ICEST-2K24 [International Conference on Engineering, Science and Technology]
In Association with
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN - 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Revolutionizing Document Security: A Comprehensive Deep Learning Approach For Signature Detection and Verification

Prof. V. S. Nalawade[1], Anuj S. Dharurkar[2], Yash P. Aoute[2], Rushikesh D. Gunavare[2]

*[1]Dean Academics, Head – Department of AI & DS Engineering, SBPCOE Indapur, Maharashtra, India

[2]BE Computer Student, Department of Computer Engineering, SBPCOE Indapur, Maharashtra, India

ABSTRACT

This paper addresses key challenges in signature verification, acknowledging the deficiencies identified in previous research. Employing cutting-edge deep learning techniques, including YOLOv5 for signature detection, CycleGAN for noise reduction, and VGG16-based feature extraction for verification, our interdisciplinary approach caters to both digital and paper-based signatures. The workflow, encompassing detection, noise reduction, and verification, ensures heightened operational efficiency and accuracy in document management.

Moreover, the project recognizes and incorporates cultural and language variations influencing signatures, enhancing adaptability. Emphasizing the ethical and privacy dimensions, it establishes a framework to safeguard personal data during the verification process. In essence, this initiative not only highlights the limitations of existing methodologies but also presents a comprehensive solution, setting a new standard for signature verification systems.

Keywords: Document Security,Signature Detection, Signature Verification, DeepLearning, Convolutional Neural Networks (CNNs), Biometric Authentication, Forgery Detection.

I. INTRODUCTION

Analysing handwritten documents and confirming signatures are crucial tasks within pattern recognition and document processing. This comprehensive exploration delves into existing literature, emphasizing advancements in text line extraction and feature extraction for offline signature verification. Notably, methods like connected component analysis and the Hough transform are scrutinized for their effectiveness in extracting text lines from handwritten documents. In the realm of offline signature verification, Alsuhimat and Mohamad propose a hybrid approach that merges CNN and HOG techniques, evaluating its performance with three classifiers. This research significantly contributes to refining feature extraction methods and improving the accuracy of offline signature verification systems.

Impedovo and Pirlo offer an extensive overview of automatic signature verification, addressing techniques employed in both offline and online systems. Their work outlines various challenges and advocates for enhancements, providing a valuable resource for researchers. Furthermore, advancements in handwriting

analysis and forensic examination of signatures develop technologies for capturing and analyzing dynamic signatures, offering a reliable means of distinguishing forgeries.

Pharmaceutical innovation faces challenges. Research merges quantum computing and machine learning to revolutionize drug discovery, simulation, and safety assessment for expedited progress.[19]

This paper explores the latest developments in handwritten document analysis and signature verification. It discusses methodologies such as connected component analysis and the Hough transform for text line extraction, as well as Alsuhimat and Mohamad'shybrid approach for feature extraction in offline signature verification. The study also reviews the work of Impedovo and Pirlo on automatic signature verification, alongside discussions on handwriting analysis, forensic examination, and standardization efforts like ISO/IEC 19794-7:2014. Overall, it offers a succinct yet comprehensive overview of the evolving landscape within these domains.There are lots of ways in which security can be comprised even if we are using different ways for communication [11].Author presented an algorithm for detecting and preventing Node isolation attack where attacker become the sole MPR of victim and isolated the victim from the rest of the network.[12]. Here the paper [14] presents various aspects and formally defining the machine learning task of identifying malicious URLs. Project innovates plant species classification using Deep Learning and leaf vein features, aiming to automate identification, accelerate research, aid conservation, and foster education in botany and technology.[18]

II. PROPOSED SYSTEM

The project proposes an end-to-end signature verification system utilizing deep learning techniques, comprising signature detection using YOLOv5, noise cleaning with CycleGAN, and verification via a VGG16-based feature extractor.

A. Problem Statement

Traditional signature verification processes are time-consuming and resource-intensive. This project aims to automate and streamline the signature verification task, saving valuable time and resources.

