DEEP FORGERY DETECTOR

A.DURGA GOWRI SANKAR[1], N.NEERAJA PRIYA[2], S.VAMSI PRASANTH[3], V.MANI KUMAR[4]
[1,2,3,4] IV B.Tech, Department of CSE, JNTUK-UCEV, Vizianagaram, AP, India.

Abstract: ***Signature validation is an important biometric technique that aims to detect whether a given signature is forged or genuine. It is essential in preventing falsification of documents in numerous financial, legal, and other commercial settings. The human resources required to process and verify the innumerable transactions that occur on a daily basis is no longer an option. The automation of signature validation is not just to verify but to detect fraud. Automated Signature validation is a solution for efficient and fast validation of the signature that is a must to offer the best. There are multiple ways to automate the process of signature validation. The performance of traditional ways like Fuzzy models, Hidden Markov models are still far from optimal when we test the systems against skilled forgeries - signature forgeries that target a particular individual. Moreover it is a time and effort consuming process since the features need to be extracted after processing an image. The current best approach is to use Deep Learning. Our work aims to automate the process of signature validation by using Deep Convolutional Neural Networks. This reduces the need of feature extraction and once a modal is trained, we can supply the raw signatures as input which helps in obtaining fast and effective results.***

Keywords: Signature validation, Fuzzy models, Hidden Markov models, Feature Extraction, Deep Convolutional Neural Networks

1. INTRODUCTION

Signatures have been considered a typical form of authentication in our society for hundreds of years. Signature verification is the most natural and friendly approach in personal authentication for many biometric-based verification systems. Signature, derived from the Latin word "Signare" (meaning "Sign"), is a stylized handwritten representation of a person's name or an identification mark that a person writes on documents/texts. A signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Signatures are learnt and acquired over a period of time rather than being a physiological characteristic, and are influenced by the physical and emotional conditions of a subject. Signature is a sign as a symbol of the name written by the hand and by the person himself as a personal marker.

A signature verification system must be able to detect forgeries, and, at the same time, reduce rejection of genuine signatures. Handwritten signature verification is a challenging task as the possibility and easiness of forging one's signature is very high. Signatures are often used in data verification either in schools, banks, corporations, hospitals, government, and much more. Due to the importance of signature function, there are many parties who want to manipulate the signatures of others. Forgeries can be of different types based on the details accessible or available to the forger. Duplicate signatures can be detrimental and included in the criminal realms. The inevitable side-effect of signatures is that they can be exploited for the purpose of feigning a document's authenticity. Hence the need for research in efficient automated solutions for signature recognition and verification has increased in recent years to avoid being vulnerable to fraud. In signature verification, forged signatures can be broken up into three different categories. These categories are based on how similar a forgery is in relation to the genuine signature and are known as random, simple and skilled. In random forgery the forger does not know the signer's name or signature shape. In simple forgery or unskilled forgery, the forger knows the name of the original signer but not what his signature looks like. While in skilled forgery, a close imitation of the genuine signature is produced by a forger who has seen and practiced writing the genuine signature. It is these skilled forgeries that this paper will focus on for signature verification.

Analysis of signatures based on the method used to capture the signatures is divided into two main categories; offline and online. In offline verification, the signature patterns are signed on paper, and then scanned by plate-form scanners whereas in online systems we use pressure sensitive tablets, cameras etc. Online data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time.

Online systems use these data captured during acquisition. Online systems could be used in real time applications like credit cards transaction or resource access. While off-Line signature verification systems take as input the 2-D image of a signature. Offline systems are useful in automatic verification of signatures found on bank checks and documents. A robust system has to be designed

which should not only be able to consider these factors but also detect various types of forgeries.

