International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 4613 - 4618

Smart Forgery Detection for Signatures Using Deep Learning and Neural Networks

Sonawane Shrunkhal, P.S. Kokare, R.S. Kothe, Ghule Riya, Muskaan Mattoo
Department of E&TC, SKNCOE, SPPU, Pune
shrunkhal8380895569@gmail.com
pskokare@sinhgad.edu
rutuja.kothe_skncoe@sinhgad.edu
riaghule03@gmail.com
muskanmattoo16@gmail.com

Abstract— *Smart forgery detection for signatures using deep learning and neural networksis a system that will play an important role in authentication of an individual's signature. Hence for various security purposes, the above stated system will be useful for instance at banks, legal documentations, government organizations, investigation purposes, business, automatic data entry etc.This system is trained on Convolutional Neural Network (CNN) that works well with the data set of 300 images. CNN has been implemented in Python using Keras with TensorFlow backend. It will compare the data set images with the image (of signature) provided by the user and hence output will be predicted whether the given image is authentic or forged.This system is expected to yield an accuracy of 80-85%. Also this system is practical and accurate enough to be deployed. Hence the above stated system successfully recognizes and identifies the signature of and individual. The planned system is highly economical and its accuracy can be increased by training this model on more data set.*
Keywords— *Forgery, Authentication, Artificial Intelligence, Neural Networks*

I. Introduction

Signature verification aims to verify the identity of a person through his/her chosen signature. A signature acts as a proof of individual. Compared to physical traits such as fingerprint, iris or face, a signature typically shows higher intra-class and time variability. Furthermore, as with passwords, a user may choose a simple signature that is easy to forge. On other hand, the signature's widespread acceptance by the public and niche applications (validating paper documents and use in banking applications) make it an interesting biometric. Signature verification systems are sub categorized into two groups: Online (dynamic) and Offline (static). In offline verification process, the signature acquisition is done only after the writing process is over. Digital image is used for representation of the signature. Forgery is the act of falsification or illegal reproduction of documents and contracts including signature of a person. The range of issues of signature forgery, signature verification has come into action. It is a technique developed to differentiate forged signatures from genuine signatures. Another aspect of the difficulty in signature verification is that even the owner of the signature cannot always write it same in all respects-there would be variations in the size of the parts of the signature and the signature as a whole, variations in orientation among the components and the whole, variations in thickness and lots more of other aspects. CNN tends to produce more accurrate results. CNNs are used for image classification and recognition because of its high accuracy.The CNN follows a hierarchical model which works on building a network and finally gives out a fully-connected layer where all the neurons are connected to each other and the output is processed.

II. Literature Survey

Offline signature verification is one of most challenging areas of pattern recognition. The previous works on this type of signature verification are summarized in table below.

ISSN: 2233-7853 IJFGCN

TABLE 1: LITERATURE SURVEY

SR. NO.	PAPER NAME/STUDIES	DESCRIPTION
1.	Handwritten Signature Verification using Deep Learning by Eman Alajrami, Belal A. M.Ashqar, Bassem S. Abu-Nasser, Ahmed J. Khalil, Musleh Faculty of Information Technology, University of Palestine, Gaza, Palestine	Splitting of data in appropriate ratio to increase accuracy. 2.Plotting the training and validation accuracies. 3.Identifying major parameters of signature and and extracting them
2.	Offline Signature Recognition and Forgery Detection using Deep Learning by Jivesh Poddar, Vinanti Parikh, Santosh Kumar Bhartia (Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, India)	1. Training of Convolutional Neural Networks with the dataset of 1320 pictures. 2. Identifying various parameters of sign to extract major features of sign and train model on those parameters.
3.	Handwritten Signature Forgery Detection using Convolutional Neural Networks. Department of Computer Sciences Technology, Karunya Institute of Technology and Sciences, Coimbatore	1. Working of necessary modules from the Keras ,TensorFlow etc. 2. Python script to train the CNN with the real and forged sign as separate classes. 3. Accuracy and loss calculation.
4.	Handwritten Signature Recognition: A Convolutional Neural Network Approach Publisher: IEEE Dept. Of Electronics and Telecommunication Engineering, Sardar Patel Institute of Technology, Mumbai, India	1. Comparison of test image with multiple specimen images to improve accuracy. 2. Images preprocessing techniques to reduce noise and inaccuracies.

