Automated Signature Verification Using AI

Contents

Introduction2

Business Requirement2

Current System2

Proposed System2

Technologies used..... 3

Risks and challenges 3

Results/ Output..... 4

Conclusion 4

Future Enhancements..... 4

Introduction

Signature can be defined as a scripted name or legal mark of an individual for a proof of identity. A signature can be accepted only if it is from the intended person. Although it is unique and private to that person, there is a possibility of forgery. Hence, in banking sector identifying the authenticity of the signature is of utmost importance.

Business Requirement

The probability of two signatures made by the same person being the same is very less. Many properties of the signature may vary even when two signatures are made by the same person. So, detecting a forgery becomes a challenging task. Our objective is to find a solution based on Convolutional Neural Network (CNN) where the model is trained with a dataset of signatures, and predictions are made as to check whether a provided signature is genuine or forged.

Current System

Nowadays, handwritten signature is one of the most widely accepted personal attribute for confirmation with identity whether it is in banking or business sector. As innumerable transactions occur on a daily basis manual signature verification is no longer an option. This is where the automated signature validation becomes important which will reduce the errors and fasten the process.

Proposed System

• Data Acquisition

Handwritten signatures are collected and some of the unique features are extracted to create the knowledge base for every individual

• Data Pre-processing

Resizing the image: The system must be able to maintain high performance regardless of the image size. So all the images are resized to a standard resolution of 28 x 28.
Data Augmentation: Image augmentation artificially creates training images through different ways of processing or combination of multiple processing, such as random rotation, shifts, shear and flips, etc. This is done using ImageDataGenerator which generates batches of image data with real-time data augmentation.
RGB to Gray scale: In layman's terms, RGB image is represented as a matrix of Red, Blue and Green values ranging from 0 to 255.Whereas in grayscale representation each pixel is a single sample which contains the intensity information. As an initial process, any RGB image has to be

converted into a grayscale image which helps to reduce the computational complexity of digital image processing.
Grayscale to numpy array: The gray scale image is converted to numpy array to store the raw values of a digital image.
Organising the data: As this is a classification problem, the training data has been divided into two groups, genuine and forged.

• Model Building

Convolutional neural network (CNN) which is a deep feed forward neural network has successfully been applied to analyse visual imagery. Convolutional networks were inspired by biological processes in that the connectivity pattern between neurons resembles the organization of the animal visual cortex. We used the Keras library with tensor flow backend to implement CNN.

• Training and Testing the Model

The model is trained using the pre-processed data and the derived model is verified using loss and accuracy metrics to see how well the model has fit the data. We obtained an accuracy of 91% which can be improved by increasing the number of training dataset. Finally, we tested the model using a signature test data to see if predictions are correct.

Technologies Used

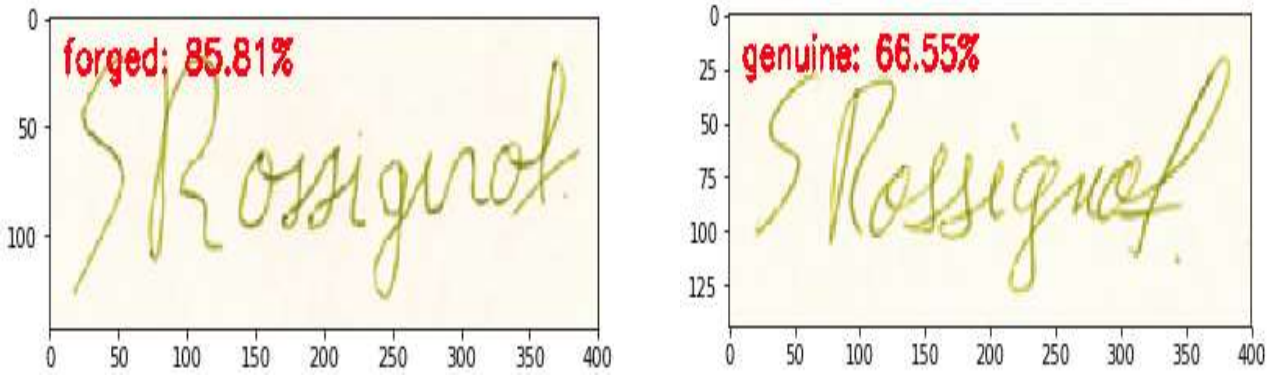
- Python
- AI and Deep learning
- OpenCV
- Keras

Risks and Challenges

Below are the risk identified for implementing proposed system;

- High intra-class variability - an individual's signature may vary greatly day-to-day.
- Large temporal variation - signature may change completely over time.
- High inter-class similarity - forgeries, by nature, attempt to be as indistinguishable from genuine signatures as possible.
- Lack of enough training samples.

Results/ Output



(i) *(ii)*

Prediction results of sample signatures i) forged signature ii)genuine signature

Conclusion

This proposed system helps to verify whether a signature is genuine or forged. The AI based automated system saves time and manual costs and avoid problems caused by intra-and inter-observations.

Future Enhancements

More types of neural networks and architectures should be tested in future research and a better method might be obtained to improve the signature verification results. In future, signature verification system can be implemented in online electronic banking systems.