2. RELATED WORK

In [1], they presented a simple and efficient approach to on-line signature verification, based on a discrete cosine transform, which has been applied to 44 time signals, such as position, velocity, pressure and angle of pen. Experiments are carried out on two benchmark databases, SVC2004 and SUSIG. The forward feature selection algorithm is used to search for the best performing feature subsets. The proposed system is tested with different classifiers, with skilled forgery, and equal error rates were 3.61%, 2.04% and 1.49% for SVC2004 Task1&2, Task2 and SUSIG databases, respectively. In [2], they proposed a system based on comparing signature image pixel by pixel with the original signature image. In this method, the image is first preprocessed (noise removal and orientation) and then matched with the actual image. The FAR and TAR of the system are 0.06 and 0.94 respectively. One of the main disadvantages of this system is the system can only identify static changes in the signature.

[3] This system is composed of two phases. They are enrollment and verification. In enrollment phase, the signature is acquired from a tablet and stored in Blob Storage along with its feature vector which is extracted by Worker Role. In the verification phase, the signature vector extracted by the worker role is compared with existing feature vector in Blob Storage. Success rate is about 92.5%. And the system is highly scalable as is it a SaaS (Software as a Service).

In [4], they presented a method for Offline Verification of signatures using a set of simple shape based geometric features. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The artificial neural network (ANN) was used to verify and classify the signatures: exact or forged, and a classification ratio of about 93% was obtained under a threshold of 90%.

[5] Their project aims to automate the process of signature verification by using convolutional neural networks (CNNs). Their model is based on the VGG16 architecture, and they used the ICDAR 2011 SigComp dataset to train their model with transfer learning. When classifying whether a given signature was a forgery or genuine, they achieved accuracies of 97% for Dutch signatures and 95% for Chinese Signatures. They also performed several experiments altering the types of training data and prediction task to make it more relevant to real-life applications, for which their methods seem promising but for which they were not able to achieve results much higher than a naive baseline.

[6] This project aims to propose an offline signature and verification system which employed an efficient fuzzy Kohonen clustering networks (EFKCN) algorithm. The recognition of signature patterns using the clustering method with the EFKCN algorithm shows relatively better result with 70% accuracy compared to the accuracy of previous research results 2 which is 53%.

In [7], an automatic signature verification system has been proposed. This work focuses on both online and offline features of handwritten signatures and aims at combining their results to verify the signature. The online and offline method verifies the signature separately and finally their results are combined and the signature is verified using SVM.

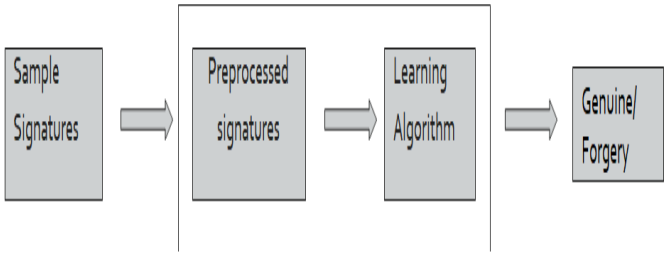


Fig.1.Proposed System Architecture

The architecture of the convolutional neural network created is shown in Fig.1. It contains three convolution layers combined with ReLU and pooling layers. Even though there are several existing models, we chose to create our own model.

3. METHODOLOGY

The CNN has developed to detect signature forgery. It contains three convolution layers combined with ReLU and pooling layers. Convolution Layer (C1): Number of filters:32, Size of filter=3x3; a Pooling Layer(S1): Max Pooling with size 2x2; another convolution Layer (C2): Number of filters:32, Size of filter=3x3; second pooling Layer(S2): Max Pooling with size 2x2; third convolution Layer (C3): Number of filters:64, Size of filter=3x3; third pooling Layer(S3): Max Pooling with size 2x2; With no padding and a stride of 1, the output size will be (n-f+1)*(n-f+1)*nf, Where nf is the number of filters, n is the size of the image, f is the size of the filter. Batch-size represents number of images we are giving at a time. It influences the speed and performance and we need to tune it. Smaller batch size means more updates in one epoch. Larger batch size yields more efficient computation however, it can yield worse performance. Batch-size used for training is 16.

Dropout consists in randomly setting a fraction rate of input units to 0 at each update during training time, which helps prevent overfitting. rate: float between 0 and 1. Fraction of the input units to drop. The noise_shape representing the shape of the binary dropout mask that will be multiplied with the input.

