International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Signature Verification using Image Processing & Neural Network

Swarali Patil[1], Pranali Misal[2], Mayuri Mhaske[3], Prof Vilas Jadhav[4]

[1,2,3]*Student, Dept. of Computer Engineering, M.G.M. College of Engineering and Technology, Kamothe, Maharashtra, India*

[4]*Prof. Dept. of Computer Engineering, M.G.M College of Engineering and Technology, Kamothe, Maharashtra, India*

Abstract - *The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. We have worked on the Offline Verification of signatures using a set of shape based geometric features. The features that are used are Baseline Slant Angle, Aspect Ratio, Normalized Area, Center of Gravity, number of edge points, number of cross points, and the Slope of the line joining the Centers of Gravity of two halves of a signature image. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system. For each subject a mean signature is obtained integrating the above features derived from a set of his/her genuine sample signatures. This mean signature acts as the template for verification against a claimed test signature. In this paper, we present how the problem has been handled in the past few decades, analyze the recent advancements in the field, and the potential directions for future research.*

Key Words: Signature Verification, Pre-processing, Feature extraction, Authentication, Matching techniques, Recognition rate, FAR, FRR, CNN, Neural Networks;

1. INTRODUCTION

Signature has been a distinguishing feature for person identification through ages. Signatures for long have been used for automatic clearing of cheques in the banking industry. When a large number of documents, e.g., bank cheques, have to be authenticated in a limited time, the manual verification of account holders' signatures is often unrealistic. Signature provides secure means of authentication and authorization. So, there is a need of Automatic Signature Verification and Identification system. The present dissertation work is done in the field of online signature verification system by extracting some special feature that makes a signature difficult to forge. In this dissertation work, existing signature verification system has been thoroughly studied and a model is designed to develop an offline signature verification system

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 [1].

Biometric field research includes hand geometry, face prints, fingerprints, voiceprints, signatures, and non-retinal blood vessel analysis. Biometrics has been widely used in physical access control applications. Unlike personal identification number or pin, biometric features are something about the characteristics of a person. Biometric features are used to provide an enhanced level of security and identification. Signatures are one of the most popular and reliable biometric features for verifying person's identity [2].

Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation. A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR). The false rejection rate (FRR) and the false acceptance rate (FAR) are used as quality performance measures. The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted.

1.1 Forgeries

There are three kinds of forgeries –Skilled Random and Casual. Shown below is a self-explanatory image of the various kinds of forgeries:

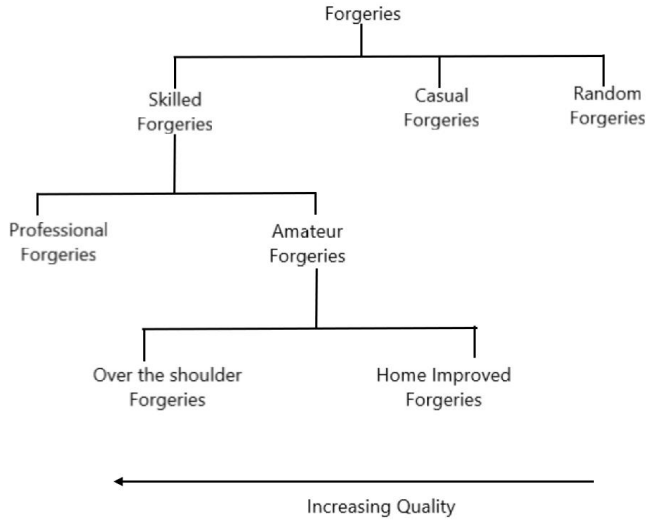

Fig -1: Types of Forgeries

1.2 Problem Statement & Objective

The Objectives of this dissertation are:

- To make sure that the right people are authorized to access high-security systems.
- The process of signature verification should be able to detect forgeries.
- To use cascading of features for the process of feature extraction of signature from the pre-processed scanned image of a signature that will give more accurate results.
- To cascade and comparison of features.

2. Data Collection

Data collection is an important stage of the signature verification process. It is necessary that the data obtained must be accurate. Incorrect signature might cause problems. Here we collect the multiple images of the signatures in form of .png or .jpg and store it into our database. 10 signature samples collected from same person or from different persons and is followed by preprocessing. The signature samples were divided into two parts (training and testing). 10 signature samples were used for training while 10 signature samples were used for testing purpose.

3. PREPROCESSING THE DATA

The aim of pre-processing is an improvement of the image data that suppresses unwilling distortions or enhances some image features important for further processing. Pre-processing contains three steps: Normalization, Re-Sampling Time and Re-Sampling Distance. As we all know, a person's signature will always differ in size every time he signs on a paper or on other materials. Thus, here comes the need for the size normalization to make each person's signature the same in size before starting to extract it features. This is to avoid the developed software to falsify a genuine signature just because of the different is sizing.