III. Proposed Methodology

The objective is to develop an offline handwritten signature verification system capable of differentiating between the genuine and forged signatures based on features extracted using CNN.This software can be used to validate signatures across many platforms like loans, legal document signing, application signing, applying and much more. Although signatures forgery are often manually detected by experts, still high accuracy is not always achieved. Automatic recognition systems can play an effective role in verifying signatures with high accuracy and in differentiating between genuine and forged signatures.This work focuses on off-line handwritten signature verification system using CNN approach.,reducing the complexity in traditional means of identification

Convolutional Neural Networks (CNNs) have proven successful in recent years at a large number of image processing-based machine learning tasks. Many other methods of performing such tasks

ISSN: 2233-7853 IJFGCN

revolve around a process of feature extraction, in which hand-chosen features extracted from an image are fed into a classifier to arrive at a classification decision.

Convolutional Neural Networks are commonly used for problems like signature which needs classification. The CNN architecture has a smaller number of trainable parameters which makes it better to use for this case.

.

2.1 PHASES:

1. *Data acquisition:* we have a dataset of signatures of 30 people with 5real and 5 forged signatures of each. We have 30-person real signatures and this dataset was collected from Kaggle Dataset. The total images are 300 Images (150 Real and 150 forged). All the images are in RGB format.

Fig. 1 Sample of Signature from Database

2. *Training Stage:* training stage consists of the following two steps: (1) Retrieval of a signature image from a database. (2) Neural network training.
3. *Testing Stage:* testing stage consists of following two steps: (1) Retrieval of a signature to be tested from a database (2) Checking output generated from a neural network
4. *Verification Stage:* The trained neural network is used to check whether the signature is genuine or forged. If the signature matches, then it shows genuine otherwise forgery.

2.2 Block diagram:

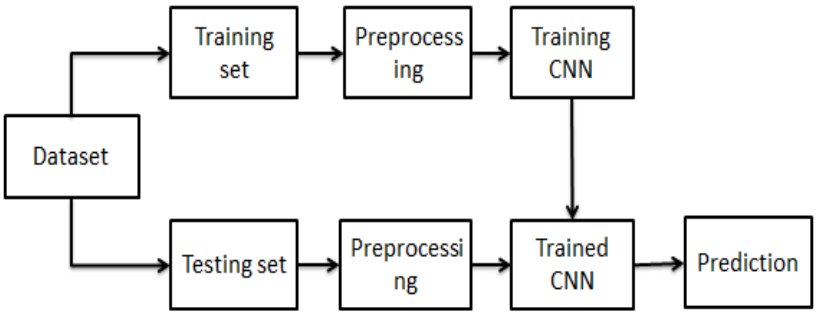

Fig. 2 Block Diagram

III. Implementation

ISSN: 2233-7853 IJFGCN

3.1 Platform features:JUPYTER NOTEBOOK is the platform used in this project. Its mostly used for features like Data visualizations,Code sharing,Live interactions with code andDocumenting code samples.

3.2 Programming language used: Python(Python 3.8) is used for the implementation of forgery detection in handwritten signatures because of the abundance of python libraries and frameworks facilitates in coding.
Libraries used: Tensorflow, Keras, Matplotlib, Numpy, Pandas, Skimage, Scikit learn etc.

3.3 Dataset : .png (images dataset), This dataset consists of English signatures both forged and original which are already present in the labelled folder.

Dataset source:https://www.kaggle.com

Here, the genuine and forged signatures are considered as two classes. The inherent properties of a handwritten signature are the main features that have to be extracted for feature space. Accordingly, the train classifiers for both the classes with the aim of finding the unique differences, using this feature space, that model the characteristics of each user.

In this work, the signature images are stored in a file directory structure which the Keras Python library can work with. Then the CNN has been implemented in python using the Keras with the TensorFlow backend to learn the patterns associated with the signatures. Then the model derived has been verified using accuracy and loss metrics to see how well the model has fit the data. Finally, the model has been tested by using a signature from a holdout set to see if the predictions are correct.

