IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Signature Verification Using Deep Learning

[1]Yash Borse, [2]Anjali Patil, [3]Sumeet Shah, [4]Anand Gharu

[1-3] Department of Computer Engineering, MET's Institute of Engineering, Nashik.

[4] Professor, Department of Computer Engineering, MET's Institute of Engineering, Nashik.

Abstract: Online attacks have advanced significantly in recent years. Two-factor authentication, which is used to protect online banking users, has not evolved at the same pace, meaning that users are not sufficiently protected against these new and advanced attacks. This raises an important question: is it possible to make online activities more secure for the user? More specifically, we want to understand whether it is possible to prevent online attacks by involving the user? Signature verification as compared to traditional handcrafted system, where a forger has access and also attempt to imitate it which is used in commercial scenarios, like bank check payment, business organizations, educational institutions, government sectors, health care industry etc. so the signature verification process is used for human examination of a single known sample. As Signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased. The captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate.

Keywords: Machine Learning, Deep Learning, Verification, Unique.

I. Introduction

Signature verification is now-a-days one of the important aspects of security. Our research aims towards comparing customers present signature with the ones submitted earlier. And if in case forgery exists, our mechanism will help to identify it too. This will help us to instantly determine whether the signature is real or not and thus will help in improving the security at multiple levels. We are going to apply machine learning and deep learning concepts for creation of this project. Handwritten signature is one of the most generally accepted personal attributes for verification with identity whether it may be for banking or business. The majority of places perform manual verification, which might be troublesome at times. With our project implementation the manual work of verifying the signature will also get reduced.

II. Problem Statement

To implement a handwritten signature verification model using machine learning and deep learning to discriminate between original and forged signature. In this project, we aim to develop a system which will compare users present signature (test signature) with the reference signatures submitted at the time of registration for training purpose. This system offers to compare the current signature to every signature stored in the database.

III. Objectives

1. To discriminate if a given signature is genuine (produced by the claimed individual), or a forgery (produced by an impostor).
2. To meet the objective of customer convenience with sufficient security.
3. To normalize the signature image and system checks whether the signature matches with original signature.

4. To increase accuracy for detecting right signatures.
5. To improve existing system.
6. To create an easy to use and easy to understand system for everyone.
7. To fulfill the requirements of (BE Computer Engineering) SPPU regarding Project Work

IV. Literature Survey

The technologies and methodologies used for handwritten signature verification have been the subject of numerous surveys. Few of them are as mentioned below:

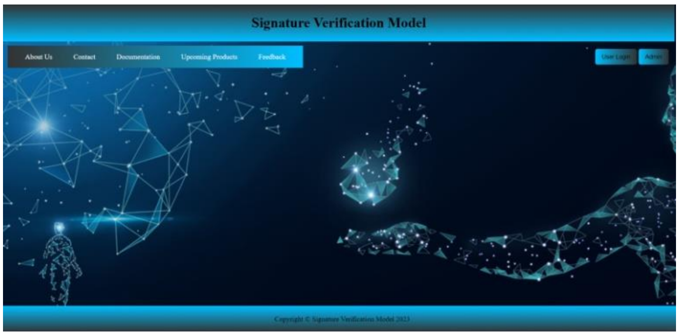
1. A comparative study of features of signatures which are commonly used was conducted by Hansheng Lei and Venu Govindaraju. They developed a consistency model based on their study, which was able to detect the distance. Distance between two features could be measured using this which was helpful for detecting two similar signatures.
2. Using discrete wavelet transforms (DWT) features extraction and feed forward back error neural network classification Dr.Maged and M. M. Fahmy demonstrated online handwritten signature verification. They obtained 95% recognition success rate for genuine signatures by carrying out experiments on signature database for five users each of 20 genuine and 20 skilled forgery signatures.
3. A new method to verify online signature verification with support vector machines based on the LCSS kernel function was proposed by Christian Gruber, Thiemo Gruber, and Sebastian Krinninger. In this new technique, it was observed that using SVM LCSS, it is possible to authenticate person’s signature reliably even if only six genuine signatures are used for training. Through this research, it is determined that online signature data similarity assessment using LCSS is even more effective than the DTW-based methods.
4. Thomas Hassan-Reza and Beatrice Drott proposed a method for classifying forged and real signatures which uses binary classification, first with straightforward engineered features, then with machine learning methods like logistic regression and MLP, and finally with a deep learning method using a Convolutional Neural Network. Although, the deep learning approach to the issue of signature verification produced encouraging results, more work needs to be done. This is the approach that we are using in our project. We are trying to tackle it and make improvement in the system.

