OFFLINE SIGNATURE FORGERY DETECTION USING CONVOLUTIONAL NEURAL NETWORK

Mr. Raj Balsekar
Ms. Rashi Gundapwar
Ms. Aditi Parekh
Ms. Manasi Desai
Prof. Swapnil Shinde
Department of Information Technology
Marathwada Mitra Mandal's College of Engineering Karvenagar, Pune.

Abstract

Handwritten Signature is considered as one of an integral part of security as it can be used for verification and authentication. Precision is not maintained every time a person does the signature, different parameters like signature strokes, length, pixel depth, continuity, etc may vary. Such Properties of the signature has to be checked before verification and authentication. So authenticating a fake signature becomes a challenging task.

A Signature Capturing and Recognition System will take the image of the signature as an input and will train the image by extracting various features and will store it in the database then using Convolutional Neural Networks it will be compared with the original source signature and recognize whether it is the original signature. For feature extraction algorithms like Grayscale and Binarization are used. Once the image is captured, it will be converted into a black and white image and then processed. This system needs to be trained very well in order to have better results. Signatures samples will be fed into the system for identification tests in order to maintain high accuracy in the system.

Feature extraction is an important stage where the features of each signature are captured using the CNN algorithm. The idea of this step is to identify each and every minor detail of a signature. Subsequently identifying the features and extracting them properly will lead to a better or more accurate verification. A centralized database of correct signatures of the customers will be available. This particular database can be used by a lot of systems that require customer information and signature information.

Keyword

Convolutional Neural Network, Classification, Feature Extraction.

I. Introduction

Nowadays, person identification (recognition) and verification is very important in security and resource access control. Biometrics is the science of automatic recognition of individual depending on their physiological and behavioral attributes. For centuries, handwritten signatures have been an integral part of validating business transaction

contracts and agreements. Among the different forms of biometric recognition system such as fingerprints, iris, face, voice, palm etc., signature will be most widely used. [3]

Signature verification and forgery detection is the process of verifying signatures automatically and instantly determine whether the signature is real or not. In this authentication process a captured signature is stored in a computer in the form of image file. The problem is to compare the user signature with a sample database signature and to verify whether the signature is genuine or forged. [2]

1. Types of Signature Verification

Signature verification and forgery detection is the process of verifying signatures automatically and instantly determine whether the signature is real or not. Static or offline verification is the process of verifying a paper signature after it has been made. The signature in question is then compared to previous samples of the target's signature, which constitutes the database or knowledge base. In the case of an ink signature on paper, the computer requires the sample to be scanned for analysis, whereas a digital signature which is already stored in a data format can be used for signature verification. [1]

2. Problem Statement

Using Convolutional Neural Network (CNN), the model is trained with a dataset of signatures, and predictions are made as to whether a provided signature is genuine or forged.

3. Objectives

The aim of this project is to develop a signature recognition and verification System by using convolutional neural network to accurately characterize each user's signature, thus offering good verification and recognition performance.

4. Relevance

The inevitable side-effect of signatures is that they can be exploited to feign a document's Authenticity. In this system, Off-line Signature Verification Based on Fusion of Grid and Global Features using Neural Network is presented. The global and grid features are fused to generate a set of features for the verification of a signature.This system presents a neural network-based recognition of offline handwritten signatures system That is trained with low- resolution scanned signature images.

II. Literature Survey

In [1] Author has proposed that, signature verification can be done with the help of two types static and dynamic. Static or offline verification is the process of verifying an electronic or paper signature after it has been made, while dynamic or online signature verification takes place as a subject creates his signature on the digital tablet or similar device. The signature in question is then compared to

previous samples of the target's signature which constitute the database or knowledge base. In case of an ink signature on paper the computer requires the sample to be scanned for analysis, whereas a digital signature which is already stored in data format can be used for signature verification.

In [2], various explanations of offline signature verification are explored. In offline signature verification, template matching and hidden markov model techniques are generally employed. These techniques are based on the structure of the signature. Template matching is a technique in digital image processing for finite small parts of an image which match a template image. When it comes to template matching, metrics like n square error or similarity index or wrapping method can be used which wraps one curve onto another that the original shape is maintained.

