IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8856

Human Signature Verification Using CNN with Tensorflow Deployment using Django Framework

Benita Merlin P[1], Santhiya G[2], Vijayalakshmi S[3]

[1] UG – Information Technology, Meenakshi Sundararajan Engineering College, Chennai, Tamilnadu

[2] UG - Information Technology, Meenakshi Sundararajan Engineering College, Chennai, Tamilnadu

[3] Assistant Professor - Information Technology, Meenakshi Sundararajan Engineering College, Chennai, Tamilnadu

ABSTRACT

The traditional function of a signature is to permanently affix to a document in which a person's uniquely personal, undeniable self-identification is used as physical evidence of that person's personal witness and certification of the content of all, or a specified part of the document. One of the most important biometric authentication techniques is signature. Every person has his/her own signature which is unique and is used mainly for the purpose of personal identification and verification of important documents or legal transactions. There are two kinds of signature verifications. They are: static and dynamic. Static (off-line) signature verification is the process of verifying an electronic or document signature after it has been made by the person, while dynamic (on-line) signature verification takes place as a person creates his/her signature on a digital tablet or a device.

The main objective of human signature verification is to prevent signature fraud by malicious people. Online signatures have many distinctive features whereas offline signatures have lower distinctive features. So offline signatures are more difficult to verify. Offline signature verification is not very efficient and is slow for a large number of document verification.

The proposed system is to overcome the drawbacks of offline signature verification. We have proposed a Deep Learning (DL) based offline signature verification method using tensorflow to verify whether the signature is genuine or forged. The Deep Learning method used in our study is the Convolutional Neural Network (CNN). It is predicted that the success of the obtained results will increase if the CNN method is supported by adding extra feature extraction methods and classify successfully the human hand signature. After the completion of training and validation of the CNN model, the accuracy of the testing is checked.

Keywords: Signature, Deep learning, Tensorflow, CNN

1. INTRODUCTION

To detect the human hand signature, we planned to design deep learning technique so that a person with lesser expertise in software should also be able to use it easily. The proposed system is to predict whether the human hand signature is forged or genuine. Samples of more number of images are collected that comprises of different classes such as Genuine and Forged signatures. Different number of images are collected for each classes that was classified into input images. we proposed a Deep Learning (DL) based offline signature verification method to prevent signature fraud by malicious people. The Deep Learning (DL) method used in the study is the Convolutional Neural Network (CNN). It is predicted that the success of the obtained results will increase if the CNN method is supported by adding extra feature extraction methods and successfully classify the human hand signature.

The system of human signature verification works on Deep learning algorithm which contains several "layers" of neural

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.8856

network algorithms, in which signatures passes through each layer giving a simplified representation of the data to the next layer. Most of the machine learning algorithms work well on the datasets which have up to a few hundred features. However, an unstructured dataset that is an image has a large number of features that this process becomes cumbersome or completely unfeasible. The Deep learning algorithm learns progressively more about the image of the signatures as it goes through each of the neural network layer. The result of the signature which is real or forged is found on the final output layer and displayed on the screen.

2. PROPOSED SYSTEM

The handwritten signature is a behavioral biometric which is not based on any physiological characteristics of the individual signature but on the behavior that changes over time. Since an individual's signature alters over time, the verification and authentication for the signature will take a long period of time which also includes the errors to be higher in some cases. Inconsistent signatures may lead to higher false rejection rates for an individual who did not sign in a consistent way.

The proposed system is to predict the human hand signature identification. Samples of more number of images are collected that comprised of different classes such Genuine and Forged signatures. Different number of images of the signatures are collected for each class which is classified into input images. In our project we have proposed a Deep Learning (DL) based offline signature verification method which is used to prevent signature fraud by malicious people. The Deep Learning method used in our proposed system is the Convolutional Neural Network (CNN). It is predicted in our system that the success of the obtained results will increase if the CNN method is supported by adding extra feature extraction methods and there will be successful classification of human hand signatures.

2.1 Training from Scratch

To train a deep learning network from scratch, we have gathered a very large number of data sets categorized as genuine and forged. After collecting the datasets, a design of network architecture which learns the features from the signatures is build and a model is created. For some new applications, or for the applications that has very large amount of output categories, this model will work well.

2.2 Transfer Learning

The Deep learning algorithms use transfer learning approach, a process that involves fine-tuning of the pre-trained model of signatures. Our project uses an existing network, such as AlexNet or GoogLeNet, and using that we feed in new data containing two classes of signatures such as real and forged. After making some tweaks to the network, we perform a new task, which is categorizing only the features of the signatures rather than other objects. This has an advantage of needing only less number of data (processing thousands of images, rather than millions) of signatures, so that the computation time will drop to minutes or hours.

2.3 Feature Extraction

A slightly less common and the more specialized approach of deep learning is to use the network as a feature extractor. Since all the layers in the deep learning model are tasked with learning certain features from images, we can pull these features out of the network at any time during the training process. The features extracted can also be used as input to a machine learning model such as support vector machines (SVM).

