Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

Automatic Signature Verification for Enhanced Document Security

Vedashri Burghate
Information Technology, Department
Prof. Ram Meghe Institute of Technology & Research, Badnera.
Amravati, India

Suhani Kharode
Information Technology, Department
Prof. Ram Meghe Institute of Technology & Research, Badnera.
Amravati, India

Harsh Dhongade
Information Technology, Department
Prof. Ram Meghe Institute of Technology & Research, Badnera.
Amravati, India

Devashish Wankhade
Information Technology, Department
Prof. Ram Meghe Institute of Technology & Research, Badnera.
Amravati, India

Prof. Dr. A. W. Burange
Information Technology, Department
Prof. Ram Meghe Institute of Technology & Research, Badnera.
Amravati, India

***Abstract* — Signatures have long been essential for transactions and consenting to responsibilities. However, both online and offline signatures can be easily forged due to a lack of robust security measures. Extensive research has been conducted to develop accurate and reliable systems for signature recognition and verification. The effectiveness of these models is typically assessed using metrics such as precision, recall, accuracy, and the F1 score, ensuring they perform well on new data. Once validated, these models can be implemented in various practical settings, including banking, legal documentation, and access control. Findings suggest that Convolutional Neural Networks (CNNs) are predominantly used for recognizing offline signatures.**

Keywords — Offline Signature Verification, CNN (Convolutional Neural Network).

I. INTRODUCTION

Each individual possesses a distinct signature, which plays an essential role in identity verification and the authentication of important legal documents. Signature verification can be categorized into two main types: static and dynamic. When developing a signature verification system, several key factors must be considered, including user acceptance, required security level, accuracy, cost, and ease of implementation. The primary goal of signature verification is to verify the authenticity of a signature, distinguishing between forged and genuine signatures. This task becomes particularly challenging in offline contexts, where the verification relies on images of scanned signatures and lacks dynamic data about the signing process.

In the digital age, where secure authentication is paramount, biometric systems play a pivotal role in ensuring the integrity of sensitive transactions and access control. Among these, handwritten signatures remain a widely adopted form of personal identification. However, the traditional methods of signature verification face challenges posed by variations in writing styles, making it imperative to employ advanced technologies for accurate and efficient authentication. This paper introduces a state-of-the-art signature verification system leveraging the strength of Convolutional Neural Networks (CNNs) have shown impressive effectiveness in image recognition, which makes them ideal for the complex challenge of analyzing and verifying handwritten signatures. Their popularity stems from their capacity to automatically extract hierarchical features from raw data, allowing the system to identify subtle patterns in signatures that traditional methods might miss.

The significance of signature verification extends across diverse sectors, from financial transactions to legal document authentication. CNNs, known for their ability to extract features and learn hierarchically, offer a valuable approach to improving the accuracy and reliability of signature authentication systems. This paper examines the architecture, training methods, and versatility of a CNN-based signature verification system, seeking to advance the development of biometric authentication technologies. Through this exploration, we seek to address the inherent challenges of signature verification, ultimately fortifying the security of digital interactions in our interconnected world.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

II. LITERATURE REVIEW

In the work [1], they focus on handwritten signature verification which is crucial in fields like biometrics, security, and finance, with applications across legal, governmental, and commercial sectors. This study reviews existing frameworks for automatic handwritten signature verification systems, focusing on key areas like preprocessing strategies, feature extraction techniques, and verification models. A comparative analysis of selected studies is provided, along with an evaluation of various signature databases to determine the best frameworks for different datasets. The paper also highlights future directions for developing more robust systems capable of handling diverse languages and signature styles, offering valuable insights for further research and innovation.

In the study [2], Signature verification is critical for document authentication, particularly for detecting forgery in the presence of distortions like rotation, scaling, and noise. This paper introduces a writer-dependent signature verification method that fuses hand-crafted features with one-dimensional convolutional neural network (1D-CNN) features to handle variations in the verification process. The feature extraction methodology is validated using a bagged ensemble learning technique, where the final decision is made through majority voting among machine learning classifiers. The approach is tested on three publicly available datasets, demonstrating its effectiveness and outperforming other existing systems documented in the literature.

In the paper [3], Online signatures are a widely accepted biometric for authentication and identification purposes. While various approaches and algorithms exist for on line signature verification, machine learning techniques have become prominent in recent years. This document presents an online signature verification system using logistic regression. The system was tested on the SVC2004 database, with different feature combinations applied to evaluate performance. The results demonstrated high accuracy, ranging between 91.7% and 98.08%, showcasing the system's effectiveness in online signature verification.

