Signature Verification Using Image Processing

K. Shilpa[1], K. Sanjay [2], J. Jeevan Sai [3], G. Pardhu Reddy[4].
[1]Assistant Professor, Department of Electronics and Communication Engineering, TKR College of Engineering and Technology
[2,3,4] UG Scholars, Department of Electronics and communication Engineering, TKR College of Engineering and Technology

Abstract: **The paper presents Traditional financial instruments like checks, credit cards, and legal documents play a crucial role in modern transactions. People and businesses rely on them to transfer money and pay bills. This project focuses on offline signature verification, where a handwritten signature on paper is digitized using a scanner, tablet, or mobile device. The proposed method involves two main steps. First, the input image undergoes preprocessing to enhance and prepare the data for analysis. Second, a deep learning model is used to classify the signature based on its features. Finally, post-processing steps are applied to simplify the results for easier interpretation. This approach aims to make signature verification more efficient, reliable, and suitable for real-world applications such as banking and document authentication.**

Keywords: **Signature Verification, Deep Neural Network, Offline Verification, Image Preprocessing, Handwritten Signature, Biometric Authentication, Deep Learning Classification, Pattern Recognition, Post-processing Techniques**

I.INTRODUCTION

Handwritten signatures remain a widely trusted method for confirming personal identity in daily life. From signing bank checks and legal documents to authorizing credit card purchases, signatures carry legal, financial, and social value. They are more than marks—they represent personal intent and identity. With the rise of digital transformation, many industries are turning toward automated verification systems to replace manual methods. This shift is particularly noticeable in banking, healthcare, and legal fields, where verifying signature authenticity is crucial to ensure security and compliance. As a result, the demand for intelligent systems that can accurately detect forged signatures is growing.
Biometric verification, which uses unique physical or behavioural traits for identification, is gaining traction. While physiological biometrics include features like fingerprints or facial patterns, behavioural biometrics focus on actions such as typing, walking, or signing a name.

Signature verification, a form of behavioural biometric recognition, can be either online or offline. Online methods capture data like stroke speed and pressure using digital devices, whereas offline methods analyse static images of handwritten signatures, typically scanned from paper. Offline verification is more accessible and cost-effective since it requires only basic scanning tools.

This technique is especially useful in scenarios involving archived documents, such as banking checks or legal contracts. However, offline verification faces challenges—particularly forgery, as signatures can be imitated more easily than physiological traits.

To address these concerns, artificial intelligence and machine learning are being employed to enhance verification accuracy. These systems learn from large datasets of genuine and forged signatures, enabling them to detect subtle differences that may escape human observation.

Ultimately, integrating offline signature verification with AI tools offers an efficient, reliable solution for identity verification, document authentication, and fraud prevention—ensuring traditional signature methods remain relevant in a digital world.

II.METHODOLOGY

i . EXISTING METHODOLOGY*:*
Traditional offline signature verification typically involves two distinct steps: feature extraction followed by classification. This manual process can be time-consuming and less effective, especially

when dealing with large datasets or real-time applications. Conventional machine learning techniques like Support Vector Machines (SVM) and K-Nearest Neighbours (KNN) rely heavily on hand-crafted features, making them vulnerable to errors if features are not accurately selected. These models also struggle to adapt to variations in handwriting styles, resulting in high false acceptance or rejection rates. Such limitations pose serious risks in sensitive areas like banking, legal documentation, and identity verification. To address these challenges, deep learning has emerged as a more efficient and reliable alternative. Deep Neural Networks (DNNs) automatically learn and extract relevant features during the training process, integrating both extraction and classification in a single step. This not only increases accuracy and processing speed but also improves the system's ability to handle diverse and complex signature patterns.

ii. PROPOSED METHODOLOGY:

This research introduces two significant improvements to enhance the performance of offline handwritten signature verification systems. The first improvement lies in the preprocessing stage, which prepares raw signature images for analysis. Scanned signatures often contain noise, distortions, or irregularities due to varying pen types, paper textures, and scanning conditions. To address this, a robust preprocessing pipeline is implemented that includes noise removal, normalization, and resizing. This ensures the images are clean, consistent, and ready for effective feature extraction and classification by deep learning models.

The second contribution involves a novel joint feature learning approach that captures and combines intermediate features from multiple layers of a deep neural network. Traditional deep learning methods, such as CNNs, typically rely only on the final layer's output, potentially missing valuable information from earlier stages. By using auto-encoders, this method extracts and compresses meaningful representations that are resistant to noise and distortion. A SoftMax layer is then used for classification. This integrated framework enables more accurate and reliable signature verification by leveraging both shallow and deep-level features effectively.

