Signature Forgery Detection using Machine Learning

Dr.CHANDRA MOHAN,Dr.ECCLESTON

Department of Engineering, Sciences and Humanities (DESH)
Vishwakarma Institute of Technology, Pune, 411037, Maharashtra, India

***Abstract*—**Signature is the most commonly used tool for identification of individuals extracted by previous signatures. Main thing is that signature is very important part in bank because withdrawal of money depends on it. For personal identification, Signature verification is a widely used biometric technique, especially in certain commercial areas such as authenticating checks. Typically, this process relies on human examination of signature samples. In banks, there is no flawless system to determine whether the signatures on checks are genuine or fake.This can lead to bank frauds. Nowadays, cases about fraud signature in banks are increasing. The Project will help to identify whether signature is real or fake. There are two types of verification- online and offline verification. This project is going to implement offline verification by using different geometric measures. This project uses python libraries like TensorFlow, Matplotlib, Pandas, and Keras.

Keywords *— Machine Learning, Computer vision, Signature Verification, Numpy, Tensorflow, Matplotlib, Pandas, Keras, Euclidean distance*

I. INTRODUCTION

This project consists of a signature forgery detection software using a machine learning algorithm in Python, which will be used as an offline signature verification system. Firstly, the algorithm is trained using a dataset of genuine signatures approved by the system.The algorithm will then create a reference signature which the algorithm will refer to when distinguishing further signatures. The system will compare specific parameters between the reference signature and the test signature. If the differences are too significant, the signature will be deemed a forgery.

II. LITERATURE REVIEW

Various methods of signature forgery detection have been seen with varying success.
Shashidhar Sandaused 11 extracted features, grouped them using a GMM (Gaussian Mixture Model) and then used an LCSS model to compare the similarities[1].

Jivesh Poddarused Harris Algorithm and Surf Algorithm, among which the Harris Algorithm gave better results. Prior to using the same, the algorithm is first trained using a Convolutional Neural Network and the Crest-Trough method. Preprocessing methods such as noise removal, scaling, and centralization are used for Convolutional Neural Networks (CNNs), while techniques like length-to-space ratio and width-to-space ratio are employed for the Crest-Trough method[2].

The literature review underscores the importance of deep learning across various fields in artificial intelligence, while acknowledging the common challenge of limited training data. Siamese networks, known for their effectiveness in one-shot learning scenarios, find application in signature verification, a domain where Convolutional Neural Networks (CNNs) are extensively studied. The proposed research introduces a novel combination of

Siamese networks and CNNs, aiming to enhance signature verification by generating a robust embedding vector. This vector is then enriched with statistical measures calculated directly on it, and a contrastive loss function is applied for further refinement. The suggested approach is positioned as an improvement over existing methods, demonstrating superior performance in terms of accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR).This research contributes to advancing signature verification methodologies through innovative combinations of established techniques[3].

Jane Bromley and James W. Bentz present an exploration of advanced techniques for signature verification. The core of their contribution lies in the introduction and detailed investigation of a Siamese time delay neural network, meticulously dissecting its architectural intricacies and distinctive features. The paper illuminates the network's capability to discern nuanced patterns within signatures, positioning it as a promising solution to the challenges inherent in signature authentication. Bromley and Bentz's work not only enhances our understanding of signature verification but also marks a significant stride in the application of neural networks to this domain, offering potential breakthroughs for improving the accuracy and reliability of signature recognition systems in the broader landscape of pattern recognition and artificial intelligence[4].

The writers conduct a thorough investigation into the authentication of online signatures, taking into account the direction of pen movement. To evaluate the efficacy of this strategy, extensive experimentation is used in the study. Yoshimura and Yoshimura offer thorough results that rigorously assess the influence of adding pen movement direction in the verification process through a methodical experimental design and implementation. The experimental results are presented, and the usefulness of this subtle characteristic in online signature verification is statistically evaluated. The research offers quantitative insights. This thorough analysis of experiment data sheds insight on the real-world applications and possible improvements in signature verification techniques, making significant technological contributions to the field of handwriting recognition[5].

