single output value. For each 2x2 area of info, the output value is essentially the maximum estimation of those 4 input pixels. This compares to handling the picture at a more elevated amount of deliberation in which highlights compare to bigger area of the info picture.

Rectified Linear Unit Nonlinearity:

REL Layers does not need any activation functions instead these layers act as the activation functions for the fully connected layers. The gradient value of these layers is very high and never tend to zero and adapts continues learning process of neurons. These layers will result in zero only when negative values are passed to these layers.

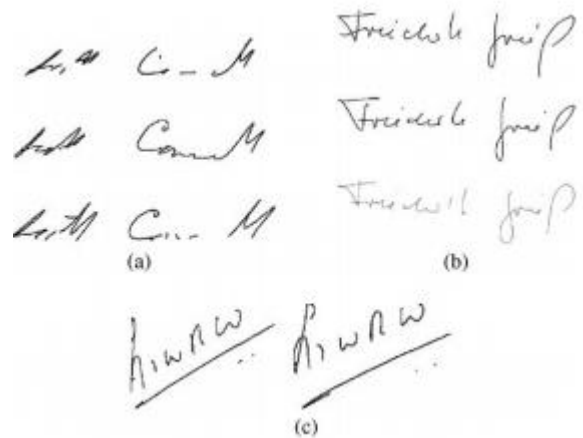


Fig1: Sample Signatures

Network Training:

After building the 16 layers of VGG architecture with the above layers. Next step leads in building the network this is obtained by sending the images to the network. For the working we take the SigComp 2011 dataset. Our dataset comes from the International Conference on Document Analysis and Recognition (ICDAR) 4N SigComp 2012 international signature verification competition. The dataset includes both online signatures. This data set has

- 25 practice signatures (Ball point Pen)
- 5 Forgeries (Ball Point Pen)
- 5 Forgeries (pencil)

Based on this, the training set and testing dataset are divided. At first the training data set is passed through the network and the related processing is done. After that the testing dataset is sent through the network.

The flow of the project is in the following way,

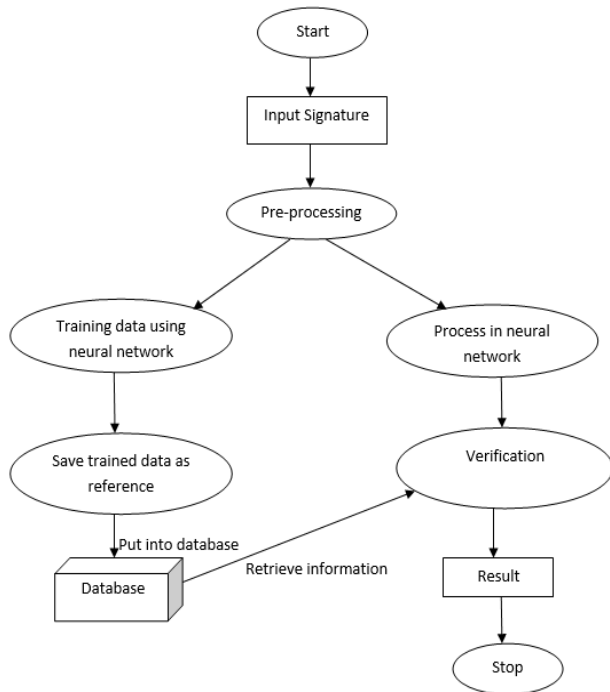


Fig2: Flow of the project

IV. RESULTS AND DISCUSSION

Based on the considered datasets, when the training set is passed through the network multiple times such that the network can establish the exact features of the signature images.

The main task is finding out whether the signature is genuine or forged. So, this can be found using acceptance rate. The acceptance rate is calculated based on the following parameters. The first parameter is total number of comparisons (**Total**) is being done and the second parameter is positive count (**PC**). If the ratio of PC and Total is more than the threshold value, then the signature is genuine one or else it is a forged one.

$$\text{Value} = \text{Positive Count} / \text{Total}$$

Based on the value obtained we can differentiate the signatures. For obtaining the most accurate results the network has been passed with training datasets multiple times.



Fig 3: Training the dataset

: 1:35 - loss: 0.7981 - acc: 0.500 - ETA: 54s - loss: 0.7450 - acc: 0.542 -
 6s - loss: 0.6551 - acc: 0.567 - ETA: 6s - loss: 0.6405 - acc: 0.605 - ETA:
 6s - loss: 0.5442 - acc: 0.729 - ETA: 6s - loss: 0.5434 - acc: 0.730 - ETA:

Fig 4.1: Result-1

```

Train on 17441 samples, validate on 7475 samples
Epoch 1/3
17441/17441 [=====] - ETA: 9:04 - loss: 0.6950 - i
Epoch 2/3
17441/17441 [=====] - ETA: 5s - loss: 0.7182 - acc
Epoch 3/3
17441/17441 [=====] - ETA: 5s - loss: 0.5591 - acc
  
```

Fig 4.2: Result-2

```

7us/step - loss: 0.6639 - acc: 0.6005 - val_loss: 0.6386 - val_acc: 0.6384
_loss: 0.5673 - val_acc: 0.7025
_loss: 0.5626 - val_acc: 0.7171
  
```

Fig 4.3: Result-3

V. CONCLUSION AND FUTURE SCOPE

We explored different avenues regarding a few minor departures from signature check undertakings. We demonstrated that convolutional neural networks work superbly of checking signatures when allowed access amid preparing to instance of certified and manufactured signatures of similar individuals whose signatures are seen at test time.

We at that point led an analysis where we tried our system on the signatures of new individuals whose signatures had not been seen at all amid preparing, bringing about execution minimal superior to a gullible gauge because of the inalienable trouble of this assignment. At long last, we professional represented a novel engineering for the correlation of signatures which has guarantee for future work in signature check, explicitly in circumstances where a perhaps produced signature can be contrasted with known authentic signatures of an underwriter.

REFERENCES

- [1] S. Ghandali and M. Ebrahimi Moghaddam, Off-Line Persian Signature Identification and Verification based on Image Registration and Fusion, In: Journal of Multimedia, volume 4, 2009, pages: 137-144
- [2] J. R. Justino , F Bortolozzi and R. sabourin , Off-line signature verification Using HMM for random, simple and skilled forgeries,ICDAR 2001, International Conference on document Analysis and Recognition, vol. 1 pp. 105-110. 2001.
- [3] Larkins, R. Mayo, M., "Adaptive Feature Thresholding for Off-Line Signature Verification", In: Image and vision computing NewZealand, 2008, pages: 1-6.
- [4] Kovari, B. Kertesz, Z. and Major, a., Off-Line Signature Verification Based on Feature Matching: In: Intelligent Engineering Systems,2007, pages 93-97.
- [5] B. Fang, C.H Leung, Y.Y. Tang, K.W. Tse, P.C.K. Kwok, and Y.K. Wong, Off-line signature verification by the tracking of feature and stroke positions, Pattern Recognition, vol. 36, pp. 91-101, 2003.