International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Author Identification using Signature Verification

Kritika Vohra and Dr. S. V. Kedar

Department of Computer Engineering, Rajarshi Shahu College of Engineering, India.

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Signature is most generally used for verification of an individual. Signature is taken into account as a mark for the identification of all the social, business and business functions that the term signature verification is of utmost importance because it may be victimized and might result in huge losses. Signature could be a behavioral biometric attribute that includes neuromotor characteristics of an individual in addition as socio-cultural influence. In this system author is identified based on signature verification. Initially pre-processing of signature image is done. Further features are extracted based on the pre-processed data. Support Vector Machine algorithm is applied on the extracted features and accuracy of signature is determined. Based on this signature is identified as genuine or forged and author is identified based on the genuineness of signature.

Keywords: *Signature, Verification, Author, pre-processing, Features, Support Vector Machine*

Introduction

Signature could be a representation of a person's name that is employed in his or her identity proof. Written signature could be a widely accepted biometric of identity verification. It is a primary mechanism for authentication and authorization. Hence, signature verification is one of the foremost difficult tasks in document forensics. There is a probability that the signature will be cast. Thus, the need for genuineness and verification of signature arises [1].

Signature verification is required in various banking sectors, government organizations, finance and other sectors such as security and forensics. For this, various features of signature need to be analyzed. The SpeedUp Local features are used for analysis which gives areas and clues about which features are exclusively considered for analysis [2].

The online signature is a trait which is used for the verification of a person's identity. For online signature verification, Hidden Markov Model was used successfully which uses small number of observations and time series modeling required proper definition of states [3]. This depends on signature curve which is based on pen's velocity value. It is decomposed into low or high partition according to velocity value. The partitioning methods based on velocity and pressure is examined using Hidden Markov Model.

For verification of offline signature, Convolution Neural Network was used followed by fully connected layer whose parameters are trained by several orders of magnitude. This CNN has been used in two different configurations; first as feature extractor in hybrid classifier and end to end classifier in Siamese network [1].

The procedure for extracting features depends upon the preprocessed signature image. One of the techniques for feature extraction is finding the Centre of gravity of the preprocessed signature image [4].
For identification of a person's handwritten signature efficient techniques to extract features from handwritten signature images are required. For this clustering is one of the techniques used for verification. In clustering, a set of data points is divided into non-overlapping groups, of clusters of points where points in cluster are more similar to one another than to points in other clusters. The term "more similar," in clustering means closer by some measure of proximity [5].

In this paper, author is identified from signature using Support Vector Machine algorithm. Initially the signature dataset is pre-processed using various pre-processing techniques like gray scale conversion, threshold and edge detection. Further feature extraction is done by extracting features from the dataset and signature accuracy is determined. A threshold value is set to identify the genuineness of signature and author is identified.

The remainder of this paper is organized in various sections. In Section II, literature survey is described, followed by Section III, which provides details on the proposed methodology. Section IV presents the partial experimental results. Finally, in Section V some conclusions are drawn.

Literature Survey

Mohitkumar A. Joshi, Mukesh M. Goswami, and Hardik H. Adesara [6] presents low level stroke feature, which were originally proposed for recognition of printed

Gujarati text, for offline handwritten signature verification. This experiment was performed on ICDAR 2009 Signature Verification Competition dataset which contains both genuine and forged signature. Recognition is performed using Support Vector Machine classifier with 3-fold cross validation. Equal Error Rate achieved is 15.59, which is comparable with the ICDAR 2009 Signature Verification Competition Result.

Kamlesh Kumari and V. K. Shrivastava [12] presents how efficiently the image processing based feature extraction techniques capture the properties of handwritten signature features that could be described algorithmically. Parameters used with knowledge model affect the accuracy of Automatic Signature Verification are also described.

Avani Rateria and Suneeta Agarwal [1] presents verifying signature with a small 3-layer deep convolutional neural network followed by a fully connected layer is proposed whose trainable parameters are several orders of the magnitude. Here, feature extractor is used in hybrid classifier scheme and Siamese network. Support Vector Machine is used for verifying the genuineness of the signature.

