Offline Signature Verification System using Machine Learning Technique

Bharathi K[1] Radhika Shetty D S[2]
[1,2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]VCET, Puttur, India

Abstract— Signatures are imperative biometric attributes of humans that have long been used for authorization purposes. Most organizations primarily focus on the visual appearance of the signature for verification purposes. Many documents, such as forms, contracts, bank cheques, and credit card transactions require the signing of a signature. Therefore, it is of upmost importance to be able to recognize signatures accurately, effortlessly, and in a timely manner. Verification can be accomplished either Online or Offline based application. Offline systems work on the scanned image of a signature. In our technique first the pre-processing of a scanned signature image is done to isolate the signature and to remove noise. In this work, an artificial neural network based on the well-known Back-propagation algorithm is used for recognition and verification. To test the performance of the system, the False Reject Rate, the False Accept Rate, and the Equal Error Rate (EER) are calculated. The system was tested with test signature samples, which include genuine and forged signatures of twenty individuals. The aim of this work is to limit the computer singularity in deciding whether the signature is forged or not, and to allow the signature verification personnel to participate in the deciding process through adding a label which indicates the amount of similarity between the signature which we want to recognize and the original signature. This approach allows judging the signature accuracy, and achieving more effective results.

Keywords: Signature; Authentication; Preprocessing; Feature Extraction; Back-Propagation

I. INTRODUCTION

As of late Machine Learning is making a ton of publicity. Artificial Intelligence is a field of Computer Science that gives computer the capacity to learn without being customized unequivocally and can gain from information and make forecasts of information by investigating the examination and developments of algorithms. Artificial Intelligence algorithm is for the most part sorted as Supervised and Unsupervised machine learning calculations. Administered learning will be learning procedure where a machine is prepared alongside signatures i.e., preparing highlights with their names. Though Un-Supervised learning is a learning strategy with unlabeled information. Artificial Intelligence has various points of interest.

Artificial Intelligence is basically utilized in two sorts of things, Prediction and Inference, where one predicts the future with the assistance of past information and different fields or field design in the information.

Machine Learning has a wide family. One among them is a division of Artificial Intelligence in the field of Computer Science that uses truthful strategies to empower Machines to learn with data, without being modified unequivocally. Back propagation is a strategy utilized in counterfeit neural systems to figure an angle that is required in the estimation of the loads to be utilized in the system. Back propagation is shorthand for "the retrogressive engendering of mistakes," since a blunder is processed at the yield and disseminated in reverse all through the system's layers.

Artificial Intelligence calculations discovers its applications in different fields, for example, Healthcare, Travel, Retail for Product Recommendations, Finance, Communication media, Security, Bio-metric and so on. Bio-metric identifiers are the particular, quantifiable attributes used to tag and depict people. Bio-metric identifiers are regularly arranged as either physiological or conduct. Physiological bio-metric identifiers are identified with the state of the body, for example, unique signature, face acknowledgment, DNA, hand geometry, iris acknowledgment, and retina. Conduct bio-metric identifiers, then again, are identified with the example of conduct of an individual, for example, composing mood, stride, what's more, voice.

A signature is a manually written delineation of somebody's name, moniker, or other imprint that an individual composes on reports as a verification personality and expectation. The author of a signature is alluded to as the signatory or the underwriter. An individual's signature is considered and treated as one of the lawful and normal methods for checking a person's personality. It is routinely written in an extraordinary way, frequently achieving an indiscernible state. Different programmed signature check techniques have been proposed all through the writing. In any case, disconnected signature acknowledgment still stays testing. This work plans to restrict the computer peculiarity in choosing regardless of whether the signature is produced by permitting the signature confirmation work force to partake in the check procedure through demonstrating the measure of closeness between the two signatures.

II. EXISTING SYSTEM

In [1] Dewi Suryani et al proposed "Offline Signature Recognition and Verifcation System" using Euclidian distance model, SVM, Hidden Markov Model, Fuzzy Model. There is a need to develop one general system in future to classify signature and enhance performance.

In [2] Luiz G. Hafemann et. al. proposed "Offline Handwritten Signature Verification Literature Review". The methodology used are preprocessing ,Feature extraction. Which improves the classification with limited number of samples.

In [3] Indrajit Bhattacharya et al. proposed "Offline Signature Verification using Pixel Matching Technique". The methodology used is Pre-processing verification-pixel Matching Technique. By using some equations from co-

ordinate geometry makes this method faster than other methods. Color matching technique makes it more secure.