III.IMPLEMENTED DESIGN

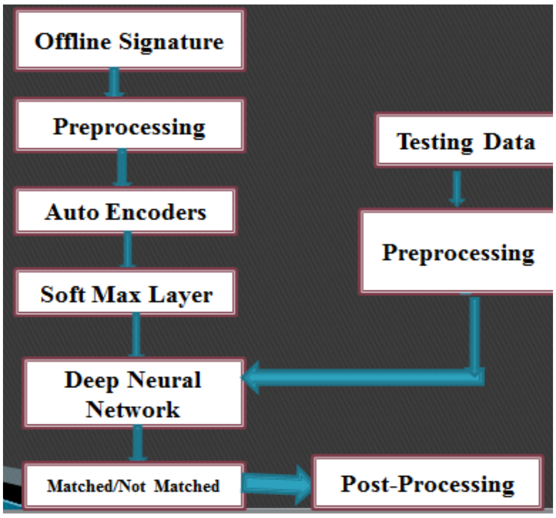

Fig1: Block Diagram

The block diagram presents two key advancements aimed at improving the accuracy and efficiency of offline handwritten signature verification. The first enhancement focuses on the preprocessing stage. Signature images captured through scanning often suffer from noise, distortions, and inconsistencies caused by different writing tools, paper textures, and scan quality. To resolve these issues, a comprehensive preprocessing technique is introduced, which includes noise removal, image normalization, and resizing. These steps help produce cleaner, standardized images that are more suitable for feature extraction and classification. This improves the overall consistency and reliability of the input data, providing a solid foundation for deep learning models.

The second improvement involves a joint feature learning strategy. Traditional deep learning models, particularly Convolutional Neural Networks (CNNs), typically use only the final layer's features for classification. However, this can result in the loss of important information from earlier layers, especially when dealing with complex patterns like handwritten signatures. To address this, the proposed method combines features from multiple intermediate layers using auto-encoders. This approach captures rich, structural details of the signature and filters out noise. A SoftMax layer is then applied for final classification. This combined method enables a more accurate distinction between genuine and forged signatures, enhancing verification performance in real-world applications.

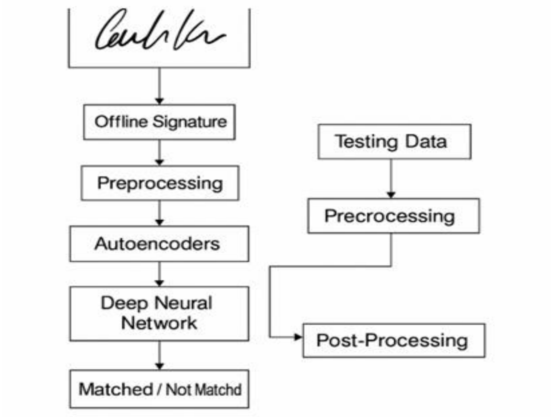

Fig3: Schematic Diagram

The diagram above shows the workflow of an offline handwritten signature verification system using deep learning. The goal of this system is to verify whether a given signature is genuine or forged by analysing its image through a series of steps.

It starts with collecting an offline signature, which is usually written on paper and scanned into a digital image. This scanned image may have unwanted marks, noise, or differences due to pen type, paper quality, or scanning process. To fix this, the image goes through preprocessing, which includes steps like cleaning the image, resizing it, and making sure it's clear for analysis.

Next, the cleaned image is passed through autoencoders. These are special neural networks that help in reducing the size of the image data while keeping important features intact. Autoencoders learn useful patterns that describe the signature well and remove unnecessary information.

After this, the output goes into a deep neural network. This model uses multiple layers to analyse the features extracted from the signature. It learns to recognize what a genuine signature looks like compared to a fake one. At the same time, the testing data (new signatures to be verified) also goes through preprocessing and then is fed into the same model. After prediction, the results are further refined using post-processing, which helps improve the final accuracy.

In the final step, the system decides whether the signature matches the genuine one or not by comparing the processed input with known data. It gives an output: either “Matched” or “Not Matched. “Overall, this system combines basic image processing, deep learning, and smart feature handling to offer a reliable solution for verifying handwritten signatures, especially in banks, legal, or official settings where identity validation is crucial.