After training the CNN model with train database we obtain parameters i.e., weights and biases that are required to classify the images into respective classes. Since training time is very long we need to save these weights so that we can use later during testing phase. Model parameters are stored into hard disk. During testing phase we load the parameters from hard disk and use it on the test database or test image which classifies the images into correct classification.

The data we are dealing with is crowd sourced and hence vary widely. This brings the need for the preprocessing of data. We need to rescale the datasets in such a way that they are of equal sizes. In this case, we are providing a document with highlighting a region for keeping the signature. This will be cropped according to the predefined positions and then down sampling is applied and is normalized.

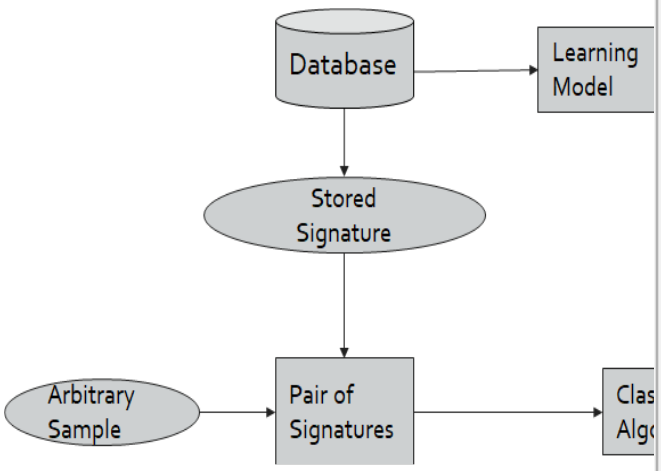


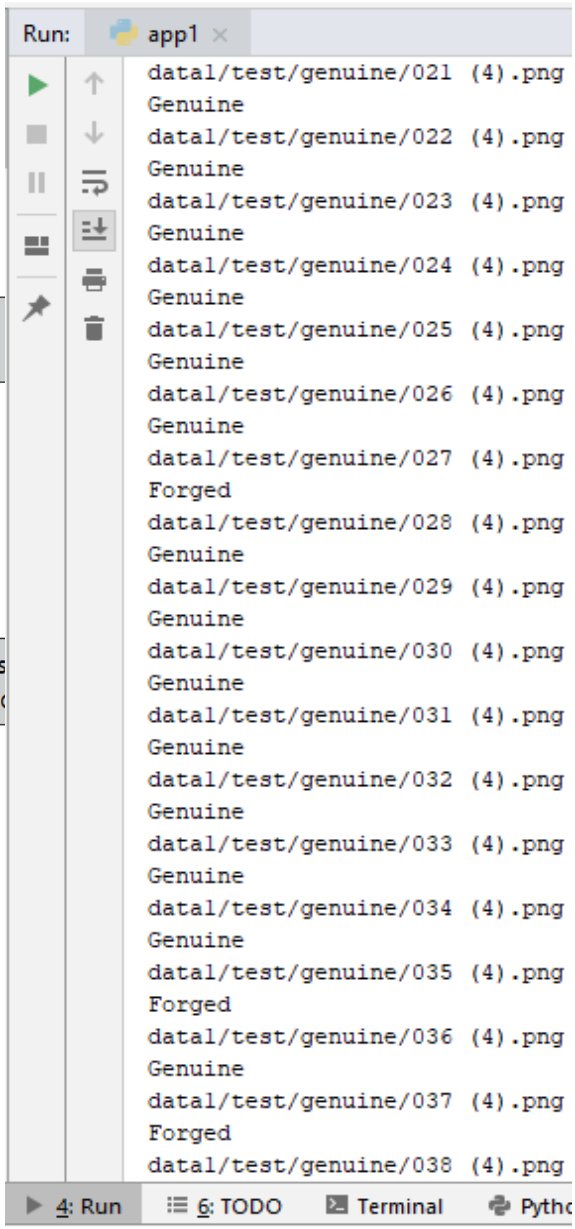
Fig.2.System Flow

4. EXPERIMENTAL RESULTS

In order to classify whether a given signature is genuine or forged there must be base to check and this base is the images of the signatures that are signed by the individuals. We have taken the data set from one of the Kaggle competitions.

