Karnataka State Council for Science and Technology

“Indian Institute of Science Campus, Bengaluru-560012

A Project Synopsis on

“Signature Forgery Detection Using TensorFlow and MLP”

Submitted in partial fulfillment towards Project Work of VIII Semester of

Bachelor of Engineering

in

Information Science and Engineering

Submitted by

Chandana N S	**4GW19IS011**
Damini D	**4GW19IS013**
Deeksha A S	**4GW19IS014**

Under the Guidance of

Mrs. Anitha Rao
Assistant Professor
Dept. of ISE,
GSSSIETW, Mysuru

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING
(Accredited by NBA, New Delhi, Validity:01.07.2017–30.06.2020&01.07.2020–30.06.2023)

GSSS INSTITUTE OF ENGINEERING & TECHNOLOGY FOR WOMEN
(Affiliated to VTU, Belagavi, Approved by AICTE, New Delhi & Govt. of Karnataka)
(Accredited with Grade ‘A’ by NAAC)
K.R.S Road, Metagalli, Mysuru-570016, Karnataka

2022-2023

PAN-No. : AAATG6551G
GST-No. : 29AAATG6551G1ZL
GSSS | GEETHA SHISHU SHIKSHANA SANGHA (R)
INSTITUTE OF ENGINEERING AND TECHNOLOGY FOR WOMEN
(Affiliated to Visvesvaraya Technological University, Belagavi. Approved by AICTE New Delhi & Govt. of Karnataka)
KRS ROAD, METAGALLI | MYSURU - 570 016 | KARNATAKA | INDIA
NBA Accredited Branches : ECE, CSE, ISE Validity : 01.07.2017 - 30.06.2023 & EEE Branch up to 30.06.2024
Accredited with Grade 'A' NAAC
QS I-GAUGE INDIAN COLLEGE RATINGS GOLD
ATAL RANKING OF INSTITUTIONS ON INNOVATION ACHIEVEMENTS Recognised Band EXCELLENT Colleges / Institutes (Private / Self Financed) Technical FOR 2020-21
Phone : 0821 - 2581304, 4257304 / 2977306 Fax : 0821 - 2581305 Email : gsssengg@yahoo.co.in, principal@gsss.edu.in Web : www.geethashishu.in

Department of Information Science & Engineering

Project Synopsis

1. **Title of the project**
   Signature Forgery Detection Using TensorFlow and MLP

2. **Name of the College & Department**
   Information Science and Engineering, GSSSIETW, Mysore

3. **Name of the Students & Guide**
   Mrs. Anitha Rao - anitharao@gsss.edu.in
   Chandana N S -chandanans2001@gmail.com
   Damini D -daminikumar20@gmail.com
   Deeksha A S -deekshahebbar137@gmail.com

4. **Keywords**
   Jupyter Notebook, Anaconda, Web Page, TensorFlow, MLP

5. **Introduction / background**

The handwritten signature is a particularly important type of biometric trait, mainly due to its ubiquitous use to verify a person’s identity in legal, financial and administrative areas. One of the reasons for its widespread use is that the process to collect handwritten signatures is non invasive, and people are familiar with the use of signatures in their daily life.

Signature forgery detection can be done for handwritten signatures. Where handwritten signatures considered as valid in bank, forensic and other places, The variations are recorded as the signature is being done and extracts features from the signature and performs several checks by comparing with a predefined database containing the signature. Hence, signature forgery detection usually gives a very high rate of successful signature forgery detections.