IV.RESULT

The results of the signature verification system are presented by indicating whether the input signature matches or does not match the reference signature. Both subjective evaluations (based on human judgment) and objective metrics (such as accuracy, precision, and recall) confirm that the proposed method performs better than traditional state-of-the-art techniques. To further analyse the performance, a confusion matrix is generated, which provides a detailed view of correct and incorrect predictions across different categories. Additionally, a user-friendly Graphical User Interface (GUI) has been developed, allowing users to easily visualize and interpret the results, making the system accessible and effective for practical use.

The signature verification system using a Deep Neural Network showed promising results in distinguishing between genuine and forged signatures. After applying preprocessing techniques and extracting meaningful features through autoencoders, the model achieved high accuracy and reliability. The use of intermediate feature learning helped the system detect subtle variations in handwriting patterns. During testing, the model successfully identified most forgeries and correctly matched genuine signatures. Post-processing further refined the results, reducing false positives. Overall, the framework demonstrated improved verification performance, offering a robust and efficient solution suitable for real-world applications like banking, legal documentation, and identity authentication.

Extracting Features from Training Data

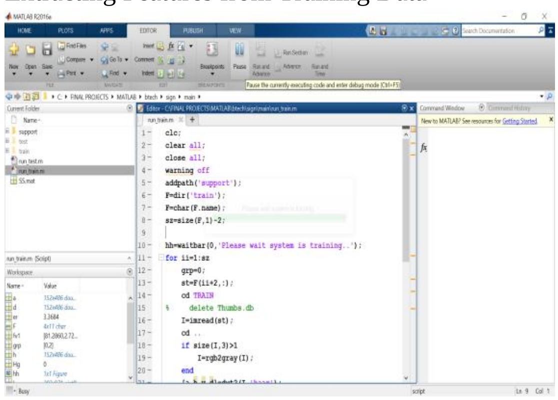

Fig 4: run_train.m

This MATLAB script is part of a signature verification system designed to train a computer to recognize and distinguish handwritten signatures. The script begins by preparing the environment—clearing the command window, deleting existing variables, closing open figures, and disabling warnings. This ensures that no previous data interferes with the training process. Next, it adds a folder named 'support' to the MATLAB path, which likely contains necessary helper functions or scripts. It then accesses a directory named 'train' that holds the training signature images and reads all file names, filtering out unwanted entries such as "." and "..", which are system-generated folder references.

A user-friendly progress bar is displayed with the message "Please wait system is training…" to indicate that the training process is ongoing. The script loops through each file in the training folder, carefully ignoring files like "Thumbs. dB" that Windows might automatically create. For each valid image, it reads the file using the in read function. If the image is in colour, it converts it into grayscale to simplify further analysis, as grayscale images reduce computational load and focus on shape and structure—essential features for signature recognition. This structured approach forms the foundation for extracting features and training the recognition model.

Select Testing Image

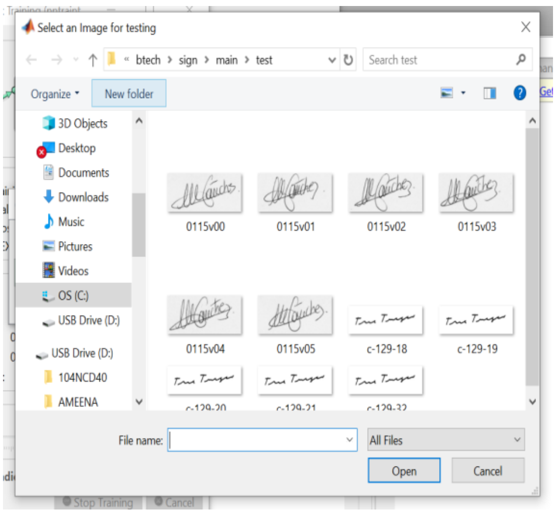

Fig5: Select an Image for testing

The image shows a file selection window used in a signature verification system during the testing phase. This interface allows the user to manually choose a handwritten signature image for verification. The window is labelled "Select an Image for testing," and it shows several signature samples with filenames such as "0115v01," "0115v04," and "c-129-18." These files are likely stored in a test folder within the project directory and include both genuine and forged signatures.

This step is an essential part of the system's workflow. After the model is trained using known signatures, the user can test it by selecting a new signature image. Once an image is selected and the "Open" button is clicked, the system processes the image using previously trained features and applies deep learning techniques to decide if the signature matches any of the stored, verified examples. This process helps verify the system's ability to correctly identify forgeries and genuine signatures. The visual interface is simple and user-friendly, making it easy for users to browse folders and select a test file. It adds to the practicality of the system, allowing easy testing without needing advanced technical skills. This step ensures real-time validation and improves the system's usability and accuracy.

