Signature Recognition and Verification Using Machine Learning Softmax Regression Model

Rajesh Vemulakonda
Assistant Professor
Department of CSE
P V P Siddhartha Institute of Technology, Kanuru, Vijayawada
vrajesh@pvpsiddhartha.ac.in

Venkata Ramana Gupta Nallagattla
Assistant Professor
Department of CSE
Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada
nallagattla@gmail.com

Abstract

In today s world forgery of signature is very widely increased. There are many “ “ sophisticated scientific techniques to identify a correct signature. As signatures are widely accepted biometric for authentication and identification of a person because every person has a distinct signature with its specific behavioural property, so it is very much necessary to prove the authenticity of signature itself. A huge increase in forgery cases relative to signatures induced a need of Signature recognition system. However human signatures can be handled as an image and recognized using computer vision and neural network techniques. In this paper we have taken a set of trained images and stored their features in a database and to test an unknown image we compare the features and calculating the matching factors. We have considered 70 % as threshold for human signature recognition. Regarding creation of recognizer we gave considered HARRIS and SUFR Features. efficient “Signature Verification System.

Keywords: *SRVS, AI&ML, CNN, Softmax regression model.*

Introduction

Machine learning is the study of computer algorithms that improve automatically through experience and by the use of data. It is seen as a part of artificial intelligence. Machine learning algorithms build a model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of applications, such as in medicine, email filtering, and computer vision, where it is difficult or unfeasible to develop conventional algorithms to perform the needed tasks. features like textures and shapes, a CNN takes just the image's raw pixel data as input and "learns" how to extract these features, and ultimately infer what object they constitute.

Machine learning involves computers discovering how they can perform tasks without being explicitly programmed to do so. It involves computers learning from data provided so that they carry out certain tasks. For simple tasks assigned to computers, it is possible to program algorithms telling the machine how to execute all steps required to solve the problem at hand; on the computer's part, no learning is needed. For more advanced tasks, it can be challenging for a human to manually create the needed algorithms. In practice, it can turn out to be more effective to help the machine develop its own algorithm, rather than having human programmers specify every needed step.

The discipline of machine learning employs various approaches to teach computers to accomplish tasks where no fully satisfactory algorithm is available. In cases where vast numbers of potential answers exist, one approach is to label some of the correct answers as valid. This can then be used as training data for the computer to improve the algorithms it uses to determine correct answers. For example, to train a system for the task of digital character recognition, the MNIST dataset of handwritten digits has often been used[1][2].

The problem of automatic handwritten signature verification is commonly modeled as a verification task: given a learning set L, that contains genuine signatures from a set of users, a model is trained. This model is then used for verification: a user claims an identity and provides a query signature Xnew.

The model is used to classify the signature as genuine (belonging to the claimed individual) or forgery (created by someone else). To evaluate the performance of the system, we consider a test set T, consisting of genuine signatures and forgeries. The signatures are acquired in an enrollment phase, while the second phase is referred to operations (or classification) phase[3][4].

A signature recognition and verification (SRVS) is a system capable of efficiently addressing two individual but strongly related tasks –

(a) Identification of the signature owner

(b) Decision whether the signature is genuine or forger. Depending on the actual needs of the problem at hand, SRVSs are often categorized in two major classes: on-line SRVSs and offline SRVSs. While for systems belonging to the former class, only digitized signature images are needed, for systems in the latter classes'. Information about the way the human hand creates the signature such as hand speed and pressure measurements, acquired from special peripheral units, is needed.

Related Work

In the existing system, they need only one pre-given signature to verify whether the given input signature is a true one or not. Here comes the first disadvantage where if they use a single signature let's assume that the user may be in a hurry and he signed it in a hurry sometimes that lead to improper or imperfect signatures so in this condition this system fails to compare them perfectly whereas in our system it takes 5 to 6 signatures let us assume the same condition that a person is in hurry in that situation he might sign one or two improperly but any one of them will be correct so it compares the new signature with duplicate one's if it matches to any one of them it will be considered as correct one or else wrong one[5][6]. So to get the proper outcome we can modify the approach of comparing the signatures in a more proper way.

