International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Automated Signature Verification for Academic Records: Enhancing Document Integrity and Administrative Efficiency

Adith D S[1], Shyma Kareem[2]

[1]Department of Computer Applications, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India
Email: *adithdileep04[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India

Abstract: ***The Signature Verification System is designed to enhance the security and integrity of document - related documents by providing a reliable solution for verifying signatures. This system aims to reduce the risk of forgery and ensure the authenticity of signatures on important documents, such as admission forms, exam papers, transcripts, and certificates. By integrating this system into the existing college administration processes, we aim to streamline and automate the verification process, thus improving efficiency and reducing the need for manual effort.***

Keywords: Deep learning models, Forgery detection, Pattern Recognition, Image preprocessing, Feature extraction, Signature classification, Behavioral signature analysis, Anomaly detection, Signature region localization, Document authenticity checking.

1. Introduction

In today's digital and paper - based environments, signature verification is crucial in ensuring the authenticity and integrity of important documents. Traditional manual verification methods are often time - consuming, prone to human error, and vulnerable to forgery. With the increasing prevalence of fraudulent activities, organizations, particularly educational institutions, need a robust and automated system to verify signatures accurately and efficiently. Colleges and universities rely on signatures for authentication in various administrative processes, such as student admissions, exam paper approvals, transcript issuance, and certificate authentication. The reliance on manual verification not only slows down operations but also increases the risk of forged signatures going undetected. Hence, there is a growing demand for a technology - driven solution that enhances the security and reliability of the signature verification process.

2. Literature Survey

Many studies have worked on improving signature verification and detection systems. Deep learning models like CNN and RNN are used to tell real and fake signatures apart. Some systems use scanned images (offline), while others track how the signature is written (online). New methods also combine different techniques to handle various writing styles. This section discusses certain works based on this topic.

Priya et al. [1] introduced a novel fuzzified deep learning approach for detecting forged signatures within healthcare mission records. Integrating fuzzy logic with deep neural networks enhances decision - making in ambiguous or borderline cases. The model demonstrates improved accuracy in detecting subtle forgeries, particularly in complex document environments with varied handwriting styles. However, the system's performance depends on high - quality labeled data and may require fine - tuning for application in other sectors outside of healthcare.

Abdulhussein et al. [2] present a signature verification model tailored for Arabic signatures, using a one - class support vector machine (OC SVM) optimized by a genetic algorithm. The approach effectively handles skilled forgeries by focusing on genuine signature patterns and refining model parameters through evolutionary optimization. The model shows strong results in identifying forgeries with minimal false acceptance. However, it may face challenges with diverse writing styles and depends on careful feature selection and parameter tuning.

Zhang et al. [3] address the detection of handwritten Chinese signatures in technical documents from power plants. The authors propose a lightweight detection method enhanced by a simple copy–paste data augmentation technique, which boosts model performance with minimal computational cost. The approach is well - suited for handling limited datasets and improves detection accuracy without requiring complex preprocessing. However, its application may be limited to document types and languages similar to the test data, with reduced generalizability to broader signature verification tasks.

Albasu et al. [4] explore the application of deep learning techniques for handwritten signature verification. The authors utilize advanced neural networks to improve the accuracy and robustness of signature authentication systems. By leveraging feature extraction and classification techniques, the model demonstrates significant improvements over traditional methods, offering higher reliability in detecting forged signatures. Despite these advancements, the study highlights challenges such as the need for large training datasets and computational complexity, which may hinder the scalability of real - time applications.

Muzaffar Hameed et al. [5] introduce Offside - SinGAN, a deep learning - based image augmentation model designed for offline signature verification. The model leverages the SinGAN architecture to generate high - quality signature variations, helping to address data scarcity and improve verification performance. By augmenting training datasets with synthetic samples, the system enhances the robustness and accuracy of signature verification systems. However, the study highlights that the model's effectiveness is strongly influenced by the quality of the generated samples and may encounter limitations when applied to diverse handwriting styles.

Hamadene et al. [6] introduce a novel method for detecting deepfake signatures by leveraging handcrafted feature extraction techniques. Unlike conventional deep learning models that may be susceptible to synthetic forgeries, the proposed approach focuses on analyzing key structural and geometrical properties of signatures, such as stroke width, direction, curvature, and local shape descriptors. These handcrafted features are used to detect subtle anomalies often present in AI - generated (deepfake) signatures that might be overlooked by end - to - end neural networks. It can better identify small mistakes in fake signatures that deep learning models may overlook. It is also faster and requires less computing power, making it suitable for low - resource systems. However, it requires expert involvement to thoughtfully design and choose appropriate features, which can be a time - intensive process. It may not adapt easily to different handwriting styles without adjustment. It also doesn't benefit as much from large amounts of data as deep learning does.

Nas et al. [7] introduced a signature verification system that uses fine - tuned transfer learning, meaning it builds on pre - trained deep learning models to recognize and verify signatures more accurately. This approach allows the system to work well even with limited signature data, reduces training time, and improves accuracy by leveraging knowledge from large datasets. It is particularly valuable for real - world applications where collecting large signature samples is difficult. However, it also has some limitations—fine - tuning can still require careful setup and computational resources, and the pre - trained model is not well - matched to the signature domain, so results may not be optimal.