Lorette and R. Plamondon explore complex techniques for handwritten signature authentication, emphasizing dynamic features. In order to capture and evaluate the complex temporal and geographical properties inherent in the process of writing a signature, the study investigates dynamic methodologies that go beyond static signature analysis. The authors carefully outline and expound upon these dynamic approaches, exploring the technical nuances and theoretical underpinnings that support their use in the verification of handwritten signatures[6].

Ali Karouni, Bassam Daya and Samia Bahla present an innovative approach to offline handwritten signature recognition and verification using the multi-layer perceptron (MLP) and Self Organizing Map (SOM) neural networks. The system involves data acquisition, pre-processing, feature extraction, and recognition/verification stages, capitalizing on the advantages of offline feature extraction. MLP and SOM are employed to capture behavioral biometrics from signatures in a signature database with samples from 10 individuals. Pre-processing steps enhance system performance, and features like image area, pure width and height, vertical and horizontal centers, and eigenvalues contribute to system robustness. The experimentation details the use of MLP and SOM for clustering and unsupervised training, yielding promising results in terms of False Rejection Rate (FRR), False Acceptance Rate (FAR), and Total Error Rate (TER). The SOM-based system achieves a minimum TER at 103 iterations, indicating effectiveness. Future work includes increasing the reference sample size and exploring hybrid systems for enhanced signature verification[7].

The authers utilize offline handwritten signature verification system comprising four steps: preprocessing, feature extraction, feature selection using a genetic algorithm, and feature verification through support vector machine (SVM). The proposed method addresses the challenges of discriminating between genuine signatures and skilled forgeries. Notably, it

incorporates a new feature set with both horizontal and vertical features. Experimental results on datasets such as MCYT, GPDS synthetic, and CEDAR demonstrate the system's effectiveness, evaluated through error rate measures including FAR, FRR, and AER[8].

This paper explores the challenges and advancements in offline signature verification, emphasizing the significance of distinguishing between genuine and forged signatures to prevent fraud. The study reviews the historical use of handcrafted features and recent applications of deep learning techniques in this domain. The offline verification process involves data acquisition, pre-processing, feature extraction, and classification. Two primary models for signature verification, Writer-Dependent and Writer-Independent, are discussed, along with engineering-based and deep learning-based approaches. Performance parameters such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Accuracy (ACC), Equal Error Rate (EER), and Average Error Rate (AER) are introduced. The paper provides an overview of publicly available datasets for offline signature verification and concludes by outlining the proposed methodology and expected outcomes[9].

The paper discusses the design and testing of on-line dynamic signature verification systems. Over 10,000 signatures were collected using a graphics tablet, and feature sets were extracted and analyzed for effective signature verification. Notably, the majority classifier, with modifications like presoft and prehard decisions, demonstrated reliable performance suitable for Point-of-Sale (POS) applications, achieving low error rates and adaptability to variations in writing speed. The system's effectiveness was confirmed through extensive experiments and comparison with simulated data. The findings support the feasibility of an adaptive and real-time signature verification system for POS applications[10].

III. METHODOLOGY/EXPERIMENTAL

A. Algorithm

The implemented algorithm utilizes a Multi-Layer Perceptron (MLP), a type of artificial neural network. This MLP is structured as a feedforward neural network, consisting of multiple layers, including an input layer, three hidden layers labeled as h1, h2, h3, and an output layer.Within the input layer, nodes correspond to features extracted from signature images. The activation function employed in each hidden layer is the hyperbolic tangent (tanh), with distinct numbers of neurons specified as n_hidden_1,n_hidden_2, and n_hidden_3 respectively. The output layer (out) contains nodes representing classes, distinguishing between genuine and forged signatures, and utilizes the tanh activation function. TensorFlow variables define the model's parameters, encompassing weights and biases for each layer, which are dynamically adjusted during the learning process. The training procedure minimizes the mean squared difference between predicted outputs and actual labels, facilitated by the Adam optimizer. Backpropagation is integral during training, fine-tuning weights and biases to align predicted outputs closely with ground truth.