B. Block Diagram

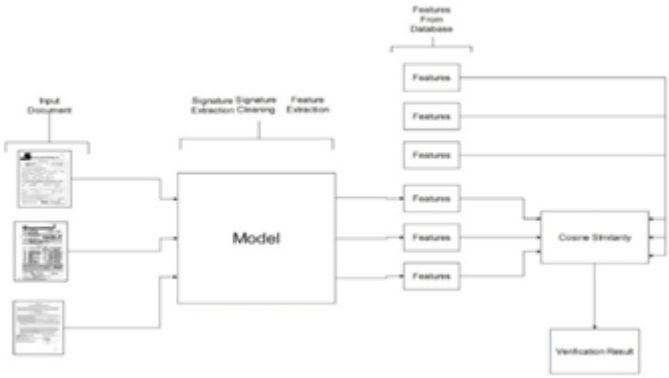

Figure1:System Architecture

The proposed system presents an end-to-end solution for signature verification, leveraging advanced deep learning methodologies. Signature detection is achieved using YOLOv5, extracting signatures from input

documents with high confidence. To address noise artifacts, a CycleGAN-based cleaning method is employed, enhancing the quality of detected signatures. Subsequently, a VGG16-based feature extractor is applied for signature verification, utilizing cosine similarity to determine the degree of similarity between reference and cleaned signatures. The workflow involves three key phases: detection, cleaning, and verification, providing a comprehensive solution for efficient and accurate signature authentication.

III.RESULT DISCUSSION

Figure2:Home Page

This is the home page of the Project and there is an option to choose which document you want to perform signature verification on. There is a detected signature button that gives the following output.

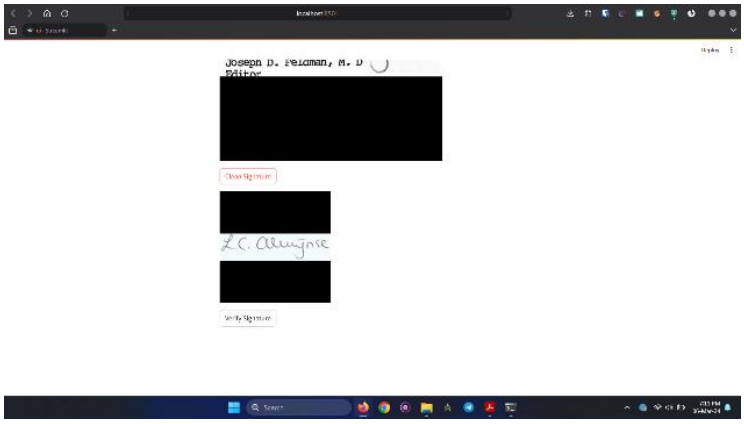

Figure3:Signature cleaned

Once cleaned the signature can be verified with the anchor image and the result of verification is displayed on the top right side of the image.

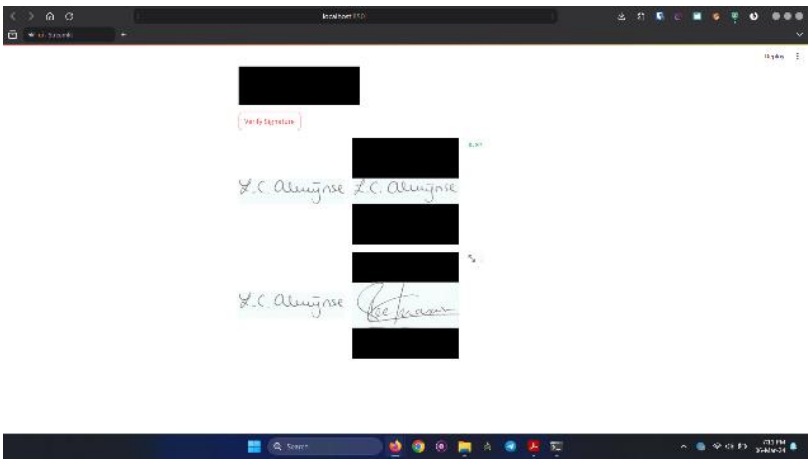

Figure4:Signature verified

The figure above shows the completed working of the document verification done using the proposed system.

IV. CONCLUSION

In conclusion, our result paper introduces an innovative system architecture aimed at verifying document authenticity through a meticulous process of signature analysis. The key steps involve signature extraction, where the model efficiently retrieves the signature from the input document. Following this, a pivotal phase of signature refinement eliminates noise, thereby enhancing the quality of the extracted signature.

The process then proceeds to feature extraction, where the signature undergoes transformation into a vector encapsulating crucial features such as shape, size, and orientation. The critical evaluation takes place via cosine similarity, quantifying the angle between the feature vector and the database features. The ultimate outcome of this process is the verification result, with a high cosine similarity score indicating a high probability of matching, thereby offering a robust measure of document authenticity.

This architecture not only tackles identified challenges but also establishes a new standard for accurate and efficient signature verification in document security applications.

V. REFERENCES

[1]. F. M. Alsuhimat and F. S. Mohamad, "A Hybrid Method of Feature Extraction for Signatures Verification Using CNN and HOG a Multi-Classification Approach," in IEEE Access, vol. 11, pp. 21873-21882, 2023, doi: 10.1109/ACCESS.2023.3252022.