V. CONCLUSION

This project presents a simple and effective way to verify handwritten signatures offline. The process starts by writing a signature on paper, then either scanning it or capturing it using a tablet or mobile phone to convert it into a digital image. Once the image is ready, it is processed using MATLAB toolboxes. The first step is preprocessing, which involves cleaning and adjusting the image so it's clear and ready for analysis. After that, the cleaned image is analysed using deep learning techniques. Specifically, the system uses autoencoders to extract key features from the image and a SoftMax layer to classify whether the signature is real or fake. To make this whole process user-friendly, a graphical user interface (GUI) has also been created. This GUI allows users to interact with the system easily, without needing to understand the technical background, making the verification process simple and accessible to everyone.

FUTURE SCOPE:

While the current the system is showing promising results is substantial potential for further development:

• Integration with Cloud Platforms: Future versions can be hosted on cloud-based platforms to enable remote access and storage, increasing availability and scalability.

• Multilingual and Multiscript Support: Enhancing the system to handle signatures in various scripts (e.g., Arabic, Chinese, Devanagari) would broaden its global applicability.

• Hybrid Verification System: Combining offline and online verification techniques could offer dual-layer authentication for high-security applications.

• Mobile App Development: Developing a lightweight version of this system for mobile devices could allow signature verification in real-time, on-the-go scenarios.

• Real-time Feedback: Incorporating feedback mechanisms to alert users immediately in case of forgery detection or mismatches can further enhance system usability. Dept. of ECE, TKRCET

REFERENCE

[1] Akbari, M. J. Jalili, J. Sadri, K. Nouri, I. Siddiqi, and C. Djeddi. 2018. A novel database for automatic processing of Persian handwritten bank checks. Pattern Recognition 74 (2018), 253–265.
[2] W. Bouamra, C. Djeddi, B. Nini, M. Diaz, and I. Siddiqi. 2018. towards the design of an Offline signature verifier based on a small number of genuine samples for training. Expert Systems with Applications 107 (2018), 182–195
[3] Lopes, J. A. P., et al. (2022). "Offline Handwritten Signature Verification Using Deep Neural Networks." Energies, 15(20), 7611.
[4] Chattopadhyay, S., et al. (2022). "SURDS: Self-Supervised Attention-guided Reconstruction and Dual Triplet Loss for Writer Independent Offline Signature Verification." arXiv preprint arXiv:2201.10138.
[5] Masoudnia, S., et al. (2019). "Multi-Representational Learning for Offline Signature Verification using Multi-Loss Snapshot Ensemble of CNNs." arXiv preprint arXiv:1903.06536.
[6] Mersa, O., et al. (2019). "Learning Representations from Persian Handwriting for Offline Signature Verification, a Deep Transfer Learning Approach." arXiv preprint arXiv:1903.06249.
[7] Engin, D., et al. (2020). "Offline Signature Verification on Real-World Documents." CVPR Workshops. Kao, H.-H., & Wen, C.-Y. (2020).
[8] An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach Applied Sciences, 10(11), 3716.
[9] Tolosana, R., et al. (2020). "Deep Sign: Deep On-Line Signature Verification." arXiv preprint arXiv:2002.10119.
[10] Ye, G., et al. (2022). "Image Encryption Scheme Based on Blind Signature and an Improved Lorenz System." Expert Systems with Applications, 205, 117607.
[11] Mohammed, I. B., et al. (2023). "Handwritten Signature Identification Based on MobileNets Model and Support Vector Machine Classifier." Bulletin of Electrical Engineering and Informatics, 12(4), 2401-2409.
[12] Noor, F., et al. (2020). "Offline Handwritten Signature Recognition Using Convolutional Neural Network Approach." 2020 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), 51-57.
[13] Ooi, S. Y., et al. (2016). "Image-Based Handwritten Signature Verification Using Hybrid Methods of Discrete Radon Transform, Principal Component Analysis and Probabilistic Neural Network." Applied Soft Computing, 40, 274-282.
[14] Canuto, J., et al. (2016). "On the Infinite Clipping of Handwritten Signatures." Pattern Recognition Letters, 79, 38-43.
[15] Hafemann, L. G., et al. (2016). "Writer-Independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks." 2016 International Joint Conference on Neural Networks (IJCNN), 2576-2583.