In [3], Author states that a signature may be termed a behavioral biometric, as it can modify depending on many essentials such as: frame of mind, exhaustion, etc. The exigent aspects of automated signature recognition and verification have been, for a long time, a true impetus for researchers. Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged.

In [4], Author proposes an online, robust, and automatic signature verification technique using the recent advances in image processing and machine learning. Once the image of a handwritten signature for a customer is captured, several pre-processing steps are performed on it including filtration and detection of the signature edges. Afterwards, a feature extraction process is applied on the image to extract Speeded up Robust Features (SURF) and Scale-Invariant Feature Transform (SIFT) features.

In [5], Author proposed that initially a set of signatures are obtained from the subject and fed to the system. These signatures are pre-processed. Then the pre-processed images are used to extract relevant geometric parameters that can distinguish signatures of different persons. Then the curves of signatures are produced by using the critical points and their equations are analyzed.

III. Proposed System

In this system, given a set of genuine signatures, the objective is to learn a model that can distinguish between genuine signatures and forgeries. The most common classification of forgeries in the literature considers Random Forgeries, where a person uses his or her signature to impersonate another individual.

Data Acquisition

Manually written signatures are collected and some unique features are extracted to create knowledgebase for each and every individual. The very first step is to collect dataset of signatures. In our proposed system, we have a dataset of 750 signatures in total in which we have 5 signatures per person and a total of 150 individuals. The dataset is divided into training dataset and testing dataset.

Pre-processing

When a signature is uploaded in the system to check whether the signature is forget or not, the system firstly performs pre-processing of the image. The image is stored in the form of matrix inside the computer. For pre-processing we used GrayScale algorithm which converts RGB image into black and white image, Geometric Transformations are performed and after that binarization is done.

Feature Extraction

After pre-processing, various features are extracted from the pre-processed image and is compared with the features extracted from the images already stored in the database. Features such as ratio, centroid, eccentricity, solidity, skewness and kurtosis are extracted from the image. These features help the system in increasing the accuracy of the output.

Comparison using CNN Algorithm

Once features are extracted, the final step is to compare the features of the input image and genuine image already stored in the database to come to conclusion as to whether the input image is genuine or forged. Comparison is done using CNN algorithm and output is displayed by the system. "Signature Matched" is displayed when the input signature is genuine and "Signature Not Matched" is displayed when signature is forged.

File Management

Initially, we take the ID of the subject as an input. It is later used to make CSV document. At that point the directory of the raw images is loaded into the file system. We need to include real signatures as well as the fake signatures in batches for mass processing. The destination directory has to be included with both training and testing sub directories. This will make the system to avoid directory error. At that point the images from the source directories for example genuine and fake are stacked as records into the system. Each image from the list is stacked, prepared and afterward final image document is made. The images are split into the separate proportion between the destination path sub-directories. When a total bunch of images is handled the CSV record is refreshed.

IV. System Architecture

Implementation Details

Initially signature image is passed for image preprocessing where normalization, image enhancement, geometric transformation, etc are applied on the image so that the image is processed perfectly and can be passed further for feature extraction. In feature extraction local and global features are extracted from the image for comparing the image that is uploaded and image stored in the database. Generally, for low level applications such as object detection and classification, global features are used and for higher level applications such as object recognition, local features are used. Combination of global and local features improves the

accuracy of the recognition. After extracting the features from the image, Convolutional Neural Network is applied on the image for matching the image with the image in the database and providing the results as to whether the image is genuine or forged. In CNN, image is passed through convolutional layer, pooling layer and fully connected layer for obtaining results. [5]