Derlin Morocho, Aythami Morales, Julian Fierrez, and Ruben VeraRodriguez [7] presents schemes for improving automatic signature recognition. This paper includes crowdsourcing the experiment to establish human baseline performance for signature recognition tasks. It also includes attribute based semiautomatic signature verification system recognized inspired in FDE Analysis. In this paper, they have proposed use of attributes for signature verification.

Htight Htight Wai, and Soe Lin Aung [4] present a method for extraction of features from Offline Signature Verification System. Signature image having in lower right corner of the bank cheque is acquired. Signature image is converted to binary image using Otsu's method and then bounded in the (rectangle). After that, a new feature extraction technique based on signature image splitting is presented. Before finding Centre of gravity of the whole signature image, it is initially detected whether it has interesting pixel or not. After finding the Centre of gravity, the image is firstly partitioned to achieve four blocks. When partitioning parts of each of four blocks, its block is detected whether it has interesting pixel or not. After detecting pixel, blocks are further partitioned until 64 sub blocks are achieved. Finally, three robust features are extracted from each sub blocks.

Proposed Methodology

In this system, genuine signature is recognized, and author is identified from the verified signature. As it involves identifying the genuineness of signature, it was necessary to create database. The dataset used is ICDAR 2011 Signature Verification Competition (SigComp2011) containing Dutch signature dataset.

A. Architecture

The system architecture is shown in Fig. 1. It involves collection of input signature image as input from user. Pre- processing of signature image is done to remove noise. Further features are extracted on the preprocessed data. Classification is done using Support Vector Machine algorithm. Accuracy of signature is determined. Based on the accuracy of signature author is identified.

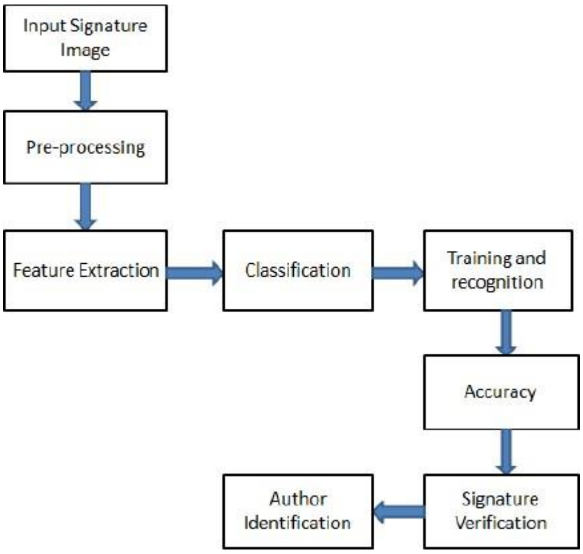

Fig. 1. System Architecture

There are four modules in this system:
Module 1: Pre-processing of input signature image
Module 2: Feature Extraction of pre-processed data
Module 3: Classification of signature using SVM Module
4: Identifying author based on recognized signature.

Module 1: Pre-processing of input signature image

Scanned signature image is taken as an input and pre-processing is performed on signature image to remove noise.

The steps included in pre-processing are:
Grayscale Conversion: Grayscale is a range of monochromatic shades from black to white. Hence, a grayscale image contains only shades of gray and no color. The reason for differentiating these images from any other color image is that less information needs to be provided for each pixel.

Threshold: Thresholding is the simplest method of segmenting the image. From grayscale image, thresholding is used to create binary images. Thresholding replaces each pixel in an image with a black pixel if the image intensity is less than some fixed constant.

Edge Detection: Edge detection is an image processing technique which helps in finding boundaries of an object within the images. It works by detecting discontinuities in brightness. Edge detection is used in image segmentation and data extraction in areas such as image processing, computer vision, and machine vision.

Module 2: Feature Extraction of pre-processed data For the verification of signature, feature extraction is done. Feature extraction includes various attributes on which are extracted on signature images for verification.

The attributes for feature extraction are:

Shape: This attribute is associated with the graphical model which used to create the signature. Labels associated to this attribute are rounded strokes, vertical strokes, horizontal strokes, calligraphic model, vertical and horizontal strokes, or unknown which can be done using edge detection process on image.

Punctuation: This attribute analyses any punctuation mark or stroke that characterizes the signature (e.g., "i" or "j" punctuation). It helps in identifying whether the signature has proper punctuation, the signature has punctuation but in the wrong place or there is no punctuation.