Size normalization is performed by scaling each character both horizontally and vertically [3].

$$x_i = \frac{x_i^o - x_{\min}}{x_{\max} - x_{\min}} W$$
$$y_i = \frac{y_i^o - y_{\min}}{y_{\max} - y_{\min}} H \quad (1)$$

Where (x_i^o, y_i^o) denotes the original point (x_i, y_i) is the corresponding point after the transformation.

$$x_{\min} = \min i\{x_i^o\},\ x_{\max} = \max i(x_i^o)$$
$$y_{\min} = \min i\{y_i^o\},\ y_{\max} = \max i(y_i^o) \quad (2)$$

Where W and H are the width and height of the normalized signature respectively. Re-sampling is done to make the raw data points equidistant in time using a simple linear interpolation algorithm as follows. The re-sampling step ΔS is a fraction of the total arc length L.

$$d_i = \sqrt{(x_i - x_{i+1})2 + (y_i - y_{i+1})2}$$

$$L = \sum_{i-1}^{n-1} d_i$$
$$\Delta S = \frac{L}{n_1} \quad (3)$$

Where di denotes the distance of point to point and n is the number of points. After re-sampling, the characters have a fixed number (n1) of points per character (50 points in our system) which provides a fixed size input.

4. FEATURE EXTRACTION

Feature extraction describes the relevant shape information contained in a pattern so that the task of classifying the pattern is made easy by a formal procedure. In pattern recognition and in image processing, feature extraction is a special form of dimensionality reduction. Feature maps are generated by applying Filters or Feature detectors to the input image or the feature map output of the prior layers.

So, the Offline signature verification has been studied from many perspectives, comprising of multiple alternatives for feature extraction. Truly speaking of the feature extraction techniques can be classified as Static or Pseudo-dynamic, where pseudo dynamic features attempt to recover dynamic information from the signature execution process (such as speed, pressure, etc.). Another category of the feature extraction methods are Global and Local features. Global features describe the signature images as a whole - for example, features such as height, width of the signature, or in general feature extractors that are applied to the entire signature image. On the other hands, local features describe parts of the images, either by segmenting the image (e.g., according to connected components) or most commonly by the dividing the image in a grid (of Cartesian or polar coordinates), and applying feature extractors in each part of the image[4].

The determination of features to be used is one of the most fundamental issues in signature verification. Local features: - Dividing the image into parts and extracting features. Global features: - Height, width, etc. [5].

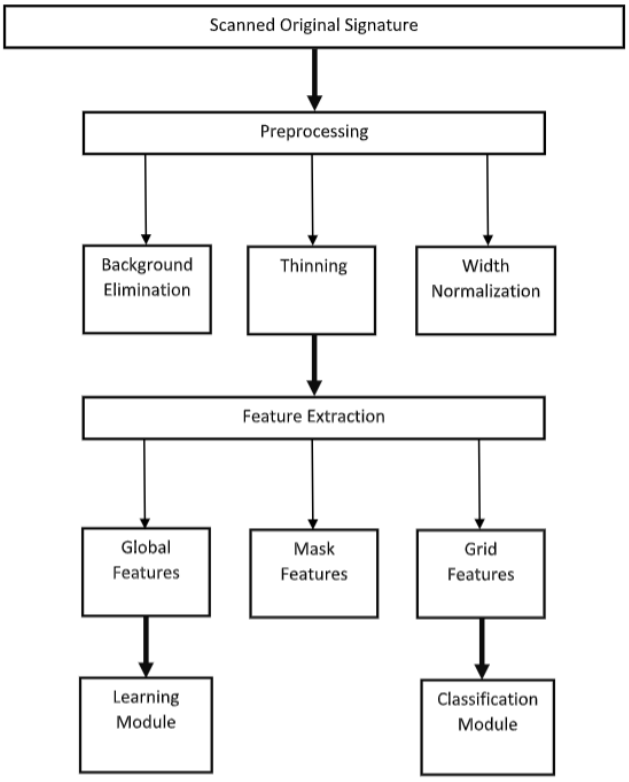

Fig -2: Block Diagram

5. DATA TRAINING

Our Data Training of the collected signature samples can be done in many ways using different classifiers but we have studied about ANN classifier. Other classifiers can be OC-SVM (Support Vector Machine), HMM (Hidden Markov Model), Deep Learning NN, CNN, etc.

An Artificial Neural Network (ANN) is inspired by the way biological nervous systems, such as the brain, process information. The key element of this is the structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons.[6] From the handwritten signature perspective, ANN solves complicated signature recognition problems using parallel operation of neurons due to their generalization capability. The most widely used ANN architectures for pattern recognition includes Multilayer perceptron (MLPs) and Radial Bases Functions (RBFs).