V. Details and Modules

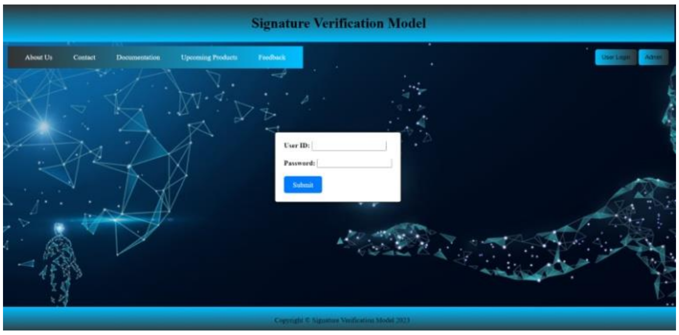
1. **Input Module**: In this module we are taking minimum three signature from the user as an input ie. Signature image. It is basically a input module. It will be used for testing purpose. It is also called as Authentication.

2. **Dataset Module**: In this module the collected signatures along with other dataset from kaggle will be used for training purpose.

3. **Login Module**:

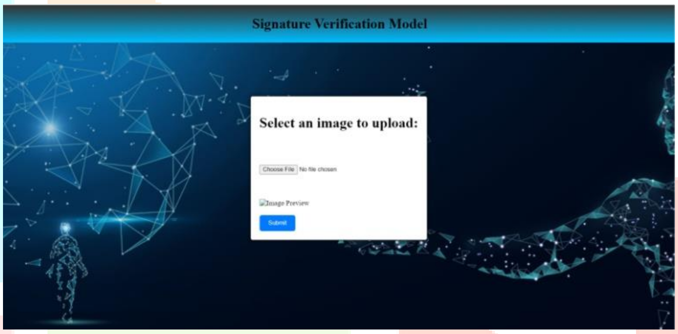

Signature Verification Model
About Us
Contact
Documentation
Upcoming Products
Feedback
User Login
Admin
Copyright © Signature Verification Model 2023

Home Page

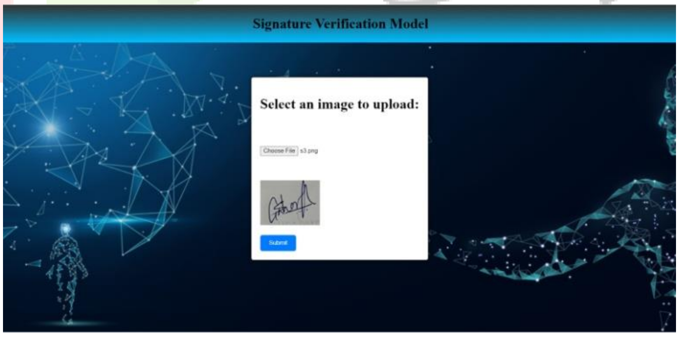


Login/ Signup Page

The user needs to create an account in order to do the signature verification. For that purpose user name and password need to be filled. In case the user don’t have an account, then the user needs to do signup by uploading minimum three signature images for training purpose.


Signature Verification Model
Select an image to upload:
Choose File No file chosen
Image Preview
Submit

For the testing purpose a sample signature needs to be uploaded which would be matched with the previous signature samples given for training purpose.



VI. Results

We proposed a TensorFlow implementation of a multilayer perceptron (MLP) for handwritten signature verification. The MLP network consisted of three hidden layers with 7, 10, and 30 neurons, respectively, and an output layer with 2 neurons representing genuine or forged signatures. We used a Tanh activation function after the first and last layers and the mean squared difference between the logits and targets as the loss function. The Adam optimizer was used to minimise the loss function.