Slant of the strokes: This attribute measures the slope that is the angle with respect to the baseline. The annotator must choose which are the most relevant strokes (if they exist, otherwise the attribute is set to zero).

Strokes length: As in the slant measures, the annotator must select up to three representative strokes (initial and ending points) to automatically calculate their lengths (in pixels).

Character spacing: This attribute measures the separation (in pixels) between or up to four most relevant characters in the signature.

Alignment to the baseline: Also known as slant which is easy to calculate in some signatures which have elongated shape but could be a challenge in signatures with high complexity which have disruptive text and flourish. It is defined as the angle between the main dominant axis of the signature and the baseline.

Flourish-characteristics: These attributes are symmetry of the most representative loops in the flourish, weight and roundness.
Proportionality:

The proportion is related to the symmetry and size of the handwriting: proportional, un proportional, mixed or unknown.

Module 3: Classification of signature using SVM This module helps to classify the signature image as genuine or forged. Classification of signature as genuine or forged is done using Support Vector Machine algorithm. It is a supervised machine learning algorithm. Support Vectors are the co- ordinates of an individual observation. Support Vector Machine is a frontier which is used to segregate two classes. Classification is done by finding the hyper plane which best differentiates two classes. Support Vector Machine is most widely used in classification problems.

A. Algorithms

For classification of signature as genuine or forged, Support Vector Machine (SVM) algorithm is used.
SVM is a machine learning task of inferring a function called classifier, from supervised training data. They are a specific class of algorithms which are characterized by usage of kernels and optimize it with an algorithm that is very fast in the linear case, acting on the margin on number of support vectors. A support vector provides several computational advantages by presenting the solution for classification of signature by providing simple hypothesis using random test points. SVM contains some features like maximum margin classifier. It is a decision strategy that separates training data with maximal margin and nonlinear function that controls input parameters to find linear separating hyper plane which does not depend upon high dimensional feature space [9].

Algorithm:

Step 1: Select a universal dataset of signature images
Step 2: Perform pre-processing on dataset of signature images including techniques like gray scale conversion, threshold and edge detection.
Step 3: Once completed with pre-processing, perform feature extraction including various features. Step 4: Depending on the feature extraction, signature should be classified.
Step 5: SVM classifier should be used to classify it into genuine and forged signature.
Step 6: Repeat steps 2-5 with all images in the training set.
Step 7: After step 6, the trained model of classifier is produced. This model is then used to classify the author as genuine or forged.

Module 4: Identifying author based on recognized signature

Once the signature is classified accuracy of signature should be determined and author should be identified. A threshold value is set which identifies the author if the value goes above threshold and author is not identified is value is below threshold.

Results and Discussion

A very basic pre-processed model is built based on the partial data. Dutch signature image is taken as input. Further, pre-processing is done on the input signature image which includes grayscale conversion, threshold and edge detection. Fig. 2 below shows the input signature image which is further pre-processed in Fig. 3 using techniques of grayscale conversion, threshold and edge detection. Fig. 3 shows SIFT detector in which an object is recognized in a new image by individually comparing each feature from the new image to this database and finding candidate matching features based on Euclidean distance of their feature vectors.