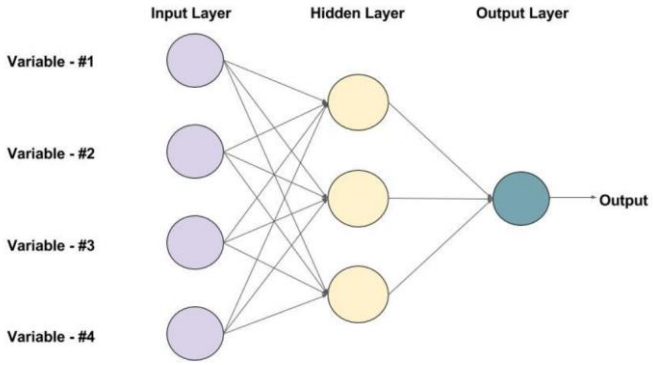

Fig -3: Feed Forward Neural Network

Based on the values obtained, the network will decide the appropriateness of the signature. The suggested scheme discriminates between original and forged signatures using artificial neural network (ANN) for training and verification of signatures. The method takes care of simple and random forgeries and the skilled forgeries are also eliminated in greater extent. The objective of the work is to reduce two vital parameters, False Acceptance Rate (FAR) and False Rejection Rate (FRR). So, the results are expressed in terms of FAR and FRR and subsequently comparative analysis has been made with standard existing techniques. Results obtained by our proposed algorithm are more efficient than most of the existing techniques [7].

6. CLASSIFICATION PROCESS

In the classification process, the classifier used is KNN which stands for k-nearest neighbors. It is basically a classification algorithm that means it assigns a class to a test image based on its feature values. The k-nearest neighbors' algorithm uses Euclidian distance method to find the distance between two training points. Thus, by using Euclidian distance, we can find k nearest neighboring training points of our test point based on its features and the class with maximum number of occurrences is taken as the

decision class for that test image and is assigned to that image. If the decision class is 'original' with same signer the image is 'Accepted' and otherwise 'Rejected' [8].

7. VERIFICATION

The above-described features from the feature extraction process are extracted from a sample group of signature images of different persons. These values are derived from each sample group are used in deriving a mean signature for each subject. The mean values and standard deviations of all the features are computed and used for the final verification. A user defined threshold is defined corresponding to the minimum acceptable degree of similarity for each person was manually estimated. Since users do not like their original signatures to get rejected, we chose the threshold on the lower side to avoid rejection of original signatures.

The Euclidian distance δ in the feature space measures the proximity of a query signature image to the mean signature image of the claimed person. If this distance is below a certain threshold then the query signature is verified to be that of the claimed person otherwise it is detected as a forged one.

8. CONCLUSIONS

Thus, this research allowed us to learn more and more about our domain and the problem of signature recognition and verification. Our research work of over different research work on the problem of signature recognition/verification was done for this paper which allowed to prepare and plan for a signature verification system that was designed and presented in this paper. The algorithm developed by us, uses various geometric features to characterize signatures that effectively serve to distinguish signatures of different persons. The system is robust and can detect random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. Using a higher dimensional feature space and also incorporating dynamic information gathered during the time of signature can also improve the performance. Improvements are found in increasing the accuracy of finding similarities in signatures and better help in concluding if the signature is real or forged.

REFERENCES

[1] Rejean Plamondon and Sargur N. Srihari. Online and off-line handwriting recognition: a comprehensive survey. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 22(1):63–84, 2000.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Julita A., Fauziyah S., Azlina O., Mardiana B., Hazura H., Zahariah A.M.," Online Signature Verification System", 2009 5th International Colloquium on Signal Processing & Its Applications (CSPA)

[3] Abdul Fadlil, Marzuki Khalid, Rubiyah Yusuf (2005). Online Handwritten Character Recognition Based On Online-Offline Features Using BP Neural Network Centre of Artificial Intelligence.K. Elissa, "Title of paper if known," unpublished.

[4] Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira," Offline Handwritten Signature Verification - Literature Review", arXiv:1507.07909v4 [cs.CV] 16 Oct 2017.

[5] Fasna T A, Dr. Rekha Lakshmanan,-"A Survey on Signature Verification ", National Conference on Advanced Computing,Communication and Electrical Systems - (NCACCES'17).

[6] Prarthana Parmar, Jahnvi Mehta, Sakshi Sharma, Krupa Patel, Parth Singh, "A Survey of Handwritten Signature Verification System Methodologies", 2019 JETIR May 2019, Volume 6, Issue 5.

[7] R. M. Samant , Mahendra Shilwant , Bhojraj Sarsambi , Mahesh Shelke," Signature Verification System", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2017.

[8] Tejas Jadhav," Handwritten Signature Verification using Local Binary Pattern Features and KNN", International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04, Apr 2019.