Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 2: 2025
ISSN : **1906-9685**

ENHANCING SECURITY: INFUSED HYBRID VISION TRANSFORMER FOR SIGNATURE VERIFICATION

K. UDAY KIRAN [1], M.VENKATA RAJESH [2]

[1]Assistant Professor, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

[2]PG Scholar, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT—Every person has a distinctive signature primarily used for personal identification and to confirm the authenticity of important papers or legal transactions. Static and dynamic signature verification are the two types available. While dynamic (online) verification occurs as a person makes their signature on a digital tablet or a similar device, static (offline) verification occurs after an electronic or document signature has been completed. Therefore, using the Support Vector Machine (SVM) algorithm and the K-Means algorithm, an intelligent model is built that gets trained on the real signature data sets and can identify forged signatures based on the available forged signature data sets. Using this model, we can attain maximum accuracy in detecting forgery in signatures. The proposed system achieves an accuracy of 95.83% for forgery detection.

Index terms—Support Vector Machine, Deep Learning, Deep Convolutional Neural Networks

I. INTRODUCTION

Offline signatures are significant today. Offline signature verification and forgery detection are complex and fraught with serious problems. The forging of signatures causes cooperating and commercial organizations to suffer substantial financial losses and damages their security reputation. Forgery is frequently observed in the banking industry since it involves sensitive information, official paperwork, and government regulations (LIC) that could be vulnerable to fraud and its effects. Therefore, a system that can tell the difference between a real signature and a forgery is needed to reduce the likelihood of theft or fraud. The two broad categories of biometrics are physiological and behavioral. A behavioral biometric uses a handwritten signature. It was the first biometric technology to be utilized before PCs and laptops were introduced. The use of handwritten signatures for identity verification in the banking and financial industries dates back many years. The verification procedure is typically carried out manually, either by someone knowledgeable about the signature database or through comparison against a few signature templates. The identification of the signature owners and the determination of whether the signature is authentic, or fake are two different problems that the signature verification system can vigorously address. Not only is the study of signature verification necessary in the field of image processing and pattern recognition. Besides being extensively utilized in money, access control, legal issues, and security, signature verification systems and other signature verification procedures are classified using two unique classes: online and offline. A pointer and an electronic tablet attached to a PC that gathers dynamic signature data are needed for online verification. These emotional traits are individual to each person, sufficiently stable, and repeating. An online signature system recognizes the action of the pen while signing, and these signatures can be validated depending on several factors, including pen pressure and writing speed. These characteristics are unique and difficult to forge.

II. LITERATURE SURVEY

Data collection, picture processing, normalization, clustering, and evaluation are carried out in the project "Offline Signature Recognition and Verification System utilizing Efficient Fuzzy Kohonen Clustering Network (EFKCN) Algorithm" by DewiSuryani, EdyIrwansyah, and Ricki Chindra. RGB to Grayscale Format conversion, binary image conversion, binary image inversion, border removal,and bounding box extraction were the pre-processing techniques used. An accuracy of roughly 70% was attained utilizing this strategy.