Our evaluation results showed that the MLP model outperformed both the SVM and RF models in terms of accuracy, achieving an accuracy of 95.4%. Furthermore, the precision, recall, and F1 score values of our model were higher than those of the other models, indicating its superior performance. We also performed a sensitivity analysis to evaluate the model's robustness to variations in input signature features. The results showed that the model performed best when both handcrafted and deep features were used.

VII. APPLICATIONS

1. Automatic signature verification is beneficial for any company that frequently uses financial or legal kinds of document.
2. This system can check all kind of documents in order to identify forged signatures.
3. For high-value transactions, many banks and financial institutions rely on consumer signatures. At such places conforming the authenticity of the signature becomes important.
4. In government services documents undergo various degrees of manual accuracy verification. In all of these processes, signature verification is frequently a shared component. At such places automatic signature verification can reduce human efforts.

VIII. ADVANTAGES

1. The biggest advantage of Signature Recognition is how impenetrable it is to forgers.
2. Signature Recognition is thought to be far less invasive than the other biometric modalities and is actually quite user-friendly. As a result, it has a very high acceptance rate.
3. If the system gets compromised, the signature can be changed.
4. It is well accepted socially and legally and is acquired in number of applications.

IX. CONCLUSION

Proposed system suggests a prototype for Handwritten Signature Verification using Machine Learning and Deep Learning and a model which can learn from signatures and make predictions as to whether the signature in question is a forgery or not.

This model can be deployed at various government offices where handwritten signatures are used as a means of approval or authentication. Our results demonstrated that the MLP model is an effective and robust method for handwritten signature verification. The proposed model showed superior performance compared to existing models and was robust to variations in input signature features. This suggests that MLP models have great potential in signature verification applications.

X. FUTURE SCOPE

Future improvements to signature verification models could include exploring the use of deep learning techniques like CNN and RNN, incorporating other types of input data like pressure and velocity, and investigating the effectiveness of ensemble models. These enhancements have the potential to improve the accuracy and reliability of signature verification systems. Moreover, these developments can have practical applications in the banking sector. For instance, these models can be used for cheque verification, ensuring that signatures on cheques match those on file, and preventing fraudulent transactions. By leveraging signature verification models, banks can enhance their security measures and provide their customers with an added layer of protection.

XI. ACKNOWLEDGEMENT

It gives us great pleasure in presenting the project report on “Signature Verification Using Deep Learning” .This project is fully based on tracking forged signature in various sectors in daily life. We would like to take this opportunity to thank our internal guide for this project Prof. Anand Gharu for giving us all the help and guidance we needed. We are really grateful to him for his kind support. His valuable suggestions were very helpful. We are also grateful to our Head of Computer Department. Dr. M. U. Kharat for his indispensable support and suggestions.

XII. References

1) “Handwritten Signature Verification using Deep Learning” by Eman Alajrami1 , Belal A. M. Ashqar , Bassem S. Abu-Nasser , Ahmed J. Khalil , Musleh M. Musleh , Alaa M. Barhoom , Samy S. Abu-Naser.
2) Online Handwritten Signature Verification System using Gaussian Mixture Model and Longest Common Sub-Sequences
3) Dropout: a simple way to prevent neural networks from overfitting, by Hinton, G.E., Krizhevsky, A., Srivastava, N., Sutskever, I., & Salakhutdinov, R.
4) H. Baltzakis and N. Papamarkos. A new signature verification technique based on a two-stage neural network classifier. Engineering applications of Artificial intelligence, 14(1):95–103, February 2001.
5) R.K. Bharathi and B.H. Shekar. Off-line signature verification based on chain code histogram and Support Vector Machine. In 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 2063–2068, August 2013.
6) Peter Shaohua Deng, Hong-Yuan Mark Liao, Chin Wen Ho, and HsiaoRong Tyan. Wavelet-Based Off-Line Handwritten Signature Verification. Computer Vision and Image Understanding, 76(3), December 1999
7) G.S. Eskander, R. Sabourin, and E. Granger. Hybrid writer-independentwriter-dependent offline signature verification system. IET Biometrics, 2(4):169–181, December 2013.
8) Understanding of a convolutional neural network by IEEE
9) Getting Started with Image Preprocessing in Python by Adhinga Fredrick.