Hameed et al. [8] introduce how machine learning is applied to authenticate handwritten signatures using image data. These systems can learn from data to tell real signatures from fake ones, which makes them faster and more accurate than manual methods. They also reduce the need for hand - crafted rules. The main advantages are better performance, automation, and the capacity to handle large amounts of data. However, they also have some drawbacks, such as needing a lot of training data, struggling with skilled forgeries, and sometimes being hard to understand or explain due to complex models.

Parcham et al. [9] introduce a new model that combines Convolutional Neural Networks (CNNs) with Capsule Networks (CapsNets) to verify signatures without needing data specific to each writer. This writer - independent approach improves flexibility and allows the system to work across different users. Its advantages include high accuracy, better handling of spatial relationships in signature features, and reduced need for user - specific training. However, it also has disadvantages such as higher computational complexity, longer training times, and the need for careful tuning of the network structure to achieve optimal performance.

Kao et al. [10] present a method to verify a signature and detect forgeries using just one genuine sample per user. It uses an explainable deep learning model, making the decision process more transparent and trustworthy. The main advantages of this approach are its practicality in real - world scenarios with limited data and its ability to explain why a signature is accepted or rejected. However, it also has some disadvantages, such as potential accuracy limitations due to using only one reference sample and the challenge of handling natural variations in genuine signatures.

3. Methodology

The proposed methodology for the signature verification system involves several key components. First, a secure database will be developed to store authenticated signatures, utilizing encryption to protect sensitive data. Multiple signature capture methods, including digital tablets, scanned images, and uploaded digital signatures, will ensure flexibility for users. The verification engine will rely on advanced machine learning and pattern recognition algorithms to accurately match signatures, minimizing false positives and negatives. The system will feature a user - friendly interface for easy document uploads, allowing smooth document processing and signature verification. To streamline the process, the system will automate the signature verification workflow, reducing manual intervention and improving efficiency. Data security will be prioritized with strong encryption and secure access controls, while compliance with legal and regulatory requirements, such as the ESIGN Act and GDPR, will be ensured. Additionally, the system will generate detailed verification reports and provide analytics on trends and performance, allowing for continuous development of the system. This methodology ensures a robust, secure, and efficient solution for digital signature verification.

3.1 Algorithm

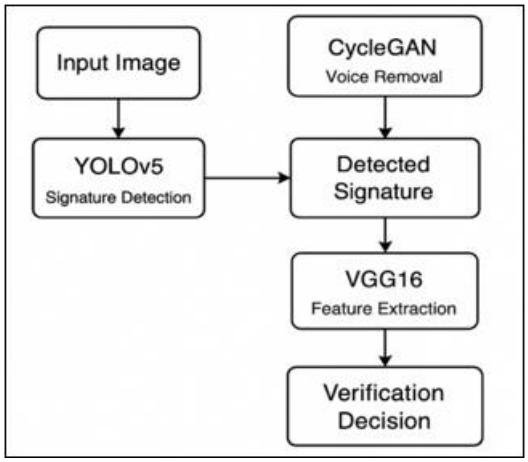
A signature verification system verifies if a message or document comes from a specific person and has not been changed. It works by verifying whether the electronic signature was forged or not. The system compares the signature with what already exists from the signature dataset. If they match, the signature is valid, meaning the message is authentic and hasn't been tampered with. There are three algorithms used:

YOLOv5 (You Only Look Once version 5): It's an improved object detection model known for its performance, flexibility, and ease of use. It operates as a single - stage detector, meaning it predicts both the class and location of objects in one step, unlike two - stage models like Faster R - CNN, which first propose areas of interest and then classify

them. YOLOv5 uses anchor boxes to predict bounding boxes for objects, learning the best fit for each object based on the training data. In a deep learning - based signature detection and verification system, YOLOv5 plays a crucial role in the signature detection phase. YOLOv5, an advanced object detection algorithm, is optimized for performance and accuracy. It is primarily used to detect objects in images and can be trained to recognize and locate signatures within scanned documents, pictures, or forms. By performing real - time object detection, YOLOv5 efficiently identifies the signature area in an image with high precision. The model works by drawing bounding boxes around detected signatures, providing the exact location of the signature within the image, and streamlining the next steps in verification.

CycleGAN plays a pivotal role in deep learning - based signature detection and verification systems by augmenting data (creating diverse signature styles), adapting the system across different domains, enhancing signature quality, and generating fake signatures for training purposes. It improves the system's robustness, accuracy, and ability to generalize across different signature variations and environments.

VGG16 is a convolutional neural network (CNN) model. VGG16 plays a critical role in signature detection and verification by acting as a powerful feature extractor, learning complex features from signature images. It can be used to compare and verify signatures based on the similarity of these features, aiding in both signature matching and forgery detection. Through transfer learning and fine - tuning, VGG16 can be adapted to work efficiently on signature datasets, even with inconsistencies in writing patterns and circumstances.