n TejasJadhav's paper titled "Handwritten Signature Verification using Local Binary Pattern Features and KNN," the pre-processing methods used: RGB to Gray Scale conversion, Otsu Thresholding, and Boundary box cropping, and feature extraction methods used: LBP image generation, texture features, and name features are used as the feature extraction methods. KNN is used in this methodology together with Euclidian distance. The accuracy of this strategy is 73.34 %.Thresholding, Edge Thinning, Noise Removal, and Noise Removal with Adaptive Filtering are the pre-processing techniques used in the Tansin Jahan, Md. Shahriar Anwar, and S. M. Abdullah Al-Mamun paper titled "A Study on Preprocessing and Feature Extraction in offline Handwritten Signatures." The methods for extracting features from a signature include finding loops and converting the signature's pixels into binary numbers. MATLAB is used in this project to run the model. The Deep Convolutional Neural Networks (DCNN) and Explainable Deep Learning are used to implement the model in the paper titled "An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach" by Hsin-Hsiung Kao and Che-Yen Wen. The pre-processing techniques include rotation, block-based data augmentation, and RGB to grayscale conversion. The accuracy of this model is 94.37%. The pre-processing techniques suggested in the project "OFFLINE SIGNATURE VERIFICATION" by Dr. M. Narayana, L. BhavaniAnnapurn, and K. Mounika included binarization, noise removal, thinning, locating the picture boundary box, solving angular problems, and size normalization. Height/width ratio, OTSU's method, linked component, and threshold are employed as feature extraction techniques. The primary way advocated for detecting signature forgery is Euclidian Distance. The efficiency of this approach was 85.42%. JiveshPoddar, Vinanti Parikh, and Santosh Kumar Bharti's paper, "Offline Signature Recognition and Forgery Detection using Deep Learning," suggests using Convolutional Neural Networks (CNN), the Crest-Trough method, the SURF algorithm, and the Harris corner detection algorithm for the model training. The accuracy of the suggested system is between 85 and 89 percent.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

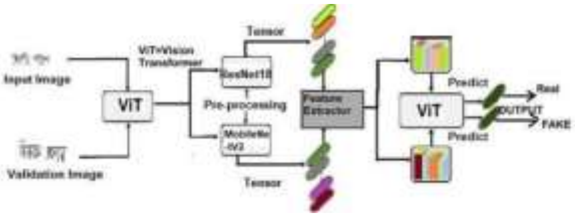

Fig. 1: System Overview

Implementation Modules

Load Dataset

In this phase, load signature images .zip dataset into program and extract the signature images from .zip file.

This data can be analyzed and extract the best features to preprocess the data**.**

Data Augmentation

Data Augmentation is the process of increasing the size of the data set. There are ways in which the process is done by rotating, flipping, shearing, and adding random noise, along with other types.

The new images in the dataset will help in training the network as well as increasing the efficiency of classifying the testing data or the new data.

Preprocessing

In this module, we pre-process the image data and convert the image data into numpy array data. This step is very important to identify the feature of the image data. This extracted features are show as array data and size can be represented as (733, 128, 128, 3).

Train Model

In this module, after spilt data as train and test data in the ratio of 80% and 20% respectively. The train data can be used for train the model and the test data can be used for test the model performance. In this project we applied CNN Model and to train the model we are using fit() method in python programming

Classification

In this module, we used our proposed model to classify the signature whether it is fake or real.

Evaluate Model

In this module, we construct and calculate confusion matrix and classification metrics to further evaluate the models.

Implementation Algorithms

CNN

- In deep learning, a convolutional neural network (CNN, or ConvNet) is a class of artificial neural network (ANN), most commonly applied to analyze visual imagery.
- CNNs are also known as Shift Invariant, based on the shared-weight architecture of the convolution kernels or filters that slide along input features and provide

translation-equivariant responses known as feature maps.