[2]. S. Gonwirat and O. Surinta, "DeblurGAN-CNN: Effective Image Denoising and Recognition for Noisy Handwritten Characters," in IEEE Access, vol. 10, pp. 90133-90148, 2022, doi: 10.1109/ACCESS.2022.3201560.

[3]. N. Suciati, N. P. Sutramiani and D. Siahaan, "LONTAR_DETC: Dense and High Variance Balinese Character Detection Method in Lontar Manuscripts," in IEEE Access, vol. 10, pp. 14600-14609, 2022, doi: 10.1109/ACCESS.2022.3147069.

[4]. H. Li, P. Wei and P. Hu, "AVN: An Adversarial Variation Network Model for Handwritten Signature Verification," in IEEE Transactions on Multimedia, vol. 24, pp. 594-608, 2022, doi: 10.1109/TMM.2021.3056217.

[5]. Soumyadeep Kundu, Sayantan Paul, Suman Kumar Bera, Ajith Abraham, Ram Sarkar, "Text-line extraction from handwritten document images using GAN", in Expert Systems with Applications, Volume 140, 112916, 2020, doi: 10.1016/j.eswa.2019.112916.

[6]. B. L. Davis, C. Tensmeyer, B. Price, C. Wigington, B. S. Morse, and R. Jain, "Text and style conditioned GAN for generation of offline handwriting lines," British Machine Vision Conference, Sep. 2020, [Online]. Available: https://www.bmvc2020-conference.com/assets/papers/0815.pdf

[7]. R. Sanchez-Reillo, J. Liu-Jimenez and R. Blanco-Gonzalo, "Forensic Validation of Biometrics Using Dynamic Handwritten Signatures," in IEEE Access, vol. 6, pp. 34149-34157, 2018, doi: 10.1109/ACCESS.2018.2849503.

[8]. Z. Xia, T. Shi, N. N. Xiong, X. Sun and B. Jeon, "A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure KNN," in IEEE Access, vol. 6, pp. 46695-46705, 2018, doi: 10.1109/ACCESS.2018.2866411.

[9]. S. Biswas, D. Bhattacharyya, T.-H. Kim, and S. K. Bandyopadhyay, "Extraction of Features from Signature Image and Signature Verification Using Clustering Techniques," in Communications in computer and information science, 2010. doi: 10.1007/978-3-642-16444-6_62.

[10]. D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 609-635, Sept. 2008, doi: 10.1109/TSMCC.2008.923866.

[11]. Swapnali, Londhe, et al. "A Cryptographic Key Generation on a 2D Graphics Using RGB Pixel Shuffling and Transposition." Proceedings of the International Conference on Data Engineering and Communication Technology: ICDECT 2016, Volume 2. Springer Singapore, 2017.

[12]. K. S. Gaikwad and S. B. Waykar, "Detection and Removal Of Node Isolation Attack In OLSR Protocol Using Imaginary Nodes with Neighbour Response in MANET," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-5, doi: 10.1109/ICCUBEA.2017.8463762.

[13]. Agalave, K. N., KudaleAkanksha Narayan, ModaleShreya Anil, and TabePragatiShadanan. "A Survey OnDeepfake Image Generation Using Sketch." (2023).

[14]. Karve, S. M, Kakad , S, SwapnajaAmol, Gavali, A. B. ., Gavali , S. B. ., &Shirkande, S. T. . (2024). An Identification and Analysis of Harmful URLs through the Application of Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 456–468.

[15]. Ghuge, M., Ranjan, N., Mahajan, R. A., Upadhye, P. A., Shirkande, S. T., &Bhamare, D. (2023). Deep Learning Driven QoS Anomaly Detection for Network Performance Optimization.Journal of Electrical Systems, 19(2).

[16]. Shirkande, Shrinivas T., et al. "An Explainable Deep Learning Model for Clinical Decision Support in Healthcare." WSN and IoT. CRC Press 225-242.

[17]. Ajinath, B. S., Sunil, H. S., Digambar, K. S., Anandkumar, B. P., Nalawade, V. S., &Sayyad, G. G. (2018). Optimizing Information Leakage and Improve Security over Public Multi-Cloud Environment. Journal of emerging technologies and innovative research.

[18]. Ekatpure, J. N., Kamble, Y. P., More, P. T., & Patankar, S. S. (2023). A Survey On Leaf Vein Morphometrics: A Deep Learning Approach to Plant Classification.

[19]. Ekatpure, J. N., Jadhav, P., Gavali, R., Kale, P., &Padasalkar, S. (2023). Pharmaceutical Data Optimisation Using Quantum Machine Learning.