3.4 CNN Architecture:

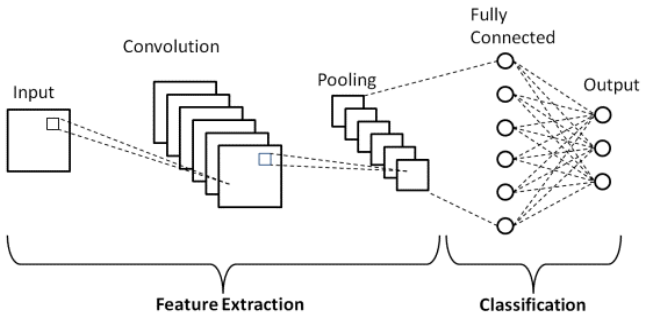

Fig. 3 CNN architecture

1. *Convolutional Layers:* They process an input image by sliding a number of small filters across each possible region and output the dot product of the kernel, i.e. the image at each region.
2. *Max-Pooling Layer:* Spatial Pooling (also called subsampling or down sampling) reduces the dimensionality of each feature map but retains the most important information. Spatial pooling can be of different types: Max, Average, Sum etc. In the case of max pooling, we define a spatial neighborhood (for example, a 2×2window) and take the largest element from the rectified feature map within the window.
3. *Fully Connected Layer:* The term “Fully connected” implies that every neuron in the previous layer is connected to every neuron in the next layer. The outputs from the convolutional and pooling layers represent high-level features of the inputimage. The

ISSN: 2233-7853 IJFGCN

purpose of the fully-connected layer is to use these features for classifying the input image into various classes based on the training dataset.

4. *Classification stage:*Over a series of epochs, the model is able to distinguish between dominating and certain low-level features in images and classify them using the Softmax Classification technique.

IV. Conclusion and Future scope

We propose an off-line handwritten signature verification method by using a single known sample and based on a deep CNN network. We ensure the reliability of theexperimental results through a series of methods, including preprocessing (removing background noise), designing controlled groups for different sample sizes and network architectures, and applying visualization techniques (to provide interpretability of the model) .

A model that can learn from signatures and make predictions as to whether the signature in question is a forgery or not, has been successfully implemented. This model can be deployed at various government offices where handwritten signatures are used as a means of approval or authentication. While this method uses CNNs to learn the signatures, the structure of our fully connected layer is not optimal

We experimented with several variations on signature verification tasks. We showed that convolutional neural networks do an excellent job of verifying signatures when allowed access during training to examples of genuine and forged signatures of the same people whose signatures are seen at test time.

We proposed a novel architecture for the comparison of signatures which has promise for future work in signature verification, specifically in situations where a possibly-forged signature can be compared to known genuine signatures of a specific signer.

We would train our model on larger datasets and allow more layers to train for more epochs. This problem would also require more time spent carefully tuning the network, which we were unfortunately unable to do for this problem.

Being able to train on a larger dataset with more signature examples per person could achieve higher accuracies, as well as training a larger network for more epochs, which we were not able to do due to time and computational resource constraints.

REFERENCE

[1] Handwritten Signature Verification using Deep Learning by Eman Alajrami, Belal A. M.Ashqar, Bassem S. Abu-Nasser, Ahmed J. Khalil, Musleh Faculty of Information Technology, University of Palestine, Gaza, Palestine.

[2] Offline Signature Verification using Deep Learning Convolutional Neural Network (CNN) Architectures GoogLeNet Inception-v1 and Inception-v3 by Jahandad, Suriani Mohd Sam, Kamilia Kamardin, Nilam Nur Amir Sjarif , Norliza Mohamed -Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia.

ISSN: 2233-7853 IJFGCN

[3] Handwritten Signature Forgery Detection using Convolutional Neural Networks by Jerome Gideon S, Anurag Kandulna, Aron Abhishek Kujur, Diana A, Kumudha Raimond.

[4] Offline Signature Recognition and Forgery Detection using Deep Learning by Jivesh Poddar, Vinanti Parikh, Santosh Kumar Bhartia (Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, India)

[5] Handwritten Signature Forgery Detection using Convolutional Neural Networks. Department of Computer Sciences Technology, Karunya Institute of Technology and Sciences, Coimbatore.

[6] Signature Verification Technique using Convolutional Neural Network Alexandra Mae C. Laylo, Mark Daryl A. Decillo, Louie Andrew F. Boo, Jeffrey S. Sarmiento International Journal of Recent Technology and Engineering (IJRTE).

[7] An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach Department of Forensic Science, Central Police University, Taoyuan 33304, Taiwan.

[8] Offline Signature Verification with Convolutional Neural Networks Gabe Alvarez galvare2@stanford.edu Blue Sheffer bsheffer@stanford.edu Morgan Bryant mrbryant@stanford.edu

[9] Handwritten Signature Recognition: A Convolutional Neural Network ApproachPublisher: IEEE Dept. Of Electronics and Telecommunication Engineering, Sardar Patel Institute of Technology, Mumbai, India.

[10] Handwritten Signature Verification Using Image Invariants and Dynamic FeaturesPublisher: IEEE Computer Science Department, Qassim University, Unaizah, Saudi Arabia

ISSN: 2233-7853 IJFGCN