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.8856

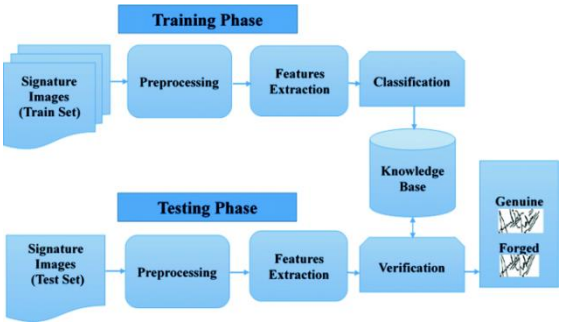

Fig. 1. Phases of human signature verification

2.4 Modules

Import the given image from dataset and training manual CNN
We have to import our data set using keras preprocessing image data generator function also we create size, rescale, range, zoom range, horizontal flip. Then we import our image dataset from folder through the data generator function. Here we set train, test, and validation also we set target size, batch size and class-mode from this function we have to train.

To train the module by using AlexNet
To train our dataset using classifier and fit generator function also we make training steps per epoch's then total number of epochs, validation data and validation steps using this data we can train our dataset. Training the module using AlexNet CNN.

To train the module by using LeNet
A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning algorithm which takes an image as input, assigns importance (learnable weights and biases) to various features in the image of the signature and be able to differentiate one signature from the other.

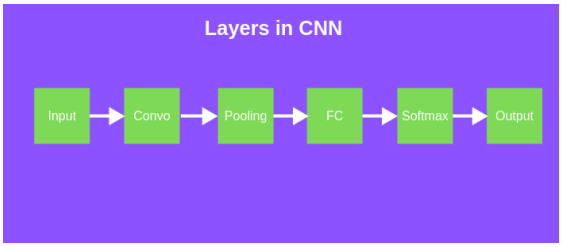

Fig. 2. Layers in Convolution Neural Network

Deploying the model in the django framework and predicting the result
In this module the trained deep learning model is converted into hierarchical data format file (.h5 file) which is then deployed in our django framework for providing better user interface and predicting the output whether the given signature is real or forged.

3. IMPLEMENTATION AND RESULT ANALYSIS

3.1 Data Acquisition

Handwritten signatures are collected and some unique features of the signatures are extracted to create knowledge base for each and every individual. A standard database of both real and forged signatures for every individual is needed for evaluating the performance of the signature verification system and also for comparing the results obtained using the other techniques on the same database.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.8856

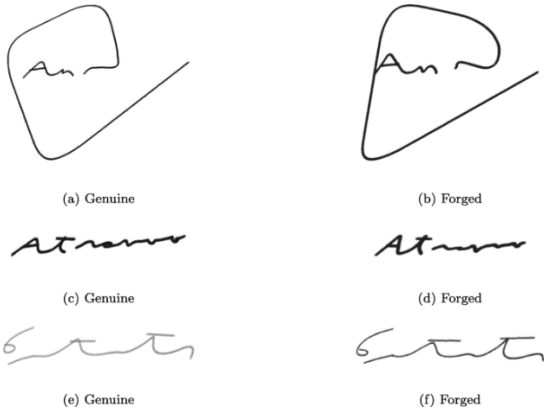

Fig. 3. Genuine and Forged Signatures

3.2 Pre-Processing

All the signatures are scanned in gray. The purpose of this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves the quality of the signatures and makes it more suitable for the extraction of features. The prepossessing stage includes a gray scale signature image which is converted to binary to make feature extraction simpler. The signatures obtained from signature are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256*256.

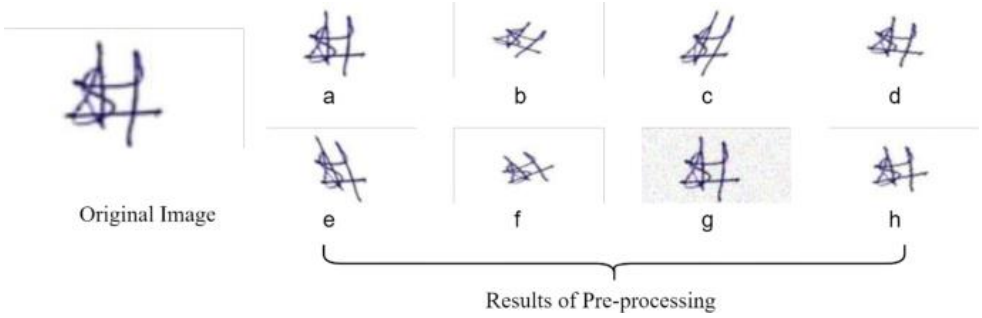

Fig. 4. Pre-Processing of Signatures

3.3 Classification

Each image of the signature goes through a series of convolution and max pooling layers which are in an alternating fashion. When every image of the signature goes through the convolution process, a predefined number of feature maps are created which are fed into a max pooling layer and it creates pooled feature maps from the feature maps received from the convolution layer which is placed before it. This pooled feature map is sent into the next convolution layer and this process will be continued until it reaches the fourth max pooling layer. The pooled feature map received from the last max pooling layer is flattened and sent into the fully connected layers. After several rounds of forward and backward propagation, the model will be trained and a prediction of signature whether it is real or forged can be made.