The CNN model developed for signature forgery detection is trained for 50 epocs initially and then tested on genuine and forged signatures. We got 88.8% accuracy. After retraining model for 50 epocs 92.7% training accuracy and 88.2% accuracy. In this work we used 50 epochs two times with a batch size 16 and number of training images 264 with data augmentation.

The results for pair of genuine signatures are shown in fig 3(a) & (b). And the results for pair of forged signatures are shown in fig 4(a) & (b). The results shows that the system developed detects forged signatures and also identifies whether the signatures are genuine or not efficiently with an accuracy of 92.7% on large database.



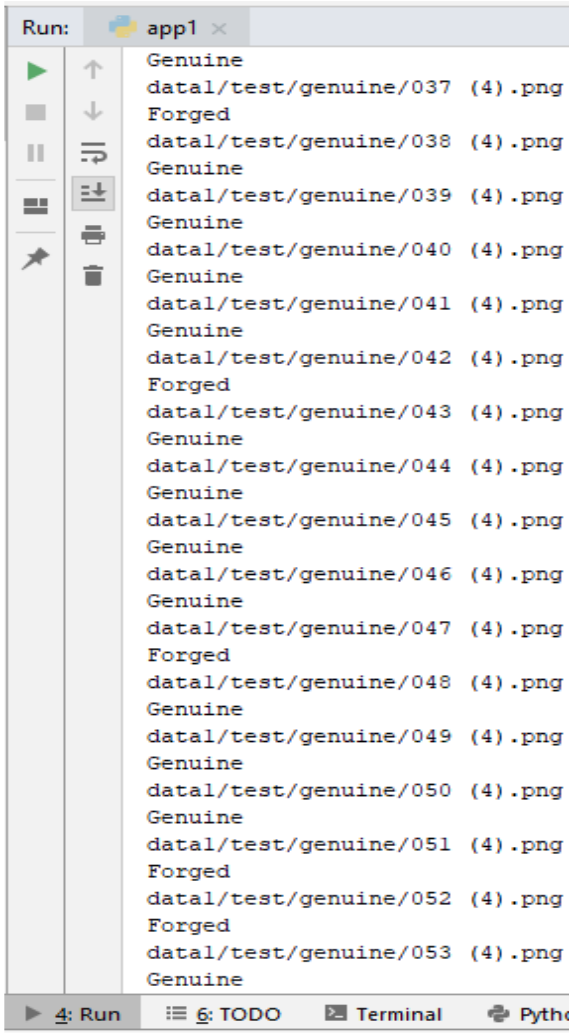
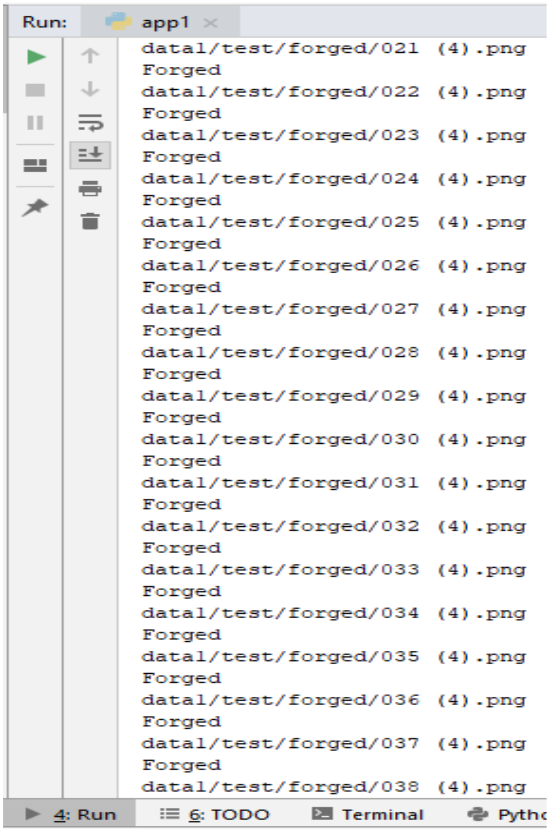