Methodology

Here a proposed system is provided where the normalization of the signature image is done and system checks whether the signature matches with original signature. Test signature is recognized with the given input training set using CNN [7][8].

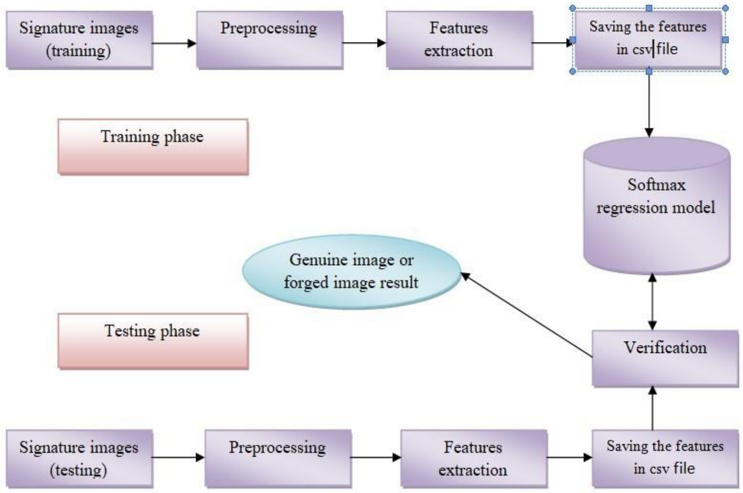
Signature images (training)
Preprocessing
Features extraction
Saving the features in csv file
Training phase
Softmax regression model
Genuine image or forged image result
Testing phase
Verification
Signature images (testing)
Preprocessing
Features extraction
Saving the features in csv file

Figure 1: Block Diagram

Experiments and Results

Then forgery detection algorithms (Softmax regression model) and herris algorithm are enforced on this classified image wherein corners points of the signatures are validated and also to ensure whether signature boundaries are perfectly aligned or not, based on the values System will display the result accordingly with an accuracy of 60%-80% depending on image quality, image lighting and image background.

Here all our real signatures and forged signatures images are present. Here is our some of the genuine and forged signatures

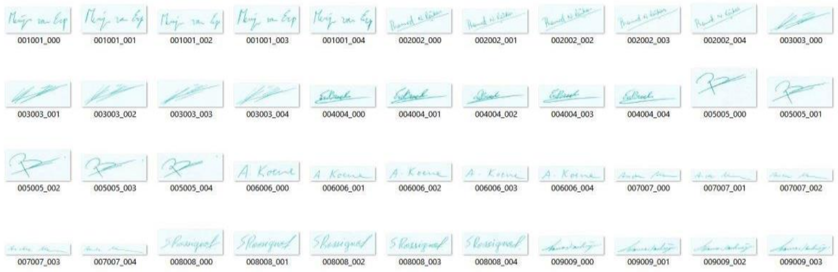

Figure 2: Genuine Signatures dataset

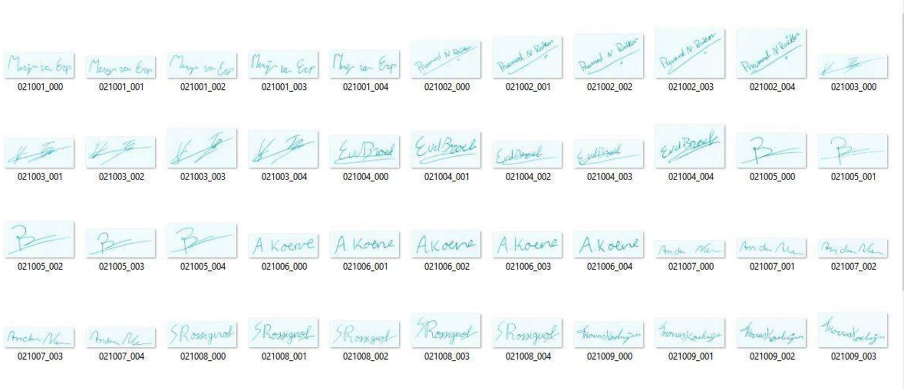

Figure 3: Forged signatures dataset Exploratory Data

When the filename is 001001_001. png the first three letters and the next three letter are same therefore the output should be Genuine Signature.