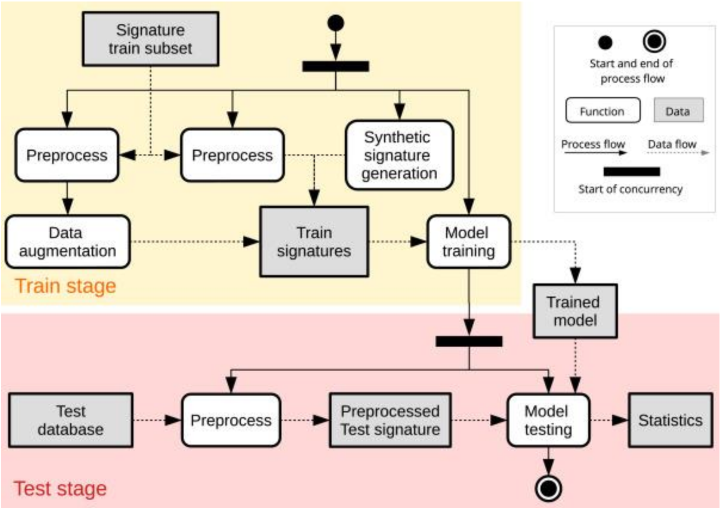
Signature verification systems aim to automatically discriminate if the biometric sample is indeed of a claimed individual. In other words, they are used to classify query signatures as genuine or forgeries. Forgeries are commonly classified in three types: random, simple and skilled (or simulated) forgeries. In the case of random forgeries, the forger has no information about the user or his signature and uses his own signature instead. In this case, the forgery contains a different semantic meaning than the genuine signatures from the user, presenting a very different overall shape. In the case of simple forgeries, the forger has knowledge of the user's name, but not about the user's signature.

a handwritten signature is widely accepted as a form of confirmation form a person in any transactions or legal documents which require authentication from the person. Since a signature act as a confirmation in any binding legal or financial process, its authenticity has to be established and it needs to be verified.

6. Objectives

- To develop the model to find signature is forged or not. Which helps bank and forensic department to find the forged signature.
- To ensuring the accuracy of records. by detecting the forgery. To protect the reputation of the signatory and the organization.
- To maintain the security of documents and objects that requires a valid signature for authorization or legal purposes.
- To prevent financial losses by detecting forged signatures, banks and financial institutions can prevent unauthorized transactions and fraudulent activities, which can cause significant financial harm

7. Methodology



Data Collection: Collect a large dataset of genuine and forged signatures for training and testing purposes. The dataset should be diverse, covering different writing styles, ink colours, and paper types. The data should be labelled, indicating whether the signature is genuine or forged. Preprocessing: The collected data needs to be preprocessed to prepare it for input into the neural network. This includes image resizing, normalization, and augmentation techniques such as flipping and rotating the images to increase the size of the dataset.

Feature Extraction: Extract relevant features from the signature images. Common features include line thickness, curvature, angle, and direction of the strokes. MLP

Architecture Design: Design an MLP neural network architecture that takes the extracted features as input and learns to classify the signature images as genuine or forged. The architecture should consist of multiple layers with nonlinear activation functions. Transfer Learning: Utilize a pre-trained MLP network on a large dataset of similar images, such as the MNIST dataset, and fine-tune the network on the signature dataset. This helps the network learn the underlying features of the signature images more efficiently.

Training and Testing: Train the MLP network using the pre processed dataset and evaluate the network's performance on a separate testing dataset. Use performance metrics such as accuracy, precision, and recall evaluating the network's performance.

Deployment: Once the MLP network is trained and evaluated, deploy the system in a realworld environment, such as a bank, where it can be used to automatically detect signature forgeries. In summary, the system design for a signature forgery detection system using MLP and transfer learning involves data collection, pre processing, feature extraction, MLP architecture design, transfer learning, training and testing, and deployment.

8. Results and Conclusions

This paper proposed a new method for off-line handwritten signature verification that depends on a MLP. The high accuracy is feasible to filter the forgery from the genuine signature, especially for skilled forgery, while the speed of the MLP is very favourable in real world application. The results are encouraging and thus should motivating the research on skilled forgery detection especially for offline handwritten signature**.**

9. What is the innovation in the project?

As we have seen many methods used SVM for validating the signature based on the strokes, in our research we are trying to implement this by using TensorFlow and MLP Classifier.

In the proposed system first data need to pre-processed, pre-processed steps involve converting image to greyscale and greyscale to binary later image will be cropped based the bounding boxes. Next features will be extracted by using ratio of images, centroid, eccentricity, solidity, and skewness of the image once these steps are done, we will apply the MLP to train the model and the output will be evaluated.

10. Scope for future work

The use of additional features improving verification results and increasing feature dimensionality. We utilized a jupyter notebook to construct the software, and it was a success. In Python, our project has been successfully tested. We also looked into the project's uses and future scope. Our solution can be by using the API we can build a mobile application and also The future work includes a more granular look at software component type, topic patterns and extracting more valuable recommendations, and machine learning models to predict optimal release windows. In practical applications, since more forgery samples will lead to a higher accuracy rate, we can create forged signatures by ourselves to further improve the performance of our proposed method.