IV. RESULTS

Fig. 2: Home Page

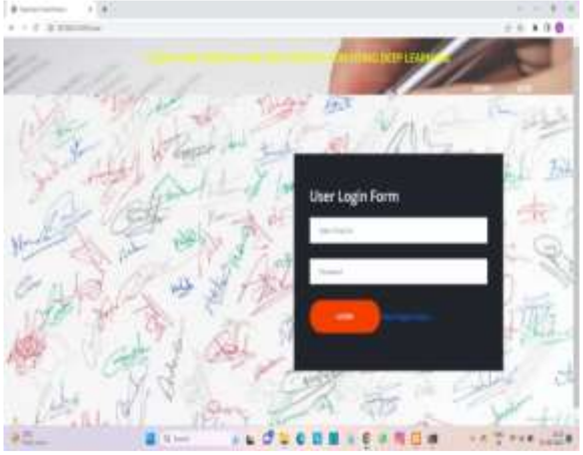

Fig. 3: User Login

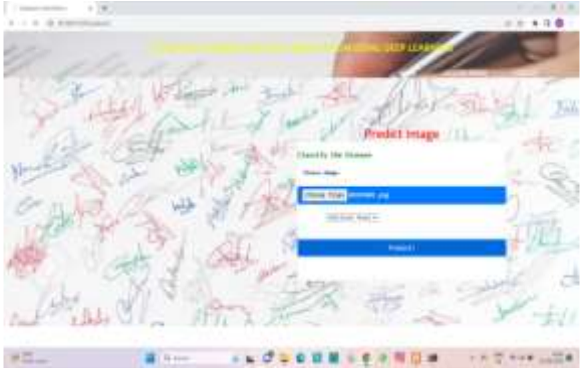

Fig. 4: Predict Image

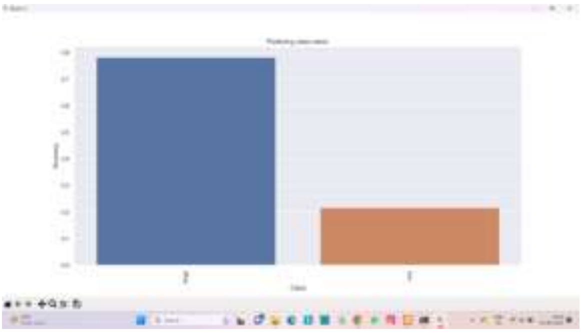

Fig. 4: Comparison Graph

V. CONCLUSION

In today's world, authentication and verification are critical as they can help prevent fraudulent activities, especially signature forgery. Hence it is necessary to build an efficient verification system to classify a signature as real or forged efficiently. efficiently recognize fraudulent activities in the signature of a person using the Support Vector Machine (SVM), which will help us to find complex relationships between data without having to perform any complex transformations on our own. Here, the model is executed in google colabs mainly to see the results required.

REFERENCES

[1] Offline Signature Recognition and Verification System using Efficient Fuzzy Kohonen Clustering Network (EFKCN) Algorithm 2017: DewiSuryani, EdyIrwansyah∗, Ricki Chindra.

[2] Handwritten Signature Verification using Local Binary Pattern Features and KNN 2019: TejasJadhav.

[3] A Study on Preprocessing and Feature Extraction in offline Handwritten Signatures 2015: Sm Abdullah Al-Mamun and Tansin Jahan Daffodil.

[4] An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach 2020: Hsin-Hsiung Kao * and Che-Yen Wen.

[5] Offline signature Verification 2017: Dr. M. Narayana and L. Bhavani Annapurna, K. Mounika.

[6] Offline Signature Recognition and Forgery Detection using Deep Learning: JiveshPoddara, VinantiParikha, Santosh Kumar Bhartia,∗ .

[7] Shahane P.R., Choukade A.S., &Diyewar A.N. (2015) "Online biometric authentication mistreatment Matlab." International Journal Of Innovative analysis in Electrical, Physics, Instrumentation, and management Engineering

[8] Zagoruyko, S., &Komodakis, N. (2015). "Learning to compare image patches via convolutional neural networks." In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 4353-4361).

[9] Fahmy, M. M. (2010). "Online handwritten signature verification system based on DWT features extraction and neural network classification." Ain Shams Engineering Journal, 1(1), 59–70.

[10] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). "Image net classification with deep convolutional neural networks." In Advances in neural information processing systems (pp. 1097-1105).

AUTHORS Profile

Mr. **K.UDAY KIRAN** has received his MCA from BAPATLA ENGINEERING COLLEGE, Bapatla in 2012 He is dedicated to teaching field from the last 2 years. His research area is Cloud Computing. At present he is working as Assistant Professor in MCA Department in QIS College of

Engineering & Technology, Ongole, Andhra Pradesh, India.

Mr. **Malleboina Venkata Rajesh** has received him B.SC(Tally) and degree from ANU 2023 and pursuing MCA in QIS College of Engineering and Technology affiliated to JNTUK in 2023-2025.