3.4 Overall Result

After training the images of the signatures using CNN, the database consisting of the signatures are tested and the result displays whether the corresponding signature is genuine or forged.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8856

Fig. 5. Sample output generated

CONCLUSION AND FUTURE WORK

Convolutional Neural Networks are a very strong and efficient algorithm that may be implemented on an embedded device. The aforementioned tests can be used to verify the algorithm's efficacy. The results of all of these tests are remarkably similar. According to algorithm tests, the training of signature datasets acquired from various angles is a critical parameter to consider. This intelligent human signature verification system will assist the people in making the most secure and efficient use of their signatures.

The future work for the project would be to deploy the human hand signature verification model to artificial intelligence on web applications.

REFERENCES

1. Bharadi, V. A. & Singh, V. I. (2014), `Hybrid Wavelets based Feature Vector Generation from Multidimensional Data set for On-line Handwritten Signature Recognition', 5th International Conference- Conuence The Next Generation Information Technology Summit (Conuence pp. 561-568).

2. Chang, H., Dai, D.,Wang, P. & Xu, Y. (2012), `Online Signature Verification Using Wavelet Transform of Feature Function Architecture of an Online Signature Verification System', 11(2011), 3135-3142.

3. Fernandes, J. & Bhandarkar, N. (n.d.), `Enhanced online signature verification system', International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November - December 2014 , pp. 205-209 , ISSN 2278-6856.

4. Fierrez-aguilar, J., Krawczyk, S., Ortega-garcia, J. & Jain, A. K.(2005), `Fusion of Local and Regional Approaches for On-Line Signature Verification', Iwbrs 2005 LNCS 3781, 188-196.

5. Hafemann, L. G., Sabourin, R. & Oliveira, L. S. (2017), `Learning features for online handwritten signature verification using deep convolutional neural networks', Pattern Recognition 70, 163-176.

6. Iranmanesh, V., Ahmad, S. M. S., Adnan, W. A. W., Yussof, S., Arigbabu, O. A. & Malallah, F. L. (2014), `Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis', The Scientific World Journal 2014, 1-9.

7. Jain, A. K., Ross, A. A. & Nandakumar, K. (2011), Introduction, in `Introduction to Biometrics', Springer, pp. 1-49.

8. Kaur, M. R. & Choudhary, M. P. (2015), `Handwritten Signature Verification Based on Surf Features Using Hmm', 3(1), 187-195.

9. Khalil, M., Moustafa, M. & Abbas, H. (2009), `Enhanced DTW based on-line signature verification', Image Processing (ICIP), 2009 16th IEEE International Conference on pp. 2713-2716.

10. Liu, Y., Yang, Z. & Yang, L. (2015), `Online signature verification based on dct and sparse representation', IEEE transactions on cybernetics 45(11), 2498-2511.

11. Nagbhidkar, K. P. & Bagdi, P. V. (2015), ` Online Signature Verification on smart phone using discrete wavelet transforms .', 2(2), 1-6.

12. Nanni, L., Maiorana, E., Lumini, A. & Campisi, P. (2010), `Combining local , regional and global matchers for a template protected on-line signature verification system', Expert Systems With Applications 37(5), 3676-3684.
URL: http://dx.doi.org/10.1016/j.eswa.2009.10.023

13. Parodi, M. & Gomez, J. C. (2014), `Legendre polynomials based feature extraction for online signature verification. Consistency analysis of feature combinations', Pattern Recognition 47(1), 128-140.
URL: http://dx.doi.org/10.1016/j.patcog.2013.06.026

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8856

14. Plamondon, R., Pirlo, G. & Impedovo, D. (2014), Online signature verification, in `Handbook of Document Image Processing and Recognition', Springer, pp. 917-947.

15. Plotz, T. & Fink, G. a. (2009), `Markov models for offline handwriting recognition: A survey', International Journal on Document Analysis and Recognition 12, 269-298.

16. Rua, E. A. & Castro, J. L. A. (2012), `Online signature verification based on generative models', IEEE Trans. Syst., Man, Cybern. B, Cybern 42(4), 1231-1242.

17. Saffar, M. H., Fayyaz, M., Sabokrou, M. & Fathy, M. (2018), `Online signature verification using deep representation: A new descriptor', arXiv preprint arXiv:1806.09986 .

18. Sharma, A. & Sundaram, S. (2016), `An enhanced contextual dtw based system for online signature verification using vector quantization', Pattern Recognition Letters 84, 22-28.

19. Thumwarin, P., Pernwong, J. & Matsuura, T. (2013), `FIR signature verification system characterizing dynamics of handwriting features'. **URL**: http://asp.eurasipjournals.com/content/2013/1/183