Post-training, model accuracy is assessed on both training and testing datasets, involving an evaluation based on mean squared differences and softmax activation for deriving class probabilities. Fundamentally, this algorithm embodies a supervised learning approach, where the neural network learns to distinguish between genuine and forged signatures by leveraging extracted features. Training is orchestrated through the backpropagation algorithm, empowered by the Adam optimizer.

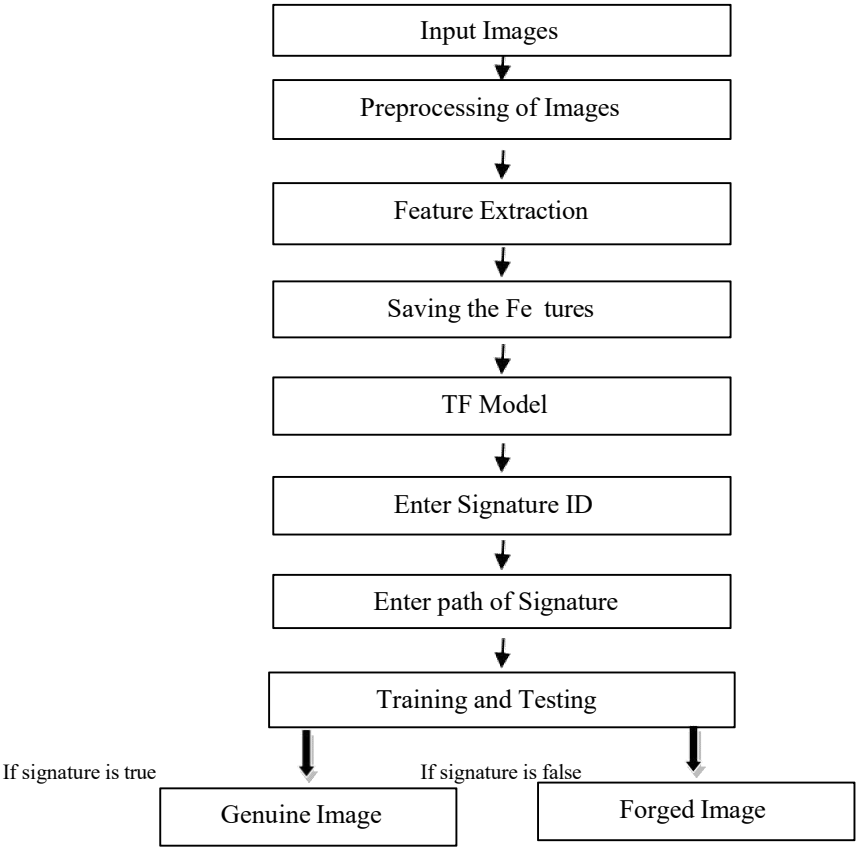

Fig. 1. Flow chart of the process

The system initiates the user interaction by prompting for the User ID as the initial input. Users are required to input their unique ID into the system for further processing. Subsequently, the system proceeds to perform ID verification by checking whether the entered user ID is already registered in the system.

In cases where the user ID is not registered, the system prompts the user to provide five sets of signatures for training purposes. This training data will contribute to building a reference for future verification.

Upon successful registration or if the user ID is already registered, the system prompts the user to provide a signature for testing. The provided signature, along with the previously obtained training signatures, undergoes a pre-processing stage to enhance the quality of the input data.

During the pre-processing stage, both the input training signatures and the testing signature are prepared for further analysis. The pre-processed training signature is then saved as a reference signature in the system's database for future verifications. Similarly, the pre-processed testing signature is saved as a sample signature for the upcoming verification process.

The system advances to the Verification stage, where the sample signature is compared with the reference signature stored in the database. A crucial step follows with a Difference Analysis, examining whether the dissimilarity between the two signatures surpasses a predefined Threshold value.