In the work [4], Handwritten signature verification plays a crucial role in biometrics, security, and finance, with applications across legal, governmental, and commercial sectors. Recent advancements in machine learning have significantly improved traditional verification methods. This study offers a comprehensive review of the existing frameworks for automatic handwritten signature verification systems, with a focus on feature extraction, preprocessing techniques, and verification models. It also includes a comparative analysis of selected studies and evaluates various signature databases based on specific parameters to identify the most suitable framework for different datasets. The paper highlights future directions for developing advanced systems capable of handling diverse languages and signature styles, providing valuable insights for further innovation and research in the field.

In their review of IoT's role in smart city development, the work [11] highlight IoT's strengths in managing data connectivity and privacy. These principles are also essential in the context of automatic signature verification, where secure data management and privacy are critical. The capability of IoT to facilitate seamless, secure data exchanges aligns with enhanced document security needs, as IoT-driven frameworks enable automated verification by allowing devices to share and process sensitive information while maintaining privacy.

III. PROPOSED WORK

The proposed signature verification system employs a deep learning architecture Built on Convolutional Neural Network (CNN) to effectively discriminate between genuine and forged signatures. A diverse dataset of signature images is collected and preprocessed to ensure data quality and consistency. The dataset undergoes resizing, normalization, and data augmentation to enhance model robustness. The CNN model is trained on the preprocessed dataset, learning discriminative features that characterize genuine signatures. Model evaluation is conducted on a separate test set to assess generalization performance. To ensure user adaptability, the system is designed to accommodate individual writing styles and variations. User-specific templates and adaptive learning mechanisms can be incorporated to further enhance system performance. A user-friendly interface is developed to facilitate system interaction and provide clear verification results. The CNN architecture will comprise convolutional, pooling, and fully connected layers, enabling the model to learn and classify the distinct characteristics of each signature effectively. Once trained, the model will be tested on unseen data to evaluate its ability to correctly identify forgeries. This system aims to minimize manual feature extraction, providing a more reliable and scalable solution for signature verification across various applications, including banking and security systems.

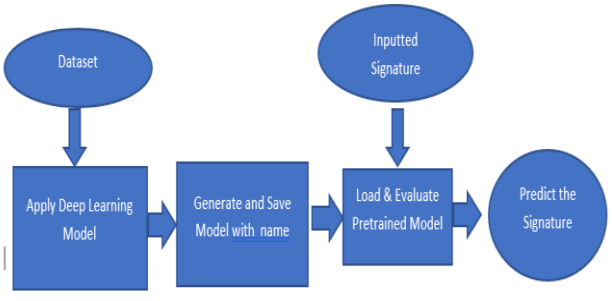

Fig. 1 Architecture of Proposed System

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

The system design for implementing a signature verification system using Convolutional Neural Networks (CNNs) involves several key steps. Here's a concise overview:

Dataset Collection: Dataset collection is a critical initial step in developing a signature verification system using Convolutional Neural Networks (CNNs). A well curated and diverse CEDAR dataset is used for training a robust model capable of recognizing and verifying various signature styles from Kaggle.

Data Preprocessing: Data preprocessing is a significant step in preparing the collected dataset for training a Convolutional Neural Network (CNN) in a signature verification system. Preprocessing involves normalizing, resizing, and augmenting the images to ensure consistency and variability. A carefully designed CNN model, with layers that reduce spatial dimensions while increasing depth, is then trained on this data.

Model Training: Model training is a pivotal phase in the development of a Convolutional Neural Network (CNN) for signature verification. This process involves optimizing the network's parameters based on a labelled dataset, enabling the model to learn discriminative features for distinguishing between genuine and forged signatures. In the context of signature verification, the following paragraph outlines key aspects of the model training phase.

Evaluation: Evaluation is a important step in assessing performance and effectiveness of the Convolutional Neural Network (CNN) developed for signature verification. For evaluating an automatic signature verification, an 80-20 split will be Based on 80% of the data dedicated to training and 20% to testing.