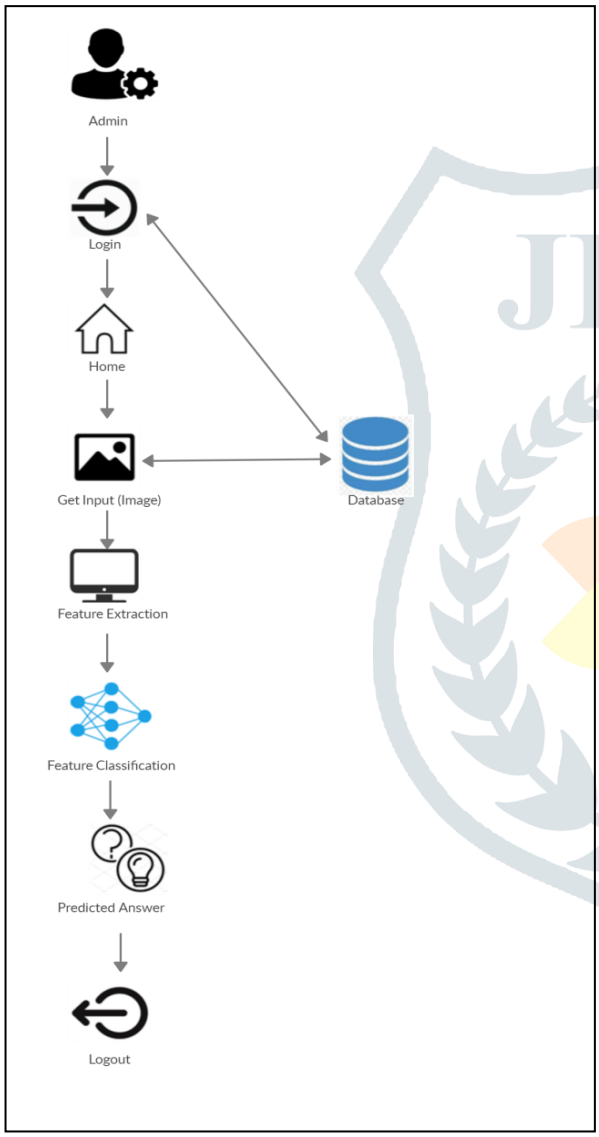

Fig.1 System Architecture

Mathematical Model

S = {s, e, X, Y, I}

s = Start of the Program

Register/Login into the system

Provide Input as an Image.

e = End of the program

X = Input of the program (Image)

Y = Output of program

I = Signature Prediction

First, user provide Input as an Image

Algorithm extract the features of image, Comparison takes place

Let F be the set of features

F= {F1, F2... ,Fn}

These features are compared with extracted features. The classifier classifies these features and determines whether the given Problem. Selection belongs to Available classified Data.

CNN Algorithm will predict the Result of Signature.

Result

Fig.2 Genuine Signature

Fig.3 Forged Signature

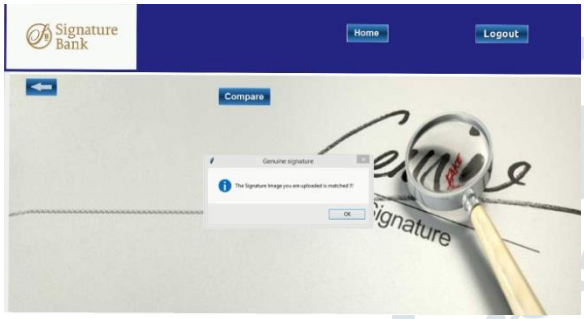

Fig.4 Output Image

Conclusion

This proposed system is focused on Bank Cheque Signature Verification System using artificial neural network. Signatures are verified based on parameters extracted from the signature using various image processing techniques.

In detecting the exact person and it provides more accuracy of verifying signatures for implementation of above, this paper uses Convolutional Neural Networks for recognition and verification of signatures of individuals.

V. References

[1] Jerome Gideon S, Anurag Kandulna, Aron Abhishek Kujur, Diana A Kumudha Raimod "Handwritten Signature Forgery Detection Using Convolutional Neural Networks", International Conference on Advances in Computing and Communication, P – 978-987 (ICACC-2018) https://www.sciencedirect.com/science/article/pii/S877050918320301

[2] Bhattacharya L., Goshp., Biswas S, (2013) "Offline Signature Verification Using Pixel Matching Technique", International Conference on Computational Intelligence : Modeling Technique and Applications(CIMTA), Proceida Technology, P – 970-977, 2013.

[3] Ashish A Dongare, Prof R. D. Ghongade(2016) "Artificial Intelligence Based Bank Cheque Signature Verification System", Vol – 03, P-ISSN 2395-0072(IRJET)

[4] Walid Hussein, Mostafa A. Salama and Osman Ibrahim (2016),"Image Processing Based Signature Verification Technique to Reduce Fraud in Financial Institution", MATEC Web of Conferences 2016.

[5] Saroj Ramdas, Geethu P. C. (2015) "Comparative Study on Offline Handwritten Signature Verification Scheme", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Vol - 02, March 2015.