When the calculated difference remains within the predefined threshold, the sample signature is validated as genuine and accepted. However, if the difference surpasses the set threshold, the sample signature is flagged as potentially forged and rejected. The final decision of the verification process determines whether the provided signature is accepted as authentic or dismissed as potentially fraudulent. This methodology establishes a dependable and secure system for signature verification, bolstering protection against forgery in user-provided inputs. Through its capacity to discern between authentic and forged signatures, this approach elevates the security and reliability of signature-based authentication systems.

IV. RESULTS AND DISCUSSIONS

In our program, only five images have been used to create a reference signature.As a method of further optimization, users can use more than five images to create a reference signature for each user, so that the algorithm will be able to properly classify discrepancies as random errors or forgery errors. This will further increase the accuracy but will also increase the amount of data to be collected initially.

Also, nine parametershave been considered in the program such as skewness over x and y axes, solidity, eccentricity, etc which give a complete definition of a signaturefor the program. For further improvements, one can use more parameters such as angle sines and cosines and thickness of pressure points.

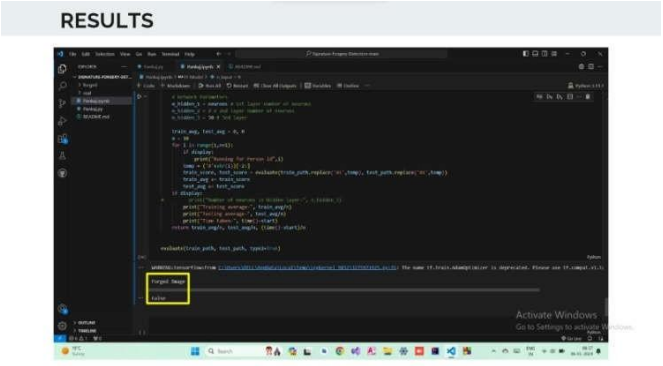

Fig. 1. Forged Image (program returns ‘False’)

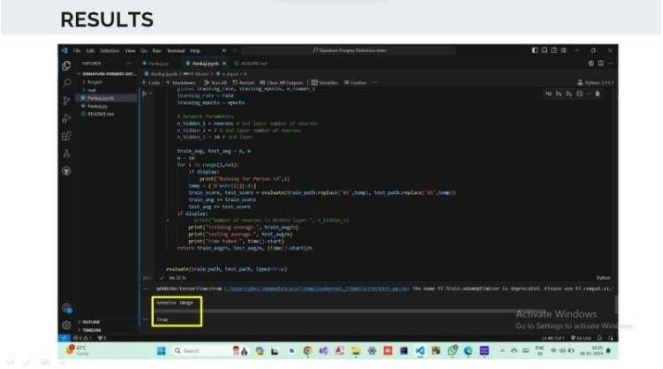

Fig. 2. Genuine Image (program returns ‘True’)

V. FUTURE SCOPE

There is scope for improvement in our project as well. The dataset used for now is pretty small in size, and is thus limited. Most machine learning projects in industry are much larger than the one that has been used here. Moreover, there may be mistakes made by the machine learning algorithm in the training phase or the test phase which will skew the results in an unfavorable way. There is also a scope to improve the accuracy of the algorithm by taking into account random human errors, such as when signatures drawn by the same person might not be exactly similar.

VI. CONCLUSION

AKeras neural network has been used to create a machine learning algorithm. It has then been trained using a dataset to recognize signature forgeries. However, there is still some fine-tuning needed for the algorithm to be able to be used in industry settings. This fine-tuning includes further improving the accuracy, reducing the effect of random errors and using a larger dataset in the training phase.

VII. ACKNOWLEDGMENT

All authors would firstly like to thank our project guide Prof. S. S. Telsang for her wonderful insights and help, without whom this project would not have come to fruition. All authors extend their gratitude to Vishwakarma Institute of Technology for affording us the chance to demonstrate our skills by tackling this challenge. Additionally, we express our heartfelt thanks to our peers for their steadfast support and encouraging words.