IV. IMPLEMENTATION RESULT

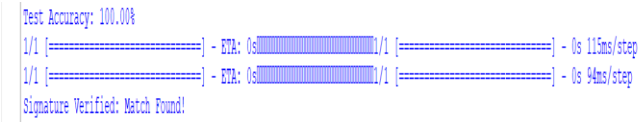

Fig. 2 Signature Verification Result

In a handwritten signature verification system, the expected outcomes typically include essential performance measures such as recall, precision, accuracy, and the F1-score (R value). Here's how these metrics might be evaluated:

1. **Accuracy**: This represents the proportion of correctly classified signatures (both genuine and forged) out of the total signatures tested. A high accuracy (e.g., 95% or above) would indicate that the model performs well in distinguishing between genuine and forged signatures.
2. **Precision**: Precision measures the proportion of true positive classifications (correctly identified genuine signatures) out of all positive classifications (both true positives and false positives). A precision close to 1 (e.g., 0.92 or 92%) shows that the system has a low false positive rate, meaning it is good at not falsely marking a forged signature as genuine.
3. **Recall**: Also known as sensitivity, recall reflects the proportion of true positives identified out of all actual positives. A recall of 90% or higher would indicate that the system is effective at correctly identifying genuine signatures, minimizing missed genuine signatures.
4. **F1-Score (R Value)**: The F1-score is the harmonic mean of recall and precision, balancing these two metrics. Ahigh F1-score (e.g., 0.91 or 91%) indicates that the model performs well both in terms of identifying genuine signatures and avoiding false positives.

Expected outcomes for an advanced handwritten signature verification system might look like this:

- **Accuracy**: 95-98%
- **Precision**: 92-95%
- **Recall**: 90-93%
- **F1-Score (R value)**: 91-94%

These metrics reflect a well-balanced system that is both accurate and reliable in verifying signatures while minimizing the risk of errors.

V. CONCLUSION

The study highlights the significant advancements in handwritten signature verification through the application of deep learning techniques. By thoroughly analyzing existing frameworks, including preprocessing strategies, feature extraction and verification models, this research provides valuable insights into the development of more reliable and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

fraud-resistant signature verification systems. By pinpointing the most suitable algorithm for different types of signatures, this research paves the way for advancements in security measures, ensuring the authenticity and integrity of signature-based transactions.

REFERENCES

[1]. Ritika and Dalip, "A Comparative Analysis of Machine Learning Based Frameworks for Handwritten Signature Verification," 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2024, pp.1275-1282, doi: 10.1109/ICESC60852.2024.10689878.

[2]. S. Tehsin, A. Hassan and F. Riaz, "Ensemble Learning for Offline Signature Verification using Fused Deep Features," 2024 s5th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan,2024, pp.1-6, doi: 10.1109/ICACS60934.2024.10473290.

[3]. M. Saleem, "Online Signature Verification Using Logistic Regression," 2023 9th International Conference on Control, Decision and Information Technologies (CoDIT), Rome, Italy, 2023, pp.1338-1342, doi: 10.1109/CoDIT58514.2023.10284050.

[4]. M. Saleem, "Online Signature Verification Using Logistic Regression," 2023 9th International Conference on Control, Decision and Information Technologies (CoDIT), Rome,Italy,2023,pp.1338-1342,doi: 10.1109/CoDIT58514.2023.10284050.

[5]. R. Sathya, S. Ananthi, R. Rupika, N. Santhiya and K. Lavanya, "Average Intensity Sign (AIS) Feature based Offline Signature Verification for Forgery Detection using Machine Learning," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy,India,2022,pp.325-330,doi: 10.1109/ICAISS55157.2022.10010812.

[6]. Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2013). A comprehensive review of biometric system security based on handwritten signature verification. IEEE Transactions on Information Forensics and Security, 8(3), 468-482.

[7]. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Offline handwritten signature verification—Literature review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(3), 788-801.

[8]. Soleimani, E., & Bidgoli, A. A. (2020). A hybrid deep learning model for offline handwritten signature verification using CNN and RNN. Journal of Imaging, 6(4), 33.

[9]. Diaz, M., Ferrer, M. A., & Morales, A. (2019). Generation of synthetic offline signatures based on real online data. IEEE Transactions on Cybernetics, 50(2), 561-572.

[10]. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2018). An evaluation of deep learning approaches for offline signature verification. Pattern Recognition Letters, 105, 378-384.

[11]. Burange, Anup & Misalkar, Harshal. (2015). Review of Internet of Things in development of smart cities with data management & privacy. 189-195. 10.1109/ICACEA.2015.7164693.