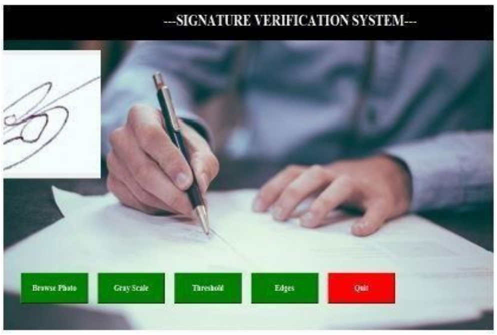

Fig. 2. Input Signature Image

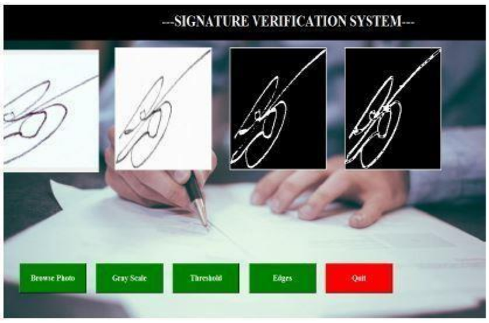

Fig. 3. Pre-processed signature

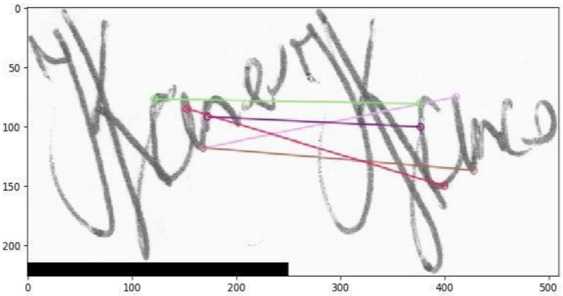

Fig. 4. SIFT detector

Conclusion

Hence, to avoid forgery of signature in any of the public, private or other sectors; signature is classified recognized as genuine or forged based on above mentioned features. Support Vector Machine helps to classify the signature as genuine or forged. As a result, it will result in determination of the signature that the signature is of the author specific.

Acknowledgement

The authors would like to thank researchers as well as the publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University, Pune and concern members of cPGCON2020 conference, organized by the Department of Computer Engineering, Amrutvahini College of Engineering, Sangamner for their constant guidelines and support. We are also thankful to the reviewers for their valuable suggestions.

References

[1]. Avani Rateria, and Suneeta Agarwal. ”Off-line Signature Verification through Machine Learning.” UPCON, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics, 2018.

[2]. Muhammad Imran Malik, Marcus Liwicki, Andreas Dengel, Seiichi Uchida, and Volkmar Frinken. ”Automatic Signature Stability Analysis and Verification Using Local Features.” 14th International Conference on Frontiers in Handwriting Recognition, 2014.

[3]. Saeede Anbaee Farimani, and Majid Vafaei Jahan. ”An HMM for Online Signature Verification Based on Velocity and Hand Movement Directions.” 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018.

[4]. Htight Htight Wai, and Soe Lin Aung. ”Feature Extraction for Offline Signature Verification System.” International Journal of Computer & Communication Engineering Research (IJCCER), Volume 1 - Issue 3 September, 2013.

[5]. Samit Biswas, Debnath Bhattacharyya, Tai-hoon Kim, and Samir Kumar Bandyopadhyay. ”Extraction of Features from Signature Image and Signature Verification Using Clustering Techniques.” T.-h. Kim, A. Stoica, and R.-S. Chang (Eds.): SUComS 2010, CCIS 78, pp. 493– 503, 2010. © Springer-Verlag Berlin Heidelberg, 2010.

[6]. Mohitkumar A. Joshi, Mukesh M. Goswami, and Hardik H. Adesara. ”Offline Handwritten Signature Verification Using Low Level Stroke Features.” IEEE, 978-1-4799-8792-4/15/$31.00_c, 2015.

[7]. Derlin Morocho, Aythami Morales, Julian Fierrez, and Ruben Vera- Rodriguez. ”Human-Assisted Signature Recognition based on Comparative Attributes.” 14th IAPR International Conference on Document Analysis and Recognition, 2017.

[8]. Rashika Shrivastava and Brajesh Kumar Shrivash. ”Offline Signature Verification Using SVM Method and DWT-Gabor Filter Feature Extraction.” IJSTE - International Journal of Science Technology & Engineering, (IJSTE/ Volume 2 / Issue 07 / 051*).*

[9]. Kruthi C., and Deepika C. Shet. ”Offline Signature Verification

[10]. Using Support Vector Machine.” Fifth International Conference on Signal and Image Processing, 2014.

[11]. Kamlesh Kumari, and Sanjeev Rana. ”Offline Signature Recognition using Pretrained Convolution Neural Network Model.” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-9 Issue-1, October 2019.

[12]. Anjali R., and Manju Rani Mathew. ”Offline Signature Verification based on SVM and Neural Network.” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Special Issue 1, December 2013.

[13]. Kamlesh Kumari, and V. K. Shrivastava. ”Factors Affecting the Accuracy of Automatic Signature Verification.”, India, IEEE, 9783805- 4421-2/16, 2016.