VIII. REFERENCES

[1] s. sanda, “online signature verification using gaussian mixture models and longest common sub sequence” department of applied signal processing blekinge institute of technology se–371 79 karlskrona: pg 12-18

[2] J. Poddar, V. Parikh, S. K. Bharti “Offline Signature Recognition and Forgery Detection using Deep Learning,” The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40), April 6 - 9, 2020, Warsaw, Poland: pg 3-5

[3] Amruta Jagtap, Dattatray D. Sawat and Rajendra Hegadi, "Verification of genuine and forged offline signatures using Siamese Neural Network", *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 35109-35123, 2020.

[4] Jane Bromley and James w. bentz, "Signature verification using a siamese time delay neural network", *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 5, pp. 358-370, 1993.

[5] Yoshimura and M. Yoshimura, "On-line signature verification incorporating the direction of pen movement - an experimental examination of the effectiveness", in From pixel, to features III: frontiers in Handwriting recognition, Eds. S. Impedova and J. C. Simon, Elsevier, 1992.

[6] Lorette and R. Plamondon, "Dynamic approaches to handwritten signature verification", in Computer processing of handwriting, Eds. R. Plamondon and C. G. Leedham, World Scientific, 1990.

[7] Ali Karouni, Bassam Daya and Samia Bahla, "Neural Network Based Offline Signature Recognition and Verification System", *Procedia Computer Science*, vol. 3, pp. 155-161, 2011.

[8] Muhammad Sharif, Muhammad Attique Khan and Muhammad Faisal, "A framework for offline signature verification system", *Pattern Recognition Letters*, vol. 139, 2018.

[9] Neha Sharma, Sheifali Gupta and Puneet Mehta, "A Comprehensive Study on Offline Signature Verification", *Journal of Physics Conference Series*, vol. 1, pp. 12-44, 1969.

[10] Lee Luan Ling et al., "Reliable online human signature verification systems", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 6, pp. 643-647, 1996.

[11] Othman Omran Khalifa, M.K. Alam and Aisha Hassan Abdalla Hashim, "An evaluation on offline signature verification using artificial neural network approach", *International Conference on Computational Intelligence and Design (ISCID)*, 2013.

[12] H. Baltzakis and Nikos Papamarkos, "New signature verification technique based on a two-stage neural network classifier", *Engineering Applications of Artificial Intelligence*, vol. 14, no. 1, pp. 95-103, 2001.
[13] Subhash Chandra and Sushila Maheskar, "Offline signature verification based on geometric feature extraction using artificial neural network", *Conference: 2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, 2016.
[14] Syed Khaleel Ahmed, Syed Khaleel Ahmed and Azhar Khairuddin, "Automatic online signature verification: A prototype using neural networks", *IEEE Region 10 Conference*, 2009.
[15] Tai-Ping Zhang, Bin Fang, Bin Xu, Heng-Xin Chen, Miao Chen and Yuan-Yan Tang, "Signature envelope curvature descriptor for offline signature verification", *2007 International Conference on Wavelet Analysis and Pattern Recognition*, 2007.
[16] Tong Qu and Abdulmotaleb El Saddik, "Dynamic signature verification system using stroked based features", *in The 2nd IEEE Internatioal Workshop on Haptic Audio and Visual Environments and Their Applications*, 2003.
[17] Vu Nguyen, Michael Blumenstein and Graham Leedham, "Global Features for the Off-Line Signature Verification Problem", *10th International Conference on Document Analysis and Recognition*, vol. 11, pp. 780-800, 2009.
[18] Zehua Zhang, Xiangqian Liu and Yan Cui, "Multi-phase Offline Signature Verification System Using Deep Convolutional Generative Adversarial Networks", *9th International Symposium on Computational Intelligence and Design (ISCID)*, 2016.
[19] I. Guyon, P. Albrecht, Y. LeCun, J. S. Denker and W. Hubbard, "A Time Delay Neural Network Character Recognizer for a Touch Terminal", Pattern Recognition, (1990).