3.2 Dataset Used

The Tobacco 800 dataset includes 800 visuals focused on the specific task of signature detection. These images are typically scanned or captured from real - world documents, and they contain instances of digital logos and signatures that you aim to detect using the YOLOv5 object detection model. The dataset is structured to be compatible with the YOLO format, which is widely adopted for training object detection models.

The Kaggle signature dataset is applied to train a CycleGAN model that transforms noisy signatures into clean ones, and vice versa.

4. Result and Discussion

To evaluate the effectiveness of the system, various performance metrics were analyzed, including accuracy, precision, recall, and F1 - score. The system was tested using a dataset of real and forged signatures collected from official college documents. The system was tested using three different deep - learning models for comparison: YOLOV5, CycleGAN, and VGG16. The following table summarizes the performance of these models in signature verification.

Model	Accuracy	Precision	Recall	F1 - Score
YOLOV5	97.8%	96.5%	97.2%	96.8%
CYCLEGAN	94.2%	92.8%	93.5%	93.1%
VGG16	96.3%	95.2%	95.8%	95.5%
Manual Verification	85.0%	83.2%	84.1%	83.6%

The graphical representation based on the above table is given below. Here we can see the performance of manual verification.

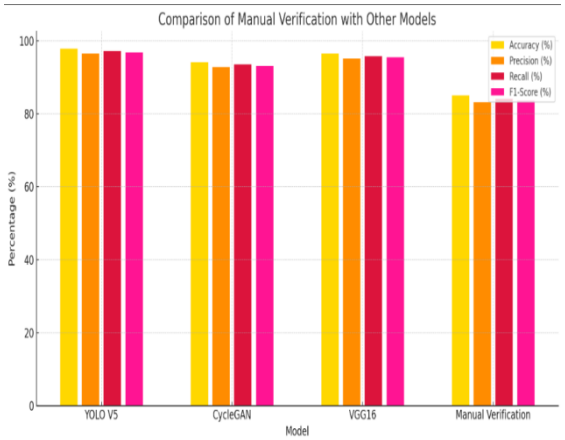


Figure 4: Graphical Representation

5. Conclusion

The Signature Verification System provides a reliable and efficient solution for verifying signatures, enhancing document security, and reducing the risk of forgery in educational institutions. By automating the verification process, the system minimizes manual errors, speeds up authentication, and ensures the integrity of critical documents such as admission forms, exam papers, and certificates. The feasibility study confirms that the system is technically, economically, operationally, legally, and schedule feasible, making it a practical and scalable solution. Through system implementation, testing, and comparison with manual verification, it is evident that the automated approach offers higher accuracy, better security, and faster processing. Incorporating machine learning methods greatly enhances the detection of forgeries, reducing the chances of fraudulent activities. This system not only benefits educational institutions but can also be extended to other sectors that require signature verification, such as banking and corporate organizations.

References

[1] Priya I., Chaurasia N., Alkhayyat A. (2024), Fuzzified Deep Learning based Forgery Detection of Signatures in the Healthcare Mission Records, ACM Transactions on Asian and Low - Resource Language Information Processing
[2] Abdulhussein A. A., Nasrudin M. F., Alyasseri Z. A. A., (2023), A Genetic Algorithm Based One - Class Support Vector Machine Model for Arabic Skilled Forgery Signature Verification, Journal of Imaging 9 (8).
[3] Zhang Y., Zhang J., Wang G., (2023), Handwritten Chinese signature detection with simple Copy–Paste augmentation on power plants technical documents, Service Oriented Computing and Applications, 17 (4) 293 - 302.
[4] Albasu F, Al Akkad M., (2023), Exploiting Deep Learning Techniques for the Verification of Handwritten Signatures, Intellekt. Sist. Proizv.21 (3) 27 - 39.
[5] Muzaffar Hameed M., Ahamad R. . Mazhar N, (2023). OffSig - SinGAN: A Deep Learning - Based Image Augmentation Model for Offline Signature Verification, Computers, Materials and Continua, 76 (1) 1267 - 1289.
[6] Hamadene A., Quahabi A., Hadid A., (2023), Deepfakes Signatures Detection in the Handcrafted Features Space, Proceedings - 2023IEEE/CVF International Conference on Computer Vision Workshops, ICCVW.
[7] Naz S., Bibi K., Ahmad R., (2022), DeepSignature: fine - tuned transfer learning based signature verification system, Multimedia Tools and Applications.
[8] Hameed M. M., Ahmad R., Murtaza G., (2021), Machine learning - based offline signature verification systems: A systematic review, Signal Processing: Image Communication.
[9] Parcham E., Ilybegi M., Amini M, (2021), CBCapsNet: A novel writer - independent offline signature verification model using a CNN - based architecture and capsule neural networks, Expert Systems with Applications.
[10] Kao H. H., Wan C. Y, (2020), An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach, Applied Sciences (Switzerland).