In [4] Supriya Singh et al. proposed "Signature Verification using LDP & LBP with SVM Classifiers". The methodology used Support Vector Machine (SVM) & chebyshev algorithm is used for verification of signature. Features like Local Binary Pattern (LBP) and Local direction Pattern (LDP). LDPs give more accurate result than LBPs when there is no pen dependence. The accuracy of SVM is higher.

In [5] Sounak Dey et al. proposed "SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification". The methodology used preprocessing, CNN and Siamese Network. In terms of future work, better preprocessing method will be designed to improve the accuracy of the geometric based feature extraction.

In [6] Aini Najwa Azmi et al. proposed "Biometric Signature Veri_cation System based on Freeman Chain Code and K-Nearest Neighbor". The methodology used data acquisition : Freeman chain code (FCC)preprocessing : binarization, noise removal, cropping and thinning. Feature extraction : FCC was extracted by using boundary-based style and six global features were calculated against split image to test the feature efficiency Verification : verification utilized Euclidean distance to measure and match in k-Nearest Neighbors.

In [7] Subhash Chandra proposed "Offline Signature Verification based on Geometric Feature Extraction using Arti_cial Neural Network". The methodology used Keywords|O_ine signature; Neural network; Geometric feature; False Acceptance Rate; False Rejection Rate.

In [8] Madhuri R.Deore, Shubhangi M. Handore proposed "Offline Signature Recognition: Artificial Neural Network Approach". The methodologies used are Discrete Wavelet Transform (DWT) and Principal component analysis(PCA) Arti_cial neural network (Back propogation algorithm) is used for the recognition of signature.The major advantage of using wavelet coefficient is its ability to perform local analysis.

In [9] Mohitkumar A. Joshi et al. proposed "Offline Handwritten Signature Verification using Low Level Stroke Features". The methodology used Preprocessing: Noise Removal, Thinning, Image Resizing Feature Extraction-Low Level Stroke (LLS) Verification.

In [10] Amit Kishore Shukla et al. proposed "Offline Signature Verification System Using Grid and Tree Based Feature Extraction". The methodologies used in Offline signature verification are Feature extraction, Euclidian distance model, FAR, FRR, Geometric center, Minimum spanning tree, Delauney triangular ratio, Biometric.

In [11] Karrar Neamah et al. "Discriminative Features Mining for Offline Hand-written Signature Verification". The methodology used Preprocessing-Size Normalizing, Binarization and Morphological Operation, Thinning Algorithm (Skelton) Feature Extraction-Gravity Center Point, Signature Image Division, Graph Generating Phase, Classification phase- graph similarity matching algorithms Validation method- Equal error rate (EER).

In [12] Kruthi.C et al. proposed "Offline Signature Verification using Support Vector Machine". The methodology used signatures scanned in a gray scale scanner. Preprocessing operations like binarization, complementation, filtering, thinning and edge detection. Features such as centroid, centre of gravity, calculation of number of loops, horizontal and vertical profile and normalized area are extracted. SVM developed using SMO. The values from the database are fed to the support vector machine which draws a hyperplane and classifies the signature based on a particular feature value.

In [13] Anjali. R et al.proposed "Offline Signature Verifcation Based on SVM and Neural Network". The methodology used Gray level Distortion, Otsus's Threshold, SVM.

The major advantage of using wavelet coefficient is its ability to perform local analysis.

In [14] Suhail M. Odeh, Manal Khalil proposed "Offline Signature Verification and Recognition: Neural Network Approach". The methodologies used are image pre-processing,

Feature extraction: Eccentricity, skewness, kurtosis, orientation. Pattern recognition through MLP neural networks(BP algorithm). Error rate reduced by 23.7% when compared to other approach.

In [15] Ali Karouni et al. proposed "Offline Signature Recognition using Neural Network Approach". The methodology used Preprocessing (simple shape based geometric features like Area, Center of gravity, Eccentricity, Kurtosis and Skewness) system is initially trained using a database of signatures. Implemented using MATLAB.