When the filename is 021001_001. png the first three letters and the next three letter are not same therefore the output should be Forged Signature.

Conclusions and Future Scope of Work

Automatic signature verification is a task where machine learning can be used as a natural part of the process. Two different machine learning approaches, one involving genuines and forgeries in a general set and another involving only genuines for a particular case were described. The first approach is analogous to using counterexamples with near misses in the learning process. Both approaches involve using a similarity measure to compute a distance between features of two signatures.

Special learning outperforms general learning particularly as the number of genuines increases. General learning is useful when the number of genuines is very small (less than four). A refined method of extracting features for signatures was also discussed which can further increase verification accuracy. An interactive software implementation of signature verification was described. Future work should consider combining the two types of learning to improve performance.

Classification of characters and learning of image processing techniques is done focused on envisaging methods that can efficiently extract feature vectors from each individual character. The method came up with gave efficient and effective both for feature extraction as well as recognition. Some genuine images are considered and check its originality to prevent any forgery.

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. This implementation may be considered extreme. In the model created in this work, two classes are created for each user (Real and forgery). Nearly 60 classes are considered for prediction. The best accuracy rate was 95. 55555%.

The Paper can be extended with a much larger dataset with a more efficient method of processing, particularly using GPUs which will increase the accuracy due to more signatures being scanned into the program, and with a higher accuracy. It is also possible to study the further implications of these methods to signature verification in commercial methods by conducting the research on a more realistic dataset.

We can attempt to explore the other implications of signature verification in applications in forensics and medicine where one could create a system for recognizing signatures for those whose signatures change due to the onset of progressive movement disorders such as Parkinson’s disease.

It could be used in the legal system by crosschecking words and signatures that may be used as evidence instead of a handwriting expert. The network can also be used this way in nearly all fields involving important documents, as signatures can be checked to prevent any type of criminal activity that might involve faking or altering critical documents, like contracts.

References

[1] A Bansal, B Gupta, G Khandelwal, SChakraverty“Offline Signature Verification Using CriticalRegion Matching” International Journal of Signal Processing, Image Processing and Pattern Vol. 2, No. 1, 2009

[2] A. Masoodand M. Sarfraz. “Corner detection by sliding rectangles along planar curves” , Computers & Graphics, Vol. 31, pp. 440-448, 2007.

[3] A K Das, A Massand , S Patil “A novel proxysignature scheme based on user hierarchical access controlpolicy” Journal of king Saud UniversityComputer and InformationSciences, 2013

[4] A Pansare and S Bhatia “Handwritten Signature Verification Using Neural Network” International Journal of Applied Information Systems (IJAIS), Vol. 1, No. 2, 2012

[5] S. Harpreet, “Robust Video Watermarking Algorithm Using K_Harries Feature Point Detection”, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 22312307, Volume-5 Issue-4, September 2015..

[6] S Garhawal and NShukla“SURF Based Design andImplementation for Handwritten Signature Verification”International Journal of Advanced esearch in Computer Scienceand Software ngineering (IJARCSSE), Vol. 3, Issue 8, 2013

[7].. D. Mitra, R. Barik, S. Roy, S. Bhattacharyya“ASurvey on Image Segmentation and Image Registration” , ACEEE-CPS, International Conference on Computing, Communication& Manufacturing, ISBN: 978-0-9940194-0-0, Pages 61-69

[8]. D. Mitra, R. Barik, S. Roy, S. Bhattacharyya“Cumulative Measurement of Image Entropy on Different Mathematical Morphological Operation”, ACEEE-CPS, International Conference on Computing, Communication& Manufacturing, ISBN: 978-0-9940194-00, Pages 35-39