Fig.3 (a) and (b) Test results for genuine signatures

5. CONCLUSION

Although signature verification is not one of the safest biometric solutions, the use of it in business practices is still justified. Moreover, signature verification has a very promising future. One major drawback is that humans are not consistent when signing their signatures. The same signature pattern of respondents may differ depending on the condition of the signature so as to allow an error in the recognition of the signature pattern. Here, we proposed a robust signature verification system, based on Deep Convolutional Neural Networks. The system is robust as it can detect random, simple and semi-skilled forgeries. Being a self-optimized CNN model, it fetched a training accuracy of 92.7% and testing accuracy of 88.2%.



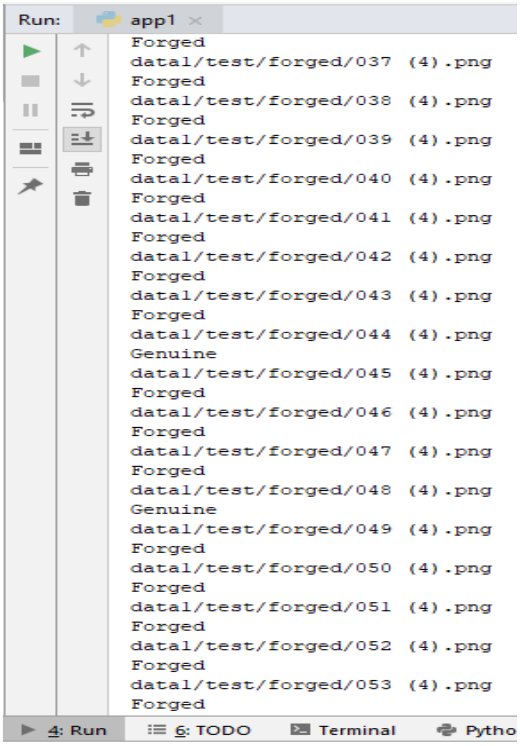


Fig.4 (a) and (b): Test results for forged signatures

REFERENCES

[1] Deep learning community. http://deeplearning.net/tutorial/
[2] Documentations from keras.io and www.tensorflow.org
[3] Yoshua Bengio, Ian J. Goodfellow, and Aaron Courville. Deep learning. Book in preparation for MIT Press, 2015
[4] CNN Tutorial- https://medium.com/@RaghavPrabhu/understanding-of-convolutional-neural-network-cnn-deep-learning-99760835f148
[5] CS231n Convolutional Neural Network for Visual Recognition - http://cs231n.github.io/convolutional-networks/
[6] Y. Bengio, "Learning Deep Architectures for AI," Foundations and Trends in Machine Learning, vol. 2, no. 1, pp. 1–127, Jan. 2009.
[7] A. Dhawan and A.R. Ganesan "Handwritten Signature Verification " ECE 533 - Project Report The University of Wisconsin Madison 2005.
[8] Beatrice Drott, Thomas Hassan-Reza, "On-line Handwritten Signature Verification using Machine Learning Techniques with a Deep Learning Approach", E:40 Master Thesis, The Faculty of Engineering at Lund University, LTH, 16 September 2015.
[9] E. J. Justino, A. El Yacoubi, F. Bortolozzi, and R. Sabourin, "An off-line signature verification system using HMM and graphometric features", in Fourth IAPR International Workshop on Document Analysis Systems (DAS), Rio de. Citeseer, 2000, pp.211222.

[10] A. Pansare and S. Bhatia "Handwritten Signature Verification using Neural Network " IJAIS - ISSN: 2249-0868 Vol. 1 - No. 2 pp. 44-49 January 2012.
[11] Ahmed, H., Shukla, S., Rai, H.M., Static Handwritten Signature Recognition Using Discrete Random Transform and Combined Projection Based Technique. In: 2014 Fourth International Conference on Advanced Computing Communication Technologies. 2014, p. 37–41. doi: 10.1109/ACCT.2014.76.