III. PROPOSED SYSTEM

The architecture diagram of the proposed system is shown in the figure below:

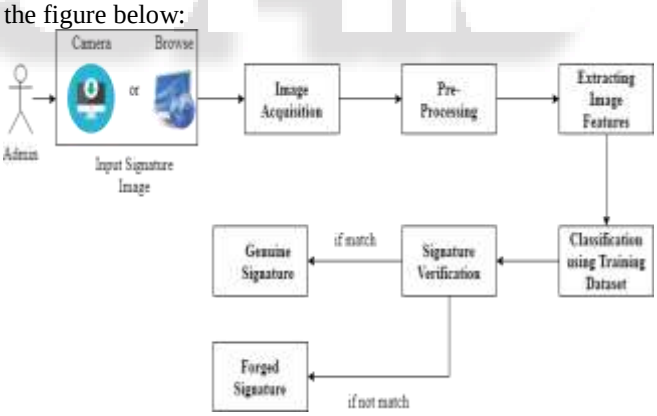

Fig. 1: Architecture diagram

Offline Signature Verification System involves following stages: Signature acquisition, Prepossessing, Feature extraction and Classification.

A. Prepossessing

The purpose in this phase is to make signatures standard and ready for feature extraction. The prepossessing stage includes following steps:

1) Convert to gray image: Here we convert the 3-D image into 2-D image i.e. converting RGB image into black and white image.
2) Background elimination: Data area cropping must be done for extracting features. After thresholding signature

image is white i.e. 1 and background is black i.e. 0. The range of threshold value is in between 0 to 255.

3) Noise removal: When the signature is scanned some noise get add into the signature image. Median filter is used to reduce the amount of variation between intensity of one pixel and other pixel.
4) Scaling: Scaling of signature is required because the size of signature of the same person may get vary. Here signature is resized to 100x100 pixels.
5) Normalization: Signature dimensions may have intrapersonal and interpersonal differences. So the image width is adjusted to a default value and the height will
6) Change without any change on height-to-width ratio.
7) Thinning: Thinning is done to eliminate thickness differences of pen by making image one pixel thick. Here we have used ZhangSuen thinning algorithm.

B. Feature Extraction

Feature extraction process is a significant advance in building up any signature verification framework since it is the way to distinguishing and separating a user's mark from another.

The extracted feature in this framework depends on shape and surface of a picture. Global feature vector is extracted which includes features like width, height, area, circularity feature, vertical and horizontal projections, vertical and horizontal centre point, upper and lower limit, connectivity feature, Global baseline feature and thinning for slant feature. Extracted features are used to train the neural network model.

C. Back Propogation Algorithm

1) Create a Feed Forward Network with inputs, hidden units and output unit.
2) Initialize all network weights to small random numbers.
3) Untill the termination condition is met do for
4) For each signature Do

Propogate the input forward through the network:

a) Input the signature to the network and compute the output of every unit in the network.

Propogate the errors backward through the network:

a) For each network output unit, calculate the error term
b) For each hidden unit, calculate its error term.
c) Update each network weight.

D. Algorithm: Training

Step 1: Authorized user starts the system.
Step 2: Retrieval of a signature images through browsing from a file
Step 3: Preprocessing the signatures by the preprocessing steps.
Step 4: Extract the features of the signature by the feature extraction steps.
Step 5: Check whether training is completed. If not, repeat Step 2 until Feed Forward
Network training model is generated.
Step 6: Stop training.

E. Algorithm: Testing

Step 1: Authorized user starts the system
Step 2: Retrieval of a signature to be tested through browsing from a file or by capturing test signature image.
Step 3: Preprocessing the signature by the steps discussed earlier.
Step 4: Extract the features of the signature by the feature extraction method.
Step 5: Extracted features are sent to the trained neural network.
Step 6: Checking output generated from a neural network declaring signature as genuine or forged
Step 7: Stop testing when task is completed.

IV. RESULTS AND ANALYSIS

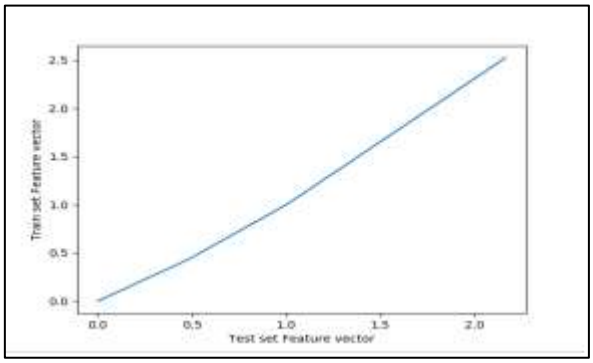

Fig. 2: Generated graph for genuine signature with accuracy 85.52%

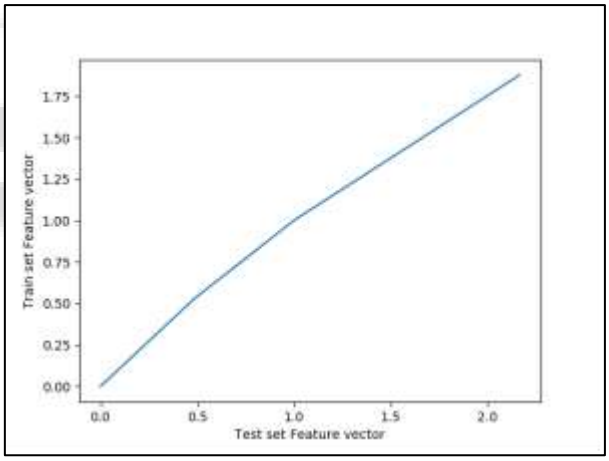

Fig. 3: Generated graph for forged signature with accuracy 80.30 %

V. CONCLUSION AND FUTURE WORK

The project is developed with an objective of providing security at organizations which focuses on having high authentication. The aim is satisfied with the help of machine learning techniques which lets the system capture or browse images of every person and verify whether it is genuine or forged thus preventing illegal activities in their organization.

The developed system provides better accuracy with some delay during training and testing. Future enhancements can be focused by implementing project in systems having high GPU for faster results and low light cameras for better recognition accuracy. It can also be implemented as Android application.

ACKNOWLEDGMENT

This work is a part of a graduation project which is done in Information Science and Engineering department. Many thanks for all who supported and helped us to develop such a system.

REFERENCES

[1] Dewi Suryani, Edy Irwansyah, Ricki Chindra, "Offline Signature Recognition and Verication System using Ecient Fuzzy Kohonen Clustering Network (EFKCN) Al- gorithm",Elseveir 2017.
[2] Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira, "Offline Handwritten Signature Verification - Literature Review" IEEE 2011 978-1-5386-1842-4/17 2017 IEEE.
[3] Indrajit Bhattacharya, Prabir Ghosh, Swarup Biswas, "Offline Signature Verification Using Pixel Matching Technique" Elseveir 2013.
[4] Supriya Singh, Prof. Manjiri Gogate, Prof. Sheetal Jagdale, "Signature Verification Using LDP LBP with SVM Classifiers" International Journal of Scientific Ecience Volume 1, Issue 11.
[5] Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llados, Uma- pada Pal, "SigNet: Convolutional Siamese Network for Writer Independent Oine SignatureVerification" Elseveir 2017.
[6] Aini Najwa Azmi Dewi Nasien Fakhrul Syakirin Omar, "Biometric signature veri- fication system based on freeman chain code and k-nearest neighbor" Springer 2016.
[7] Subhash Chandra, "Offline Signature Verification Based On Geometric Feature Ex- traction Using Artificial Neural Network" 2016.
[8] Madhuri R. Deore, Shubhangi M. Handore, "Offline Signature Recognition: Artifi- cial Neural Network Approach," IEEE ICCP Conference 978-1-4799-8081-9/15 2015 IEEE.
[9] Mohitkumar A. Joshi, "Offline Handwritten Signature Verification Using Low Level Stroke Features" 978-1-4799-8792-4/15 2015 IEEE 2015
[10] Mohitkumar A. Joshi, Mukesh M. Goswami, Hardik H. Adesara, "Offline Signature Verification System Using Grid and Tree Based Feature Extraction "IEEE 2014.
[11] Karrar Neamah, Dzulkifli Mohamad, Tanzila Saba, Amjad Rehman, "Discriminative Features Mining for Offline Handwritten Signature Verification" Springer 2014.
[12] Kruthi C, Deepika C Shet, "Offline Signature Verification Using Support Vector Machine" 978-0-7695-5100-5/13 2013 IEEE DOI 10.1109/ICSIP.2014.
[13] Anjali. R, Manju Rani Mathew, "Offline Signature Verifcation Based on SVM and Neural Network" ISSN Vol. 2, Special Issue 1, December 2013.
[14] Suhail M. Odeh, Manal Khalil, "Off-line Signature Verification and Recognition: Neural Network Approach" IEEE 2011978-1-61284-922-5/11 2011 IEEE.
[15] Karouni, "Offline Signature Recognition Using Neural Network Approach" El- seveir 2010.
[16] Erich Gamma, Richard Hellm, Ralph Johnson and John Vlissides: Design Patterns Elements of Reusable Object-Oriented Software, Pearson Education, 2007
[17] Michael Blaha and James Rumbaugh, Object- Oriented Modelling and Design with UML, 2nd Edition, Pearson Education, 2005, pp21-157.
[18] Satzinger, Jackson and Burd: Object Oriented Analysis and Design with the